Ján Komara and Paul J. Voda

Metamathematics of Computer Programming

Institute of Informatics, Comenius University, Bratislava

April 30, 2001

Preface

A Historical Parallel.

We have seriously considered to call this book *Principia Programmationis* in allusion to the celebrated *Principia Mathematica* by Russell and Whitehead, which was published in 1911 in a gallant attempt to reduce mathematics to logic. Mathematics had stormily developed and matured during the nineteenth century and there was a real need to lay it on firm foundations. Especially after the Russell's paradox has shattered the monumental efforts in this direction by G. Frege and seriously dented the credibility of the naive set theory of G. Cantor.

Logicians have agreed only much later that the attempt was futile because with its principle of infinity mathematics relies on extra-logical facts, i.e. facts which do not hold in all possible worlds. The Zermelo-Fraenkel set theory is nowadays accepted by most mathematicians as the foundations of mathematics.

With the benefit of this hindsight we do not attempt in this book to reduce computer programming to logic. We reduce it to the most basic of formal theories: to the formalization of arithmetic known as *Peano Arithmetic* (PA for short). We think that after a half-century of tumultuous development of computer programming languages, and after many presentations of formal theories of programming (some of which go even beyond the powers of ZF) we have succeeded in the explication of mosts aspects of modern computer programming languages in such a simple formal theory (at least as its semantics is concerned). We view our choice of PA as a kind of Occam's razor. No programming language can be without arithmetic and we believe that nothing more is needed.

We have been encouraged in this belief by the successful use of our implementation of our computer programming language CL (*C*lausal *L*anguage) in teaching of mathematical logic and theory of programming for the last four years at University of Bratislava. We have approximately three hundred students per year taking four courses based on CL. CL is not only a programming language but also a formal system for the specification and proofs of properties of its programs.

Outline of the Text.

There is one more parallel between Principia Mathematica and the present text. Both, in their detailed development of their respective subjects (which cannot be avoided for the first time), can be perceived as tedious. In our case we refer here to the development of Peano Arithmetic in Chapters 7 and 8. The development is necessary for the formal justification of general recursive definitions which are considered de rigueur in modern computer programming.

We have included as an extended introduction a long Chapter 1 entitled *Case for the Theory of Programming in Peano Arithmetic* in order to shield a reader interested mainly in the general ideas of our philosophy from the rather technical development of the subject . We argue in the chapter in favor of the explication of computer programming in arithmetic. This means that an implemented computer programming language based on these concepts should use a formal system of arithmetic. Peano arithmetic is then the most natural choice. The introductory chapter covers the entire text in sufficient detail for the reader to understand our ideas and it avoids the formal apparatus of theorems and proofs although we present the necessary definitions with some technical details. If the reader is well-versed in mathematical logic and/or the theory of computer programming he might be even satisfied with the argument contained in the chapter. He will perphaps go to the following chapters only for a detail or two.

The explication of computer programming in the arithmetic is formally done in the Part II of this text. We have included the Part I, entitled *First-order theories and Peano arithmetic*, mainly as a prerequisite for the understanding of Part II. In this part we discuss first-order theories in general and Peano arithmetic in detail. The part is inluded not only to make this text self-contained but also to investigate the proof system of CL which are the signed tableaux of Smullyan. Since we extensively use the proof system for concrete proofs (as opposed to merely investigating it metatheoretically), we present the tableaux in the positive sense as proving logical consequence rather than in the usual negative sense of deriving contradictions. In the chapters dealing with Peano arithmetic we then investigate strong schemas of extensions of PA by definitions which support the kinds of flexible recursive definitions needed in the practice of computer programming.

The Part II is entitled *Computer programming* and it deals within the framework of PA with

– the definition of the clausal language,
– it is enlivened by many examples of actual CL programs together with proofs of their properties,
– discusses in the metatheory the computation of clausal programs,
– introduces data types in order to optimize the execution of clausal programs on computers,

– shows how to obtain the flexibility of high-order programming with functionals in the first-order Peano arithmetic,
– discusses the questions of modularization and abstract specification of programs in the language of second-order Peano arithmetic but within a framework which is conservative over PA and thus does not add any extra power (except expressivity) to it.

Targeted Audience.

We are fully aware that the answer to the question of whom is this text addressed to may solicit in the reader an unbelieving sneer, but the text is meant for three types of audience with all pairwise intersections almost empty.

Students. The first type are the novices in the field of theory of computer programming where we use this book in the teaching of two courses to our second year undergraduate students. The first course is *Logic for computer scientists* where we teach mathematical logic (up to and including the Completeness theorem) and Peano arithmetic. We deal in the course with the predicate calculus (propositional, equational, and quantification logic) as covered in Chapters 2 through 5) but rather than studying it formally, we stress the practical work in computer labs where we extensively use CL for proofs of tautological, quasitautological, logical, and arithmetical consequence. The latter consists of the development of Peano arithmetic as presented in Chapter 7 where we expect the students to prove all theorems of PA given in the chapter in the proof system of CL.

The second course is *Specification and verification of computer programs* where we use the formulas of PA for the the specification of programs, clausal definitions for their definition, and the proof system of CL for the proofs that the defined functions and programs meet the specifications. We completely cover the Chapters 11 through 16 of Part II. The material contained in these chapters contains more than four hundred theorems, (most of them proved in the text) of programs with clausal definitions. The programs deal with numeric, list and tree processing, as well as with symbolic problems. Our students are expected to prove in CL all theorems given in the text.

Logicians. The second type of audience are logicians interested in Computer Science. Obviously, they are not expected to have any problems with the material covered in Part I, but they might appeciate that the metatheory is completely finitary (we even give a new finitary proof of conservativity of Skolem axioms; something not normally done in the introductory texts). Logicians are also familiar with at least two mathematically impeccably founded programming languages, namely the language of Primitive recursive functions and of Primitive recursive functionals of finite types (Gödel's T). They also know how to compute such functions **effectively**. They might, however, be not aware of complex set of requirements which the designers of computer programming languages have to meet.

Of course, all logicians know that a computer programming language must be able to execute the programs **efficiently**. There are additional, no less important, pragmatical requirements of readability, simplicity, easy programmability, extensibility, and modularity. These are necessary because computer programs are large and they constantly undergo change. A good computer programming language should have versatile data structures within a typed environment. It must have provisions for modular design where whole blocks of code can be replaced with a new one without affecting the rest of the program. Our logician readers might be interested in how do we propose to meet this formidable set of practical criteria within the constraints of both of the relatively terse language of PA and of the relative weakness of its axioms.

Computer Scientists. The third, and probably the most critical, type of audience are Computer Scientists, especially those interested in the theory of programming. During the last fifty years an enormous number of computer programming languages emerged (and most of them quickly submerged) that our computer scientist reader is extremely sceptical of a yet another programming language. Moreover, a choice of a programming language is like a choice of dress to wear. Everyone has a strong set of preferences and adhers to a certain style. Just like fashion, programming languages are judged by value judgements with an apparent absence of objective criteria. Not all programming languages are based on a formal theory. This is not too unexpected as such languages are direct descedants of programs for Turing machines and the latter are basically kitchen recipes (do first this, then that, and repeat until done).

A Theory of Computer Programming .

The languages based on a formal theory widely differ in the strength of the theory. The theory may be as strong (even stronger) as ZF. For instance the languages based on the HOL (High-order logic) framework, or the language of the OBJ variety which are based in category theory. A wide group of languages is based on highly non-trivial theory of domains of Scott needed for the explication of continuous functionals. Examples are the well-known functional language Haskell and the language and the proof system PVS.

We try to explicate computer programming in a style and strength in many respects similar to the Computational logic of Boyer and Moore. The main difference is that we use as basis a formalization of arithmetic and everyone is familiar with arithmetic (if not with PA) from high school. Not only is the semantic basis of CL simple, but also the language of clausal definitions is entirely within the language of Peano arithmetic. The definitions have no reserved words whatsoever.

We know that many computer scientists, scarred by complexities of formal theories, tend to ignore them and they wholly concentrate on the writing of programs without pausing to ask what they do and what kind of objects they manipulate with. Situation is even worse because more often than not a programming language is designed only for its ellegant syntax and neat features. Only after the syntactical issues of its computation (so called *operational* semantics) have been fixed, the language designer starts to worry about the semantical issues of what the programs are (so called *denotational* semantics).

This practice of syntax before semantics runs totally opposite to the typical situation in mathematics where, as J. Shoenfield in the introduction to his *Mathematical logic* so convincingly argues:

> We may now describe what a mathematician does as follows. He presents us with certain basic concepts and certain axioms about these concepts. He then explains these concepts to us until we understand them sufficiently well to see that the axioms are true. He then proceeds to define derived concepts and to prove theorems about the basic and derived concepts. The entire edifice which he constructs, consisting of basic concepts, derived concepts, axioms, and theorems, is called an *axiom system*.

This is exactly how we propose to build a framework for computer programming languages except that the edifice which we construct is a framework for programming languages. Our basic concept is that programs are computable functions. By the Thesis of Church-Turing the computable functions are Turing computable functions over natural numbers and so we decide that our programs are to be definitions of functions and predicates over natural numbers. We do not have to build the theory of natural numbers from the scratch because we can use its well-known formalization: Peano arithmetic. We still have to introduce the derived concepts as used in computer programming (data structures, types, etc.). And we also have to bootstrap PA to the extent that it admits a very flexible kind of extensions by clausal definitions of functions and predicates. Clausal definitions serve a dual purpose. They describe *extensionally* the properties of the defined functions and predicates and at the same time they serve *intensionally* as rules for the computation of these objects.

Our experience with CL, which is an implementation of these ideas, shows that our students have no problems with understanding that they are writing programs operating over natural numbers. They also know that our coding of data structures into numbers in the style of LISP is perfectly natural. Finally, they can see that we can execute CL programs with the efficiency of Pascal and C operating over symbolic data structures.

Our Contributions. The main contribution of this book is an integrated attempt to explicate many of the issues of modern computer programming within a single framework of Peano Arithmetic. Within this overall goal there are some new perspectives which are our own:

1. the design of the clausal language with extensible syntax yet totally within the language of Peano arithmetic (no reserved words),
2. a new view of abstraction types (abstract data types) which goes around the sorts and congruences needed in the usual algebraic approach,
3. the development of a fragment of second-order Peano arithmetic which is conservative over first-order PA and offers a flexible calculus of extensions (modularization),
4. the characterization of a fragment of *bland* intensional functionals (as opposed to *curried* functionals) which can be introduced into PA with the typing comfort not available for the codes of primitive recursive (curried) functionals.

In the Part I dealing with logic we have contributed the following:

1. a presentation of the Henkin reduction of quantification logic to tautologies in three natural steps via quasitautological consequence,
2. a positive calculus of Smullyan's signed tableaux which gives them the flavor of natural deduction,
3. a simple finitary proof of conservativity of Skolem axioms,
4. a simple new Δ_0-definition of the graph $2^x = y$ of the exponentiation function,
5. a simple Δ_1-definable function V which is not provably recursive in PA. The function V is closely connected to the Wainer-Schwichtenberg fast growing hierarchies of functions.

Acknowledgments.

Table of Contents

1. Case for the Theory of Programming in Peano Arithmetic

This chapter is intended as an extended introduction. We informally present in it the entire material of this text. We argue here in favor of declarative programming over the domain of natural numbers within the most fundamental of formal theories: Peano arithmetic. Our argument is not in favor of a single language. We argue for the use of PA as a framework for the theory of computer programming. Although we occasionally discuss our language CL it should be understood only as an example of a possible implemetation of the ideas.

The style of presentation in this chapter is aimed at logicians and computer scientists. We suppose that the reader is acquainted with the language and basic methods of first-order logic as well as with the basic issues of the theory of computer programming languages. Undergraduate students will probably not be able to follow the exposition unless they have had a first reading exposure to the predicate calculus and the theory of programming languages.

An important note: The extended introduction temporarily serves also as a detailed description of the yet not written chapters and sections. This should explain a more detailed overview of these parts here. Eventually, when the missing chapters and sections will be supplied, some of the explanatory material will be removed. The level of presentation of parts not yet written is usually higher and more technical than the level of finished parts because the description is meant for expert logicians and computer scientists who might be refereeing this text.

1.1 Effectively Computable Functions

1.1.1 Formal systems. Both mathematical logic and theory of computer programming study formal systems. Formal systems deal with concretely presented syntactic objects. Syntactic objects in logic are terms and formulas and programs in computer programming.

Syntactic objects are usually assigned denotations in some mathematical domain. The usual presence of a system of derivations with rules of inference is the main reason for the study of formal systems in the logical discipline called *metamathematics*. Semantic questions of denotation are usually nonconstructive whereas the manipulation of syntactic objects can be done by effectively computable processes.

1.1.2 Effectively computable functions. Mathematical logic was developed in order to give firm foundations to mathematics. As it turned out, the characterization of *effectively computable* functions in logic was an important subgoal of this foundational goal. Such functions can be evaluated by a mechanical procedure. Alan Turing gave in 1936 a completely satisfactory explication of computable functions by means of what is now called Turing machines. He used the term *computer* to designate the agent performing the mechanical procedure. Turing meant a human computer, but as it turned out some ten years later chiefly by efforts of John von Neumann and Turing himself, computers could be constructed as mechanical or electronic devices.

The theory of computer programming studies the effectively computable functions but due to the practical limitations of computer hardware it has to deal mostly with its rather small subclass of *efficiently* (feasibly) computable function.

1.1.3 The domain of effectively computable functions. Although one can develop the theory of computable functions over integers (both negative and positive numbers), over a subset of real numbers, over word domains, or over many suitably structured domains; logicians know that it suffices to restrict the theory of computable programs to the domain $\mathbb{N}$ of *natural numbers*: $0, 1, \ldots$. This is, first of all, because the greatest success of nineteen century mathematics was the discovery that all numeric domains can be defined from the domain of natural numbers. The second reason is that K. Gödel in the proof of his Incompleteness theorem convincingly demonstrated that symbolic (syntactic) objects can be coded into numbers. The process of coding is called *arithmetization* and the codes are *Gödel numbers*.

Whether we can do the same reduction to $\mathbb{N}$ of domains of computer programming languages is by no means obvious. We will argue in Sect. 1.3 in favor of the reduction but the majority of computer scientists think that special domains are necessary in order to attain efficiency.

1.1.4 Notational basis for computable functions. We know from elementary school that addition and multiplication can be effectively computed when their operands are concretly presented as, say, decimal numerals. The choice of notation basis is not important when we are interested only in effectivity and so mathematicians prefer *monadic* notation where the natural number n is presented as the syntactic object, called a *monadic numeral*: $(0\overbrace{{}'\ldots{}'}^{n})$.

When we want also efficiency then the base should be positive and the most natural one for electronic computers is binary. *Binary numerals* are terms constructed from the constant 0 by applications of two unary functions, called *binary successors*, and written in a postfix notation: $x\mathbf{0} = 2{\cdot}x + 0$ and $x\mathbf{1} = 2{\cdot}x + 1$. The reader will note that, for instance, we have

$$5 = 2{\cdot}(2{\cdot}(2{\cdot}0 + 1) + 0) + 1 = 0\mathbf{101} \ .$$

Leading zeroes cause notational ambiguity because $1 = 0\mathbf{1} = 0\mathbf{01} = 0\mathbf{001}\ldots$ and so we require that binary numerals of a form $\tau\mathbf{0}$ have the term $\tau \not\equiv 0$. We designate by $\underline{n}_b$ the binary numeral denoting the number n. This term yielding function satisfies:

$$\begin{aligned} \underline{0}_b &\equiv 0 \\ \underline{n\mathbf{0}}_b &\equiv \underline{n}_b\mathbf{0} \qquad \text{if } n > 0 \\ \underline{n\mathbf{1}}_b &\equiv \underline{n}_b\mathbf{1} \ . \end{aligned}$$

The reader will note that for any number x we have

$$x = 0 \lor \exists z(x = z\mathbf{0} \land z > 0) \lor \exists z\, x = z\mathbf{1}$$

with the numbers z uniquely determined, and with the three conditions pairwise exclusive.

1.1.5 Closure of operations over natural numbers. Addition and multiplication are *closed* over natural numbers. This means that both $x + y$ and $x{\cdot}y$ are natural numbers when x and y are. The remaining two basic arithmetical operations go outside of natural numbers, for instance $3 - 5$ and $\frac{3}{5}$. We must use instead *modified subtraction* $x \dot{-} y$ satisfying:

$$x \dot{-} y = \begin{cases} x - y & \text{if } x \geq y, \\ 0 & \text{otherwise} \end{cases}$$

and *integer division* and *remainder* functions $x \div y$ and $x \mod y$ satisfying:

$$\begin{aligned} y > 0 \rightarrow x = (x \div y){\cdot}y + x \bmod y \land x \bmod y < y \\ x \div 0 = x \bmod 0 = 0 \ . \end{aligned}$$

All five basic arithmetic functions over $\mathbb{N}$ can be efficiently computed by elementary school algorithms.

Unless we explicitly say otherwise all our functions and predicates will be over natural numbers until the end of this chapter. Also our variables and quantifiers will range over natural numbers.

1.2 Imperative vs. Declarative Programming

The style of programming derived from operations of Turing machines where programs are recipes for the manipulation of computer's store is called in computer science *imperative* programming. The style of programming where programs are definitions of mathematical objects such as functions or predicates is called *declarative* programming. The difference between the two styles is best explained with two definitions of the greatest common divisor function.

1.2.1 Greatest common divisor. The binary relation x *divides* y, in symbols $x \mid y$, can be defined in the language of logic by

$$x \mid y \leftrightarrow \exists z\, x{\cdot}z = y \ .$$

A number z is the *greatest common divisor of* x *and* y, in symbols $\gcd(x,y) = z$, iff $x = y = 0$ and $z = 0$ or if $x + y > 0$ and z divides both x and y where z is the largest of such numbers d:

$$x + y > 0 \rightarrow z \mid x \wedge z \mid y \wedge \forall d(d \mid x \wedge d \mid y \rightarrow d \leq z) \ . \tag{1}$$

We have $1 \mid x$ and $1 \mid y$ and so when $x + y > 0$ we can effectively find the greatest common divisor by a brute force search which starts from x and goes downwards towards 1.

The ancient mathematician Euclides discovered a faster algorithm computing gcd which relies on the following property of divisibility:

$$y > 0 \rightarrow (z \mid x \wedge z \mid y \leftrightarrow z \mid y \wedge z \mid x \bmod y). \tag{2}$$

1.2.2 The algorithm of Euclides imperatively. The algorithm of Euclides can be expressed by an imperative computer program in the style of Pascal as:

$$\begin{array}{l} \{x = x_0 \wedge y = y_0\} \\ \textit{while } y > 0 \textit{ do} \\ \quad a := x \bmod y;\ x := y;\ y := a; \\ \{\gcd(x_0, y_0) = x\} \ . \end{array} \tag{1}$$

The algorithm proceeds by operation on three registers x, y, and a located on the tape of a Turing machine or in the memory of a computer. It is basically a kitchen recipe which says that the contents of the three registers should be repeatedly swapped in the given order as long as the register y contains a positive number.

When the algorithm is started with the registers x and y containing the numbers x_0 and y_0 respectively and with arbitrary contents of the contents of register a then when, and if, the swapping terminates the register x will contain the number $\gcd(x_0, y_0)$. The reader will note that the text enclosed within the pair of braces {} is not a part of the program and should be viewed as a remark.

For arguments $x_0 = 12$ and $y_0 = 21$ we need six tests of the register y which happen in the following sequence of memory snapshots with the contents of registers given immediately above the single solid lines:

x	y	a
12	21	–
12	21	12
21	21	12
21	12	12
21	12	9
12	12	9
12	9	9
12	9	3
9	9	3
9	3	3
9	3	0
3	3	0
3	0	0

1.2.3 The algorithm of Euclides declaratively. We will discuss in Part II of this text how *Peano arithmetic*, which is a well-known logical theory formalizing the arithmetic, permits an introduction of the binary function symbol gcd by a *clausal definition*:

$$\gcd(x,0) = x \tag{1}$$
$$\gcd(x,y) = \gcd(y, x \bmod y) \leftarrow y > 0\ . \tag{2}$$

The reader will note that $\leftarrow$, which is customarily used in clausal definitions, is just a converse implication. The two clauses should be understood as the axioms implicitly characterizing the function gcd. The definition is legal because a *meausure* of the two arguments x and y goes down in recursion. The measure is the second argument y and since, the following is easily provable in PA:

$$y > 0 \rightarrow x \bmod y < y\ ,$$

the second argument $x \bmod y$ of the recursive application $\gcd(y, x \bmod y)$ in the clause (2) decreases because the clause is applied only when $y > 0$.

Incidentally, this is exactly the reason why the imperative program (1) always terminates. We, namely, go into the *while* only when $y > 0$. The register y will contain $x \bmod y$ just before the next iteration where x and y are the values at the moment of the entry to the *while*.

The computation of $\gcd(12, 21)$ can be visualized as a sequence of syntactic operations, called *reductions*, which are initially applied to the term $\gcd(12, 21)$ and which use the two clauses in an attempt to simplify the term to a numeral:

$$\gcd(12,21) \overset{(2)}{=} \gcd(21,12) \overset{(2)}{=} \gcd(12,9) \overset{(2)}{=} \gcd(9,3) \overset{(2)}{=} \gcd(3,0) \overset{(1)}{=} 3\ .$$

The reader will note that the computation sequence is structurally equivalent to the underlined memory snapshots for the imperative program where the two arguments of gcd play the role of the registers x and y.

1.2.4 Proving the two gcd **programs correct.** We will now briefly look into the question of how to formally ensure that the imperative and declarative programs for the greatest common divisor work correctly. The function gcd is uniquelly determined by satisfying its *specification* 1.2.1(1) in the following form:

$$\gcd(x,y) \mid x \wedge \gcd(x,y) \mid y \tag{1}$$
$$x+y>0 \wedge d \mid x \wedge d \mid y \to d \leq \gcd(x,y) \tag{2}$$
$$\gcd(0,0) = 0\ . \tag{3}$$

The simplest way of proving the correctness of the imperative program is to reason in a system of formal arithmetic, say PA, where we have already demonstrated the conditions (1) through (3). From the conditions we prove the recurrences 1.2.3(1)(2). We then annotate the imperative program with comments as follows:

$\{x = x_0 \wedge y = y_0 \wedge \gcd(x,y) = \gcd(x_0,y_0)\}$
while $y > 0$ *do*
  $a := x \bmod y;\ x := y;$
  $y := a;\ \{\gcd(x,y) = \gcd(x_0,y_0)\}$
$\{y = 0 \wedge x \stackrel{1.2.3(1)}{=} \gcd(x,0) = \gcd(x,y) = \gcd(x_0,y_0)\}\ .$

We can then use the calculus of pre and post conditions by A. Hoare and show that the formulas given at the annotated points can be proved. The formula $\gcd(x,y) = \gcd(x_0,y_0)$ is an *invariant* of the *while* loop because it holds whenever one tests $y > 0$.

In order to prove that the invariant holds at the end of the body of the loop one has to prove in Hoare's calculus:

$\{x = x_1 \wedge y = y_1 \wedge \gcd(x_1,y_1) = \gcd(x_0,y_0)\}$
$a := x \bmod y;$
$\{a = x_1 \bmod y_1 \wedge y = y_1 \wedge \gcd(x_1,y_1) = \gcd(x_0,y_0)\}$
$x := y;$
$\{a = x_1 \bmod y_1 \wedge x = y_1 \wedge \gcd(x_1,y_1) = \gcd(x_0,y_0)\}$
$y := a;$
$\{y = x_1 \bmod y_1 \wedge x = y_1\}$
$\{\gcd(x,y) = \gcd(y_1, x_1 \bmod y_1) \stackrel{1.2.3(2)}{=} \gcd(x_1,y_1) = \gcd(x_0,y_0)\}$

In order to prove the correctness of the declarative definition of the function gcd by clauses 1.2.3(1)(2) we have to demonstrate its specification formulas (1) through (3).

We prove $\forall x(1)$ by complete induction on y. We take any x and consider two cases. If $y = 0$ then, since $\gcd(x,0) = x$ by 1.2.3(1), we trivially have $\gcd(x,0) \mid x$ and $\gcd(x,0) \mid 0$. If $y > 0$ then we have $\gcd(x,y) = \gcd(y, x \bmod y)$ by 1.2.3(2) and, since $x \bmod y < y$, we obtain $\gcd(y, x \bmod y) \mid y$ and

$\gcd(y, x \bmod y) \mid x \bmod y$ by IH. We then use 1.2.1(2) to get $\gcd(y, x \bmod y) \mid x$.

We prove $\forall x(2)$ by complete induction on y. We take any x, assume $x + y > 0$, $d \mid x$, $d \mid y$ and consider two cases again. If $y = 0$ then, since we must have $x > 0$, we get $d \le x = \gcd(x, 0)$. If $y > 0$ then, since $d \mid x \bmod y$ by 1.2.1(2) and $y < x \bmod y$, we get

$$d \overset{\text{IH}}{\le} \gcd(y, x \bmod y) = \gcd(x, y) \ .$$

Property (3) trivially follows from 1.2.3(1).

1.2.5 Imperative versus declarative programming I. If we do not care about the correctness of our programs and are concerned only with their efficiency then we should probably program imperatively because such programming is with few restrictions. If we are willing to live with some restrictions of declarative programming then as discussed in Par. 1.2.7 the declarative development of highly symbolic programs can be faster and cheaper even without proofs of correctness.

If the correctness of our programs is important then the proofs are much easier for declarative programs as was shown in the preceding paragraph. In both cases we had to use a formal theory axiomatizing the domain of our objects. For the example of the greatest common divisor the domain was $\mathbb{N}$ and so the the formal theory will probably be PA. In both cases we had to introduce the function gcd into the theory and prove some of its properties.

For the proof of the declarative program we never left PA because the clausal definition of the new function was in the language of PA and its clauses were axioms. The proof proceeded by simple induction.

For the proof of the imperative program we uses two languages: the imperative programming language and the language of PA. We also used two formal systems: the calculus of Hoare and PA. The correctness proof was much longer, we had to introduce auxiliary variables, and at the end we have proven only the *partial* correctness of the program. We still have to do an inductive proof that the program always terminates.

The only argument in favor of imperative programming is efficiency. In the given example both programs have comparable efficiency. In the following paragraph we show the same for another example.

1.2.6 Fibonacci function. The function $\mathrm{fib}(n)$ yielding the n-th element of the well-known *sequence of Fibonacci* satisfies the following recurrences:

$$\mathrm{fib}(0) = 1 \tag{1}$$
$$\mathrm{fib}(1) = 1 \tag{2}$$
$$\mathrm{fib}(n + 2) = \mathrm{fib}(n + 1) + \mathrm{fib}(n). \tag{3}$$

The definition is by a straightforward recursion decreasing the argument in $<$. We can directly use the recurrences for computations. For instance, we can compute $\mathrm{fib}(4) = 3$ as follows:

$$\mathrm{fib}(4) \overset{(3)}{=} \mathrm{fib}(3) + \mathrm{fib}(2) \overset{2\times(3)}{=} \mathrm{fib}(2) + \mathrm{fib}(1) + \mathrm{fib}(1) + \mathrm{fib}(0) \overset{(3);2\times(2);(1)}{=}$$
$$\mathrm{fib}(1) + \mathrm{fib}(0) + 1 + 1 + 0 \overset{(2);(1)}{=} 1 + 0 + 2 = 3 \ .$$

The only problem is that the computation sequence is too long. In order to compute the number $\mathrm{fib}(n+2)$ one needs to use the recurrence (3) exactly $\mathrm{fib}(n+2)$ times as can be proved by a simple induction. The Fibonacci function grows as fast as the exponential function and to compute the function in this way is simply too wasteful.

The following Pascal-like program computes $\mathrm{fib}(n)$ into the variable b:

$a := 1;\ b := 0;$
while $n > 0$ *do*
$\quad n := n \dot{-} 1;\ c := a;\ a := a + b;\ b := c;$

The reader will note that the loop is executed only n times. This example is usually given as the 'standard argument' against declarative programming where the recursive version is clearly inferior to the imperative one. The argument is fallacious as one should define an auxiliary ternary function $f(n, a, b)$ with two *accumulators* a and b by *primitive recursion* decreasing the first argument:

$f(0, a, b) = b$
$f(n + 1, a, b) = f(n, a + b, a).$

By straightforward induction on n we can then prove:

$$\forall k\, f(n, \mathrm{fib}(k + 1), \mathrm{fib}(k)) = \mathrm{fib}(n + k)$$

and then explicitly define:

$$\mathrm{fib}(n) = f(n, 1, 1).$$

The number of recursions of f is exactly the same as the number of iterations of the loop of the imperative program. Moreover, a good compiler can remove the so called *tail recursion* in the definition of f and compile it exactly as the *while*-loop in the above Pascal-like program.

1.2.7 Imperative versus declarative programming II. Imperative programs can be better compiled than declarative ones when large data structures are modified in them. Imperative programs can do updates directly in the memory. This is not possible in declarative programs without some restrictions. We will discuss this point in more detail **UNFINISHED** and only note here that our implementation of CL is written in the declarative programming language Trilogy 2 designed and implemented in 1991 by one of the authors. Trilogy 2 has declarative provisions for in situ updates and thus the CL compiler excecutes with comparable efficiency as if it were written in an imperative language.

Trilogy programs, by being declarative, are on a much higher level of abstraction than the commands for the modification of storage typical for imperative programming. It is our estimate that the cost of implementation and maintenance of the Trilogy 2 compiler for CL was about a quarter of what the cost would have been had we implemented CL in an imperative language.

1.3 Arguments in Favor of Natural Numbers

We have argued in the prececeding section in favor of declarative over imperative programming. With the decision that our programs should have denotations as functions and predicates we must still decide on the domain of interpretation. We know from Church-Turing thesis that natural numebers suffice as the domain of computable functions. In this section we extend the argument to programming languages and we outline a natural development of data structures needed in computer programming within the domain $\mathbb{N}$. This kind of development is called *arithmetization*.

Arithmetization of Word Domains.

1.3.1 Word domains. Turing machines operate over word domains which consist of finite sequences of symbols from an alphabet. More precisely, an *alphabet* Σ is given by a finite set of *symbols* $\{a_1, a_2, \cdots, a_n\}$. A *word* over an alphabet Σ is a finite sequence of symbols of Σ. The *empty* word is the empty sequence denoted by $\emptyset$. The *length* of a word is the length of its sequence. The *domain of words* over Σ, denoted by Σ^*, is the set of all words over Σ.

Theory of computability codes a natural number n by a word of length n over a one element alphabet where $a_1 \equiv |$. We denote by $|^n$ the sequence $\overbrace{|\cdots|}^{n}$. A finite sequence of numbers x_1, x_2, $\ldots$, x_n can be then coded as a word over the two element alphabet $a_1 \equiv |$, $a_2 \equiv \#$ as

$$\#|^{x_1}\#|^{x_2}\ldots\#|^{x_n} \ .$$

1.3.2 Arithmetization of word domains. Word domains are by no means more general than natural numbers. We can turn functions over the word domain Σ^* given by the p-element alphabet $\Sigma = \{a_1, a_2, \cdots, a_p\}$ into functions over natural numbers by means of *p-adic representation* of natural numbers. For that purpose we define p functions, called *p-adic successor* functions, S_1, S_2, $\ldots$, S_p as follows:

$$S_i(x) = p{\cdot}x + i \ .$$

It is not difficult to see that every natural number has a unique representation as a *p-adic numeral*:

$$S_{i_m}\, S_{i_{m-1}}\, \dots\, S_{i_2}\, S_{i_1}(0)$$

where $m \geq 0$ and for every $1 \leq j \leq m$ we have $1 \leq i_j \leq p$. This p-adic numeral codes the word $a_{i_1} a_{i_2} \dots a_{i_m}$. Note that the empty word $\emptyset$ is coded by the p-adic numeral 0. Thus every natural number is a code of exactly one word over Σ. P-adic numerals should be viewed as concrete objects consisting of terms in the form of sequences of function symbols S_i which are terminated by 0.

The reader will note that the monadic representation of natural numbers introduced in Par. 1.1.4 is a special case of p-adic representation with $p = 1$. The monadic successor function $S_1(x) = 1{\cdot}x{+}1 = x'$ is the successor function.

1.3.3 Dyadic representation of $\mathbb{N}$. A special case of p-adic representation with $p = 2$ is the *dyadic* representation. The advantage of the dyadic representation over binary (see Par. 1.1.4) is that there is no restriction on leading digits. The dyadic successor functions S_1 and S_2 are written in the postfix notation: $x\mathbf{1} = 2{\cdot}x + 1$ and $x\mathbf{2} = 2{\cdot}x + 2$. *Dyadic numerals* are the least class of terms containing the constant 0 and with every term τ also the terms $\tau\mathbf{1}$ and $\tau\mathbf{2}$.

Consider the first eight words from the sequence of words over the two symbol alphabet $\mathbf{1}$, $\mathbf{2}$ which is ordered first on the length and within the same length lexicographically:

$$\emptyset, \mathbf{1}, \mathbf{2}, \mathbf{11}, \mathbf{12}, \mathbf{21}, \mathbf{22}, \mathbf{111}, \dots$$

The corresponding dyadic numerals are:

$$\begin{aligned}
0 &= 0\\
0\mathbf{1} &= 2{\cdot}0 + 1 = 1\\
0\mathbf{2} &= 2{\cdot}0 + 2 = 2\\
0\mathbf{11} &= 2{\cdot}(2{\cdot}0 + 1) + 1 = 3\\
0\mathbf{12} &= 2{\cdot}(2{\cdot}0 + 1) + 2 = 4\\
0\mathbf{21} &= 2{\cdot}(2{\cdot}0 + 2) + 1 = 5\\
0\mathbf{22} &= 2{\cdot}(2{\cdot}0 + 2) + 2 = 6\\
0\mathbf{111} &= 2{\cdot}(2{\cdot}(2{\cdot}0 + 1) + 1) + 1 = 7\ .
\end{aligned}$$

The process of going from operations over certain domain to the operations over the codes of elements of the domain in $\mathbb{N}$ is called the *arithmetization* of the domain.

1.3.4 Dyadic size. The *dyadic size* function $|x|_d$ yields the number of dyadic successors in the dyadic numeral denoting the number x. The function is the arithmetization of the *word-size* function taking a word over $\{\mathbf{1},\mathbf{2}\}$ and yielding its length. The dyadic size function has a clausal definition:

$$
\begin{aligned}
&|0|_d = 0\\
&|x\mathbf{1}|_d = |x|_d + 1\\
&|x\mathbf{2}|_d = |x|_d + 1\ .
\end{aligned}
$$

Clearly, the numbers x such that

$$2^n - 1 = 0\mathbf{1}^n \leq x \leq 0\mathbf{2}^n = 2^{n+1} - 2$$

and no others have the dyadic size n.

1.3.5 Dyadic concatenation. The basic operation over words is *concatenation*. For instance, the words **211** and **122** over the alphabet $\{\mathbf{1},\mathbf{2}\}$ are concatenated into the word **211122**.

The arithmetization of concatenation over the alphabet $\{\mathbf{1},\mathbf{2}\}$ is the binary function $x \star y$, called *dyadic concatenation*. It yields a number whose dyadic representation is obtained from dyadic representations of x and y by appending the digits of y after the digits of x. The function has the following clausal definition:

$$x \star 0 = x \tag{1}$$
$$x \star y\mathbf{1} = (x \star y)\mathbf{1} \tag{2}$$
$$x \star y\mathbf{2} = (x \star y)\mathbf{2}\ \ . \tag{3}$$

The dyadic word **211** is coded by the number $0\mathbf{211} = 11$ and the word **122** by $0\mathbf{122} = 10$. We obtain the code of the concatenated word **211122** by using the clauses of the dyadic concatenation function in a computation as follows:

$$0\mathbf{211} \star 0\mathbf{122} \overset{(3)}{=} (0\mathbf{211} \star 0\mathbf{12})\mathbf{2} \overset{(3)}{=} (0\mathbf{211} \star 0\mathbf{1})\mathbf{22} \overset{(2)}{=} (0\mathbf{211} \star 0)\mathbf{122} \overset{(1)}{=} 0\mathbf{211122}\ .$$

The reader will note that although the code of the concatenated words is $0\mathbf{211122} = 88$, the computation can proceeds by a simple rewriting without ever having to convert into the decimal notation.

The arithmetization of word domains is so natural that we will identify words with their codes.

Arithmetization of Finite Sequences.

1.3.6 Symbolic domains. Computer programming, in addition to the standard numerical types, involves a large number of *data structures* such as n-tuples, multidimensional arrays (vectors and matrices), lists, stacks, tables, trees, graphs, etc. Standard programming languages (both imperative and functional ones) therefore work with quite complicated domains obtained by solutions of recursive identities. We think that this is an unnecessary complication and we look for a solution to the programming language LISP which offers excellent coding of symbolic data structures into the domain of *S-expressions*. This domain is freely generated from the set of countably many *atoms* by a binary operation *cons*. There is no advantage in having infinitely many atoms, just one, say, *nil* suffices. There is also no advantage of having S-expressions as a separate domain. Nothing is lost and much is gained by the arithmetization of the domain of S-expressions in $\mathbb{N}$.

1.3.7 Pairing function. We obtain the coding convenience of LISP in the domain of natural numbers by arithmetizing the domain of symbolic expressions with the help of a suitable binary *pairing* function (x, y). The function, which, will be discussed in detail in Sect. 8.3, will have the following properties:

$$(x, y) = (v, w) \rightarrow x = v \land y = w \tag{1}$$
$$v < (v, w) \land w < (v, w) \tag{2}$$
$$x = 0 \lor \exists v \exists w\, x = (v, w)\ . \tag{3}$$

The property (1) is called the *pairing property* and it ensures that for every number n in the range of the pairing function, i.e. such that $n = (x, y)$ for some x and y, the numbers x and y, called the *first* and *second projections of* n respectively, are uniquely determined. The pairing property says that the pairing function is an injection. From the property (2) we get $0 \leq x < (x, y)$. This means that 0 is not in the range of the pairing function and so it has no projections, i.e. $0 \neq (x, y)$. Thus the number 0 is an *atom* and plays the role of the atom *nil* of LISP. The property (3) asserts that the pairing function is onto the set $\mathbb{N} \setminus \{0\}$, i.e. that 0 is the only atom.

1.3.8 Pair numerals. It can be easily proved by complete induction that every natural number n can be uniquely presented as a term called *pair numeral*. The class of pair numerals is the least class of terms containing 0 and with every two terms τ_1 and τ_2 also the term (τ_1, τ_2). We call this the *pair representation* of $\mathbb{N}$.

1.3.9 Pair size. The length of the pair numeral τ denoting the number x is $5{\cdot}n{+}1$ where n is the number of pairing operations used in the construction of the term τ. The arithmetization of the length function is the *pair size* function $|x|_p$ yieding the number of pairing operations needed for the construction of the pair numeral denoting x. The function is defined by the following clausal definition:

$|0|_p = 0$
$|(x, y)|_p = |x|_p + |y|_p + 1\ .$

1.3.10 Cantor's pairing function. Without fixing the pairing function (x, y) we do not know the pair representation of any natural number except 0 and our next step is to determine the function. We first note that the standard *diagonal* function J of Cantor (see [4]) when offset by one (to account for the atom 0), i.e. the function

$$J(x,y) = (x+y)\cdot(x+y+1) \div 2 + x + 1 \ ,$$

satisfies the properties 1.3.7(1) through 1.3.7(3). The initial segment of J is tabulated in Fig. 1.1. The subscripts of values for $J(x,y)$ give the pair size $|J(x,y)|_p$.

$J(x,y)$	0	1	2	3	4	5	6	$\cdots$
0	1_1	2_2	4_3	7_3	11_4	16_4	22_4	$\cdots$
1	3_2	5_3	8_4	12_4	17_5	23_5	30_5	$\cdots$
2	6_3	9_4	13_5	18_5	24_6	31_6	39_6	$\cdots$
3	10_3	14_4	19_5	25_5	32_6	40_6	49_6	$\cdots$
4	15_4	20_5	26_6	33_6	41_7	50_7	60_7	$\cdots$
5	21_4	27_5	34_6	42_6	51_7	61_7	72_7	$\cdots$
6	28_4	35_5	43_6	52_6	62_7	73_7	85_7	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Fig. 1.1. Pairing function $J(x,y)$

Unfortunately, the pairing function J is not suitable for us because it cannot be used for the development of small functional computational classes such as polynomial time, polynomial space, linear space etc. This was demonstrated in [24]. The reason why J is not suitable can be seen when we enumerate the natural numbers in the J-pair representation. The numbers with the same pair size are not grouped together as it is the case with the binary size of numbers enumerated in the binary notation. We can see from Fig. 1.1 that in the middle of the group of consecutive numbers 4 through 10 we have two numbers with the pair size 4, namely $8 = J(J(0,0), J(0, J(0,0)))$ and $9 = J(J(0, J(0,0)), J(0,0))$, while the remaining numbers have the pair size three.

1.3.11 Suitable pairing function. We obtain a suitable pairing function (x,y) by keeping the numbers with the same pair size together. For that we note that every natural number in pair representation can be viewed as a *binary tree*. Here 0 is represented by the *empty* tree and the number (x,y) is represented by a tree with the left subtree representing x and the right subtree representing y. Note that that the number of inner nodes of the tree representing x is $|x|_p$. We *enumerate* all binary trees by listing the binary trees with the lesser number of inner nodes before the ones with larger number of inner nodes. Two different binary trees t_1 and t_2 with the same number of inner nodes are listed *lexicographically*. This means that t_1 is listed before t_2

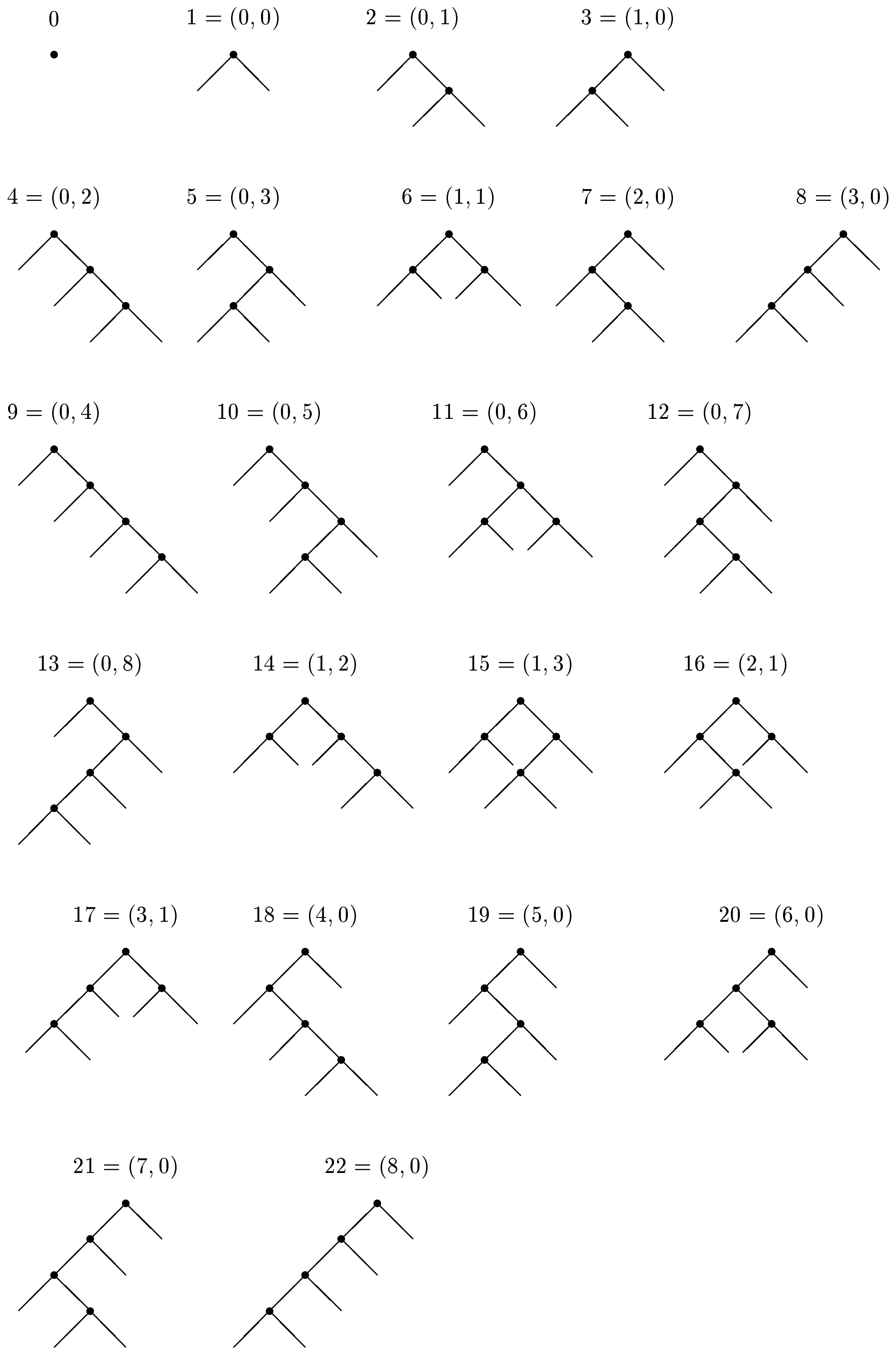


Fig. 1.2. Enumeration of binary trees

if its left subtree is listed before that of t_2, or if the left subtrees are identical, the right subtree of t_1 is listed before that of t_2. An initial segment of the enumeration is given in Fig. 1.2.

The enumeration of binary trees uniquely fixes the pairing function (x, y). Namely, for two numbers x and y we take the x-th and y-th binary trees t_1 and t_2 (counting from zero). The position of the binary tree $\langle t_1, t_2\rangle$ is the value of (x, y). Fig. 1.3 lists the initial segment of values of (x, y) in a tabular form. The subscripts give the pair size $|(x, y)|_p$. The function will be formally introduced into PA in Sect. 8.3 where we also prove the properties 1.3.7(1) through 1.3.7(3) as theorems of PA.

It can be shown that as a consequence of keeping the numbers with the same pair size together we will have $|x|_p = \Theta(\log(x))$, i.e. $|x|_p = O(\log(x))$ and $\log(x) = O(|x|_p)$. This property assures a natural characterization by pairing of computational complexity classes such as polynomial time or space (see [24]).

(x,y)	0	1	2	3	4	5	6	$\cdots$
0	1_1	2_2	4_3	5_3	9_4	10_4	11_4	$\cdots$
1	3_2	6_3	14_4	15_4	37_5	38_5	39_5	$\cdots$
2	7_3	16_4	42_5	43_5	121_6	122_6	123_6	$\cdots$
3	8_3	17_4	44_5	45_5	126_6	127_6	128_6	$\cdots$
4	18_4	46_5	131_6	132_6	399_7	400_7	401_7	$\cdots$
5	19_4	47_5	133_6	134_6	404_7	405_7	406_7	$\cdots$
6	20_4	48_5	135_6	136_6	409_7	410_7	411_7	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Fig. 1.3. Pairing function (x, y)

1.3.12 Projection functions. The pairing property 1.3.7(3) asserts that every non-zero number x has a form (v, w) for some numbers v and w which are uniquely determined by 1.3.7(1). The numbers are accessed by unary projection functions. The *first projection* function H (head) satisfies the following identities:

$$\begin{aligned} H(0) &= 0 \\ H((v, w)) &= v \;. \end{aligned}$$

The *second projection* function T (tail) satisfies the following identities:

$$\begin{aligned} T(0) &= 0 \\ T((v, w)) &= w \;. \end{aligned}$$

It should be clear that we have

$$x = (H(x), T(x)) \leftrightarrow x > 0 \;.$$

1.3.13 Contraction to unary functions. We now establish a natural correspondence between n-ary and unary functions and predicates over $\mathbb{N}$.

If f is an n-ary function then we denote by $\langle f\rangle$ its *contraction*, which is an unary function defined as follows:

$$\langle f\rangle(x) = \begin{cases} f(x_1, x_2, \ldots, x_n) & \text{if } x = x_1, x_2, \ldots, x_{n-1}, x_n \\ 0 & \text{otherwise.} \end{cases}$$

From the above we get

$$f(x_1, x_2, \ldots, x_n) = \langle f\rangle((x_1, x_2, \ldots, x_{n-1}, x_n)) \ .$$

We note that the contraction $\langle f\rangle$ of an unary function f is the function f itself. For $n > 1$ we clearly have

$$\begin{aligned} \exists x_1 \cdots \exists x_n\, x = (x_1, \cdots, x_n) &\leftrightarrow x = H\,T^0(x), H\,T^1(x) \,\cdots\, H\,T^{n-2}(x), T^{n-1}(x) \\ &\leftrightarrow T^{n-2}(x) > 0 \end{aligned} \tag{1}$$

and thus we have

$$\langle f\rangle(x) = \begin{cases} f(H\,T^0(x), H\,T^1(x) \,\cdots\, H\,T^{n-2}(x), T^{n-1}(x)) & \text{if } T^{n-2}(x) > 0 \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

If R is an n-ary relation then we denote by $\langle R\rangle$ its *contraction*, which is an unary predicate, satisfying:

$$\langle R\rangle(x) \leftrightarrow \exists x_1 \exists x_2 \ldots \exists x_n\, (\, x = (x_1, x_2, \ldots, x_{n-1}, x_n) \land R(x_1, x_2, \ldots, x_n)\,) \ .$$

From this we get

$$R(x_1, x_2, \ldots, x_n) \leftrightarrow \langle R\rangle((x_1, x_2, \ldots, x_{n-1}, x_n)) \ .$$

Thus in the presence of pairing there is no essential difference between n-ary and unary functions, except that the expression $f(x)$ is meaningless for an n-ary function whenever $n > 1$ but well-defined for its contraction $\langle f\rangle(x)$.

1.3.14 Conventions for the symbol comma. We will usually omit the outermost pairing parentheses around pairing (τ_1, τ_2). Thus, for instance, we can write $f(x) = g(x), h(x)$ instead of $f(x) = (g(x), h(x))$. We postulate that the pairing operator ',' groups to the right, i.e. that (τ_1, τ_2, τ_3) abbreviates $(\tau_1, (\tau_2, \tau_3))$. We assign the lowest precedence to pairing. Thus $x + y \cdot v, z$ is an abbreviation for $((x + (y \cdot v)), z)$.

The omission of parentheses around pairing can lead to ambiguities in situations where commas could be confused with the separators of arguments of n-ary functions. In such situations when we write $f(\tau_1, \cdots, \tau_n, \cdots, \tau_{n+m})$

we (obviously) treat the commas as separators of arguments if $m = 0$ and we understand the expression as an abbreviation for $f(\tau_1, \cdots, (\tau_n, \cdots, \tau_{n+m}))$ if $m > 1$. Thus the first $n-1$ commas separate the arguments while the remaining ones are the infix pairing operators. We adopt similar comma conventions for n-ary predicates.

For instance, if f is binary then $f((\tau_1, \tau_2), (\tau_3, \tau_4, \tau_5))$ can be abbreviated by the dropping of the outermost pairing parentheses to $f((\tau_1, \tau_2), \tau_3, \tau_4, \tau_5)$. The reader will note that we cannot drop the parentheses around τ_1, τ_2. If R is an unary predicate then $R((\tau_1, \tau_2))$ can be written as $R(\tau_1, \tau_2)$.

We extend the dual role of commas to sequences like $\vec{x}$ and $\vec{\tau}$. For instance, when f is an n-ary function then the basic property of its contraction $\langle f \rangle$ is:

$$\langle f \rangle(x_1, \cdots, x_n) = f(x_1, \cdots, x_n) .$$

The commas on the left of the identity stand for the pairing operator while they are separators on the right. We can abbreviate this to $\langle f \rangle(\vec{x}) = f(\vec{x})$ with the same understanding about the commas in the sequence $\vec{x}$.

1.3.15 Arithmetization of finite sequences over $\mathbb{N}$. There is a simple way of arithmetizing finite sequences over natural numbers. We assign the code 0 to the empty sequence $\emptyset$. The non-empty sequence $x_1\, x_2\, \ldots\, x_n$ is coded by the number $(x_1, x_2, \ldots, x_n, 0)$ (see Fig. 1.4). The reader will note that the assignment of codes is one to one, every finite sequence of natural numbers is coded by exactly one natural number, and vice versa, every natural number is the code of exactly one finite sequence of natural numbers. Codes of finite sequences are called *lists* in computer science and this is how we will be calling them from now on.

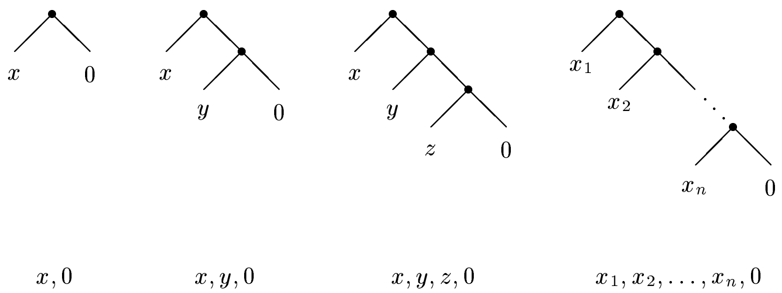


Fig. 1.4. Lists

1.3.16 Length of lists. The list $x_1, x_2, \ldots, x_n, 0$ codes a finite sequence of natural numbers of length n and we say that the list has the *length* n. The length function $L(x)$ has the following clausal definition:

$$L(0) = 0$$
$$L(x, y) = L(y) + 1 \quad .$$

1.3.17 Concatenation of lists. The binary *list concatenation* function $x \oplus y$ has the following clausal definition:

$$0 \oplus y = y \tag{1}$$
$$(v, w) \oplus y = v, w \oplus y \quad . \tag{2}$$

As an example we show here the computation of $(1, 2, 3, 0) \oplus (4, 5, 0)$. The computation uses the clauses as rewriting rules and there is no need during the computation to convert into decimal (or binary notation):

$$(1, 2, 3, 0) \oplus (4, 5, 0) \overset{(2)}{=} 1, (2, 3, 0) \oplus (4, 5, 0) \overset{(2)}{=} 1, 2, (3, 0) \oplus (4, 5, 0) \overset{(2)}{=} 1, 2, 3, 0 \oplus (4, 5, 0) \overset{(1)}{=} 1, 2, 3, 4, 5, 0 \; .$$

1.3.18 List indexing. The binary *list indexing* function $(x)_i$ yields the i-th element (counting from 0) of the list x. For instance, $(0, 1, 2, 3, 0)_2 = 2$. The indexing function is defined by the following clausal definition:

$$(0)_x = 0$$
$$(v, w)_0 = v$$
$$(v, w)_{i+1} = (w)_i \; .$$

Arithmetization of Trees.

1.3.19 Arithmetization of labeled binary trees. The type Bt of *binary trees labeled by natural numbers* can be defined in most functional programming languages by a *union type*:

$$Bt = E \mid Nd(\mathbb{N}, Bt, Bt) \; ,$$

This asserts that a value of type Bt is either the *leaf* E or a *node* of the form $Nd(x, t_1, t_2)$ where t_1 and t_2 are values of type Bt and $x \in \mathbb{N}$ is the *label* of the node. The constant E and the function Nd are called *constructors*.

We arithmetize the values of the type Bt with the help of two constructor functions $E = 0, 0$ and $Nd(x, t_1, t_2) = 1, x, t_1, t_2$. Note that this guarantees that we have $E \neq Nd(x, t_1, t_2)$. The predicate $Bt(t)$ holding of codes of labeled binary trees t has a clausal definition corresponding to the union type definition:

$$Bt(E)$$
$$Bt\, Nd(x, t_1, t_2) \leftarrow Bt(t_1) \land Bt(t_2) \quad .$$

We identify labeled binary trees with their codes and from now on we will say the *binary tree* t instead of the *code of the binary tree* t.

1.3.20 Flattening of binary trees. As an example of an operation over binary trees we consider the function $Flat(t)$ taking a binary tree t and yielding the list of all labels in t read off t from left to right. The function has the following clausal definition:

$$\begin{aligned}&Flat(E) = 0\\&Flat\,Nd(x, t_1, t_2) = Flat(t_1) \oplus (x, Flat(t_2))\ .\end{aligned}$$

We can save the repeated concatenation by keeping the flattened list in an accumulator with an auxiliary binary function $f(t, a)$:

$$\begin{aligned}&f(E, a) = a\\&f(Nd(x, t_1, t_2), a) = f(t_1, x, f(t_2, a))\quad .\end{aligned}$$

We can now explicitly define a fast flatten by:

$$Flat(t) = f(t, 0)\ .$$

The correctness of this definition on labelled trees follows from the following property:

$$Bt(t) \rightarrow \forall a\, f(t, a) = Flat(t) \oplus a$$

proved by complete induction on t.

1.3.21 Binary search trees. A binary tree t is a *binary search tree* if for every subtree of t labeled by n all labels in its left son are less than n and all labels in the right son are greater than n. This is equivalent to the requirement that the labels of a binary search tree read off from left to right increase. Hence, the predicate Bst holding of binary search trees has the following explicit definition:

$$\begin{aligned}Incr(t) &\leftrightarrow \forall i \forall j (i < j < L(t) \rightarrow (a)_i < (a)_j)\\Bst(t) &\leftrightarrow Incr\,Flat(t)\ .\end{aligned}$$

1.3.22 Membership in binary search trees. The binary predicate $x \in_b t$ of *membership in binary search tree*, has the following property:

$$Bst(t) \rightarrow (x \in_b t \leftrightarrow \exists i (i < L(Flat(t)) \wedge (Flat(t))_i = x))\ .$$

The predicate has the following clausal definition:

$$\begin{aligned}&x \in_b Nd(y, t_1, t_2) \leftarrow x < y \wedge x \in_b t_1\\&x \in_b Nd(y, t_1, t_2) \leftarrow x = y\\&x \in_b Nd(y, t_1, t_2) \leftarrow x > y \wedge x \in_b t_2\ .\end{aligned}$$

Arithmetization of Symbolic Expressions

1.3.23 Numeric terms. Suppose that we wish to operate symbolically on numeric terms, which we call here *expressions*, and which are formed from constants n and variables x_i by the arithmetic operators $+$ and $\cdot$. Functional programming languages use the following union type to specify the domain of expressions:

$$Expr = Cns(\mathbb{N}) \mid Var(\mathbb{N}) \mid Add(Expr, Expr) \mid Mul(Expr, Expr) \ .$$

We arithmetize the expressions with the help of four constructors with explicit clausal definitions:

$$\begin{aligned}
&Cns(x) = 0, x \\
&Var(x) = 1, x \\
&Add(x, y) = 2, x, y \\
&Mul(x, y) = 3, x, y \ .
\end{aligned}$$

We can now code, for instance, the expression $356{\cdot}x_3 + x_5$ by the number

$$\begin{aligned}
&Add(Mul(Cns(356), Var(3)), Var(5)) = \\
&\quad 2, (3, (0, 356), 1, 3), 1, 5 = 3\,442\,660\,716\,284 \ .
\end{aligned}$$

That the code is larger than three trillion should not be too surprising as its pair size is 25 and the ratio between the length of decimal numbers and pair size is roughly 1 to 2 (the ratio between the length of dyadic and pair size is roughly 1 to 1.

The predicate $Expr(a)$ true of codes a of expressions corresponds to the above union type and has the following clausal definition:

$$\begin{aligned}
&Expr\ Cns(c) \\
&Expr\ Var(i) \\
&Expr\ Add(a, b) \leftarrow Expr(a) \wedge Expr(b) \\
&Expr\ Mul(a, b) \leftarrow Expr(a) \wedge Expr(b) \ .
\end{aligned}$$

1.3.24 Denotation function for expressions. We now define the binary *denotation* (valuation) function $Val(c, v)$ taking the code c of an expression τ and an *assignment* v which is a list assigning the value $(a)_i$ to the variable x_i. The application $Val(c, v)$ yields the value of the expression τ when the variables occurring in the expression take their values from the assignment v. The denotation function has the following clausal definition:

$$\begin{aligned}
&Val(Cns(c), v) = c \\
&Val(Var(i), v) = (v)_i \\
&Val(Add(a, b), v) = Val(a, v) + Val(b, v) \\
&Val(Mul(a, b), v) = Val(a, v) \cdot Val(b, v) \ .
\end{aligned}$$

This is a typical example where we wish to use the default clauses in order not to clutter the definition. We do not care what value is yielded by the application $Val(c, n)$ if c does not code an expression. The reader will note that in such case the value is not necessarily 0 because c can be ‘almost’ an expression. For instance $Val(Add(0, Cns(1)), 0) = 1$.

Arithmetization of Numeric Domains

1.3.25 Arithmetization of the domain of integers $\mathbb{Z}$. Integers, which extend the natural numbers with the negative whole numbers, are used in computer programming perhaps more often than the natural numbers. Instead of extending the domain of natural numbers $\mathbb{N}$ to the domain $\mathbb{Z}$ of integers we arithmetize the latter domain in $\mathbb{N}$. For that we need two constructor functions $+(x) = 0, x$ and $-(x) = 1, x$ which respectively code the positive (including 0) and negative (excluding 0) numbers. The predicate $\mathbb{Z}(k)$ which holds if k codes an integer has the following explicit definition:

$$
\begin{aligned}
&\mathbb{Z}(+(n)) \\
&\mathbb{Z}(-(n+1)) \ .
\end{aligned}
$$

The subtraction function $x - y$ which is closed over the domain $\mathbb{Z}$, i.e. such that

$$\mathbb{Z}(x) \land \mathbb{Z}(y) \rightarrow \mathbb{Z}(x - y)$$

holds, has the following explicit clausal definition:

$$
\begin{aligned}
&+(n) - +(m) = +(n \dot{-} m) \leftarrow n \geq m \\
&+(n) - +(m) = -(m \dot{-} n) \leftarrow n < m \\
&+(n) - -(m+1) = +(n + m + 1) \\
&-(n+1) - +(m) = -(n + m + 1) \\
&-(n+1) - -(m+1) = -(n \dot{-} m) \leftarrow n \geq m \\
&-(n+1) - -(m+1) = +(m \dot{-} n) \leftarrow n < m \ .
\end{aligned}
$$

We can define other arithmetic functions over $\mathbb{Z}$ in a similar style.

1.4 Extensional Issues of Definability in PA

The reader accepting our arguments in the preceding sections agrees that our programs are to be definitions of computable functions and predicates over the domain $\mathbb{N}$ of natural numbers. Definitions are concrete objects given in a formal system of arithmetic and the defined function and predicate symbols posses denotations in the domain $\mathbb{N}$. Formal systems are necessary because neither humans nor computers can work directly with the abstract domain of natural numbers. The most natural candidate for the formal system is the Peano arithmetic.

In this section we discuss the definitions of functions and predicates in PA from the *extensional* point of view where we are not interested whether they are computable. Non-computable functions and predicates play important role in the theory of programming because they are used with advantage for the specification and proofs of properties of computable functions.

Recursive Bootstrapping of Peano Arithmetic

1.4.1 Peano arithmetic. Peano arithmetic is formulated as a first-order logical theory in the language consisting of the constant 0, the unary function symbol x', and of two binary function symbols $x + y$ and $x \cdot y$. The intended interpretation of PA is in the *standard model* $\mathcal{N}$ with the domain of natural numbers $\mathbb{N}$ and with the interpretation of its symbols in the above order as the number 0, the *successor* function $S(x) = x + 1$, the addition, and the multiplication functions.

The axioms of Peano arithmetic are

$$
\begin{gathered}
0 \neq x' \\
x' = y' \to x = y \\
0 + y = y \\
x' + y = (x + y)' \\
0 \cdot y = y \\
x' \cdot y = x \cdot y + y
\end{gathered}
$$

plus the infinite number of *induction axioms* of the form

$$\phi[0] \wedge \forall x(\phi[x] \to \phi[x']) \to \phi[x] \tag{1}$$

for every formula $\phi[x]$ of the language. It is easy to see that all axioms are satisfied in the standard model $\mathcal{N}$.

We denote by $\underline{n}_m$ the monadic numeral (see Par. 1.1.4) for n. Precisely, $\underline{n}_m$ is defined as a metatheoretical function yielding terms of PA to satisfy:

$$
\begin{aligned}
\underline{0}_m &\equiv 0 \\
\underline{n+1}_m &\equiv (\underline{n}_m)' \;.
\end{aligned}
$$

1.4.2 Classification of formulas of PA. UNFINISHED definability of functions and predicates

1.4.3 Fragments of Peano Arithmetic. UNFINISHED

Σ_i-definable in T. Provably recursive in T. Primrec.

1.4.4 Extensions of Peano arithmetic. Computer programming consists of defining new functions and predicates. Formal tools for this activity in logic are *extensions* of theories, in our case extensions of PA. This happens by the addition of a new function or predicate symbol to the language of the current extension of PA together with new axiom(s) defining the symbol.

We do not wish the extended theory to be *inconsistent* in the sense that it can prove theorems not satisfiable in the standard model, for instance $0 = 1$. Once $0 = 1$ is a theorem, the theory can prove any formula. The unextended theory PA cannot prove any formulas not satisfied in $\mathcal{N}$ and so it is consistent.

In order to maintain the consistency we restrict our extensions to *conservative* ones. Conservative extensions do not prove any new theorems in the language before the extension, i.e. formulas which do not contain the new symbol. Since $0 = 1$ is such a formula the extended theory is consistent. We actually go even further and restrict our extensions to *extensions by definitions* which are a special case of conservative extensions where the extended theory cannot prove any properties not expressible already in the original language of PA. New function and predicate symbols are thus only a notational convenience which make our theorems and definitions more readable. We gain on expressivity but not on power.

When we say PA in the following we always mean the current extension of Peano arithmetic.

1.4.5 Extensions of PA by explicitly defined predicates. We can extend PA with the binary comparison predicate $x < y$ by adding it to the language of the theory and then add a new axiom fully describing the predicate:

$$x < y \leftrightarrow \exists z\, x + z' = y \ .$$

We can then use the axiom in proving properties of the new symbol, for instance the transitivity:

$$x < y \wedge y < z \rightarrow x < z \ .$$

The extension does not add any strength to PA because we can always eliminate all occurrences of $<$ from a formula by replacing applications $\tau_1 < \tau_2$ by formulas $\exists z\, \tau_1 + z' = \tau_2$.

In general, for any formula $\phi[x_1, \ldots, x_n]$ of the current extension T of PA we can form its extension S by *explicit definition of a predicate* by adding a new n-ary predicate symbol R together with its *defining axiom*:

$$R(x_1, \ldots, x_n) \leftrightarrow \phi[x_1, \ldots, x_n] \ . \tag{1}$$

The new symbol can be always eliminated from a formula ψ of S by a *translation* similar to the one describes above whereby we obtain a formula $\psi^\star$ of T. The extended theory S proves that the two formulas are equivalent: $\psi \leftrightarrow \psi^\star$. The conservativity of S over T follows from the fact that S proves ψ iff T proves $\psi^\star$.

We can even use the new predicate symbol R in induction formulas ψ of the form 1.4.1(1) where ϕ is arbitrary formula of the language of S. This is because the translation $\psi^\star$ is an induction formula provable in the theory T. S, by being an extension of T, proves $\psi^\star$ and, since it also proves $\psi \leftrightarrow \psi^*$, the theory S proves the induction formula ψ.

The reader will note that we have already used a definition by explicit definition of a predicate in Par. 1.2.1 where we have defined

$$x \mid y \leftrightarrow \exists z\, x{\cdot}z = y \ .$$

1.4.6 Extensions of PA by contextually defined functions. We can extend PA by explicit definitions of functions similarly to extensions by explicit definitions of predicates. For instance, we can introduce the *square* function x^2 by explicit definition: $x^2 = x{\cdot}x$. In general case we can take a term $\tau[x_1, \ldots, x_n]$ and introduce a new n-ary function symbol f by explicit definition with the defining axiom:

$$f(x_1, \ldots, x_n) = \tau[x_1, \ldots, x_n] \; . \tag{1}$$

While certainly useful, this kind of extensions does not fully utilize the power of logical notation to the same extent as extensions by explicit definitions of predicates. Formulas ϕ in extensions 1.4.5(1) can contain arbitrary propositional connectives and quantifiers. The simpler syntax of terms τ in extensions (1) has not the same power of expression.

We can use formulas in explicit definitions of function symbols where we define a new function symbol in the context of a formula where instead of the function f we introduce its *graph* $f(x_1, \ldots, x_n) = y$ as an $(n+1)$-ary relation. For instance, the modified subtraction function $x \dot{-} y$ can be introduced by an explicit contextual definition as:

$$x \dot{-} y = z \leftrightarrow x \geq y \land x + z = y \lor x < y \land z = 0 \; .$$

The trick is that no matter what the numbers x and y are, exactly one of $x \geq y$ and $x < y$. Moreover, in the former case there is a unique z s.t. $x + z = y$.

In general, for any formula $\phi[x_1, \ldots, x_n, y]$ of the current extension T of PA for which T proves the *existence* and *uniqueness* conditions:

$$\exists y \phi[x_1, \ldots, x_n, y] \tag{2}$$

$$\phi[x_1, \ldots, x_n, y_1] \land \phi[x_1, \ldots, x_n, y_2] \rightarrow y_1 = y_2 \tag{3}$$

we can form the extension S by *contextual definition of a function* by adding a new n-ary function symbol f together with its *defining axiom*:

$$f(x_1, \ldots, x_n) = y \leftrightarrow \phi[x_1, \ldots, x_n, y] \; . \tag{4}$$

The new symbol can be always eliminated from a formula ψ of S by a translation $\psi^\star$. The main idea is that for every formula $\psi[y]$ s.t. $\psi[f(\tau_1, \ldots, \tau_n)]$ is a formula of S the theory S proves

$$\psi[f(\tau_1, \ldots, \tau_n)] \leftrightarrow \exists y (f(\tau_1, \ldots, \tau_n) = y \land \psi[y])$$

Since (4) is axiom of S, the theory then proves:

$$\psi[f(\tau_1, \ldots, \tau_n)] \leftrightarrow \exists y (\phi[\tau_1, \ldots, \tau_n, y] \land \psi[y])$$

where the formula on the right has at least one application of f less then the formula on the right. Continuing in this way, we can eliminate all applications of f from the formula ψ whereby we obtain a translation $\psi^\star$, which is formula of T such that T proves $\psi \leftrightarrow \psi^\star$. That S is conservative over T follows from the highly non-trivially demonstrated fact that S proves ϕ iff T proves $\phi^\star$.

We can use the new function symbol f in induction formulas because they are theorems of S for the same reason as was the case with the explicit definition of predicates.

1.4.7 Introduction of integer division into PA. As an example of extension by contextually defined functions we show how to introduce the integer division function $x \div y$ into PA by contextual definition:

$$x \div y = q \leftrightarrow y > 0 \land \exists r(x = q{\cdot}y + r \land r < y) \lor y = 0 \land q = 0 \ .$$

This can be done because PA proves the existence condition:

$$\exists q(y > 0 \land \exists r(x = q{\cdot}y + r \land r < y) \lor y = 0 \land q = 0)$$

as directly following from $y > 0 \to \exists q \exists r(x = q{\cdot}y + r \land r < y)$. The uniqueness condition follows easily from the uniqueness of quotients and remainders:

$$q_1{\cdot}y + r_1 = q_2{\cdot}y + r_2 \land r_1 < y \land r_2 < y \to q_1 = q_2 \land r_1 = r_2 \ .$$

1.4.8 The case analysis function D. Another example of extension by contextually defined functions is the introduction into PA of the ternary *case discrimination function* D satisfying:

$$D(0, y, z) = z$$
$$D(x + 1, y, z) = y \ .$$

Computer scientists can visualize the function as

$$\textbf{if } x > 0 \textbf{ then } y \textbf{ else } z \ .$$

The case discrimination function is introduced into PA by the folowing contextual definition:

$$D(x, y, z) = v \leftrightarrow x > 0 \land v = y \lor x = 0 \land v = z$$

whose existence and uniqueness conditions obviously hold.

1.4.9 Characteristic functions of predicates. The *characteristic function* of an n-ary predicate P is the n-ary function f such that:

$$f(\vec{x}) = \begin{cases} 1 & \text{if } P(\vec{x}) \\ 0 & \text{otherwise.} \end{cases}$$

We obviously have

$$f(\vec{x}) > 1 \leftrightarrow P(\vec{x}) \ .$$

We usually designate the characteristic function of a predicate P by P_*.

1.4.10 Characteristic functions of = and <. The binary characteristic functions $=_*$ and $<_*$ of the identity and less than predicates can be introduced into PA by contextual definitions:

$$(x{=_*}y) = z \leftrightarrow x = y \land z = 1 \lor x \neq y \land z = 0$$
$$(x{<_*}y) = z \leftrightarrow x < y \land z = 1 \lor x \geq y \land z = 0$$

whose existence and uniqueness conditions hold trivially.

1.4.11 Extensions of PA by definitions. Let T be an extension of PA and S_1 an extension of T either by explicit definition of a predicate P or by contextual definition of a function f.

We say that a theory S whose language is the same as S_1 is an *extension by definition* of T if S and S_1 are *elementarily equivalent* i.e. if both theories prove exactly the same theorems.

The theory S is conservative over T, permits to translate away the introduced symbols, and proves all induction formulas containing the newly introduced symbol. An *extension by definitions* is a finite sequence of extensions with every sequence an extension by definition.

We will sketch out below how to formulate a few increasingly more powerful forms of extensions of PA in a sense of expressive power and comfort but which will still be extensions by definitions. Comfortable and easy to use forms of extensions of PA are needed in order to obtain the kind of programming style computer programmers are used to. The schema of extensions by clausal definitions is such a powerful and easy to use schema. Clausal definitions have yet another important property because they are flexible enough to control the computation of defined functions and predicates. We will discuss this in Sect. 1.6.

UNFINISHED If a function or a predicate is provably recursive in $I\Sigma_1$ then we will usually not mention this explicitly and just say that it is introduced into PA. For any other extension we mention either the definability of the formula and/or the strength of the theory.

Δ_1 deinable in $I\Sigma_1$ and is provably recursive there

UNFINISHED power of extensions by definitions, give characterization.

1.4.12 Extensions of PA by explicitly defined functions. UNFINISHED remainder mod

1.4.13 Extensions of PA by minimalization.

$$\vdash_{\mathrm{PAx}} f(\vec{x}) = \mu_y[\phi[\vec{x}, y]].$$

$$\phi[\vec{x}, f(\vec{x})] \land \forall y(y < x \to \neg\phi[\vec{x}, y]).$$

$$[\sqrt{x}] = \mu_y[x < (y+1)^2] \tag{1}$$

1.4.14 Partial Functions. UNFINISHED They are Δ_2-definable but can be computed on their domains.

1.4.15 Extensions of PA by primitive recursion.

1.4.16 Extensions of PA by course of values recursion with measure. Let T be the current extension of PA. We wish to extend T to a theory S by the addition of a new n-ary function symbol f such that S proves identity

$$f(\vec{x}) = \tau[f;\vec{x}]\ . \tag{1}$$

We have indicated in the term τ that it can have occurrences of at most the variables $\vec{x}$ and that it can apply the function symbol f. The term τ is thus in the language of S. We will see in **UNFINISHED** that such an extension is always possible when the term τ is *regular* meaning that there is a *measure* function $m(\vec{x})$ in which all recursive applications $f(\vec{\rho})$ in τ goes down, i.e. $m(\vec{\rho}) < m(\vec{x})$ holds.

The best we can do for terms τ which are either not regular or we do not now yet whether they are such is to satisfy the recursive identity with *guards*:

$$f(\vec{x}) = \tau[\dot{\lambda}\vec{y}.D((m(\vec{y}) <_* m(\vec{x})), f(\vec{y}), 0);\vec{x}]\ . \tag{2}$$

The *lambda* notation simply means that every recursive application $f(\vec{\rho})$ in τ is surrounded by a guard:

$$D((m(\vec{\rho}) <_* m(\vec{x})), f(\vec{\rho}), 0)$$

which guarantees that we go to recursion only if $m(\vec{\rho}) < m(\vec{x})$.

We will introduce the function f into PA by minimalization with the help of a predicate arithmetizing the computation of f into a *computation* tree. For the sake of simplicity we assume that f is unary and that the term τ is built up from the variable x and from the numerals $\underline{n}_m$ by pairing (τ_1, tau_2) and by applications of unary functions $g_1, \ldots, g_k$. The reader will note that this is actually no restriction because the functions g_i can be contractions and instead of defining an n-ary function f we define its contraction $\langle f\rangle$.

Computation trees are binary and they have triples $\langle \rho, a, v\rangle$ as labels in their non-leaf nodes. The node with such a label records the computation of a subterm ρ of τ with the value a assigned to the variable x and with v recording the value (denotation) of ρ in this assignment. The sons of the node record the necessary subcomputations.

The form of the term ρ determines the shape of the sons t_1 and t_2 as follows. If $\rho \equiv \rho_1, \rho_2$ then the computation tree looks as follows:

$$\begin{array}{ccc} & \langle(\rho_1,\rho_2), a, (v_1, v_2)\rangle & \\ \langle \rho_1, a, v_1\rangle & & \langle \rho_2, a, v_2\rangle \\ \cdots t_1 \cdots & & \cdots t_2 \cdots \end{array}$$

where the value v_1 of ρ_1 is computed in the left son and the value v_2 of ρ_2 is computed in the right son. The value of (ρ_1, ρ_2) is then the pair (v_1, v_2).

If $\rho \equiv x$ or $\rho \equiv \underline{n}_m$ then the respective computation trees are:

$$\langle x, a, a\rangle \qquad\qquad \langle \underline{n}_m, a, n\rangle$$

where there are no subcomputations because the values of x and $\underline{n}_m$ can be determined directly as a and n respectively.

If $\rho \equiv g_i(\rho_1)$ then the computation tree is

$$\begin{array}{c} \langle g_i(\rho_1), a, g_i(v)\rangle \\ \langle \rho_1, a, v\rangle \qquad\qquad \\ \cdots t \cdots \qquad\qquad \end{array}$$

where we record in the left son the computation of the argument ρ_1 into the value v and then the value of $g_i(\rho_1)$ is then $g_i(v)$. There is not need to record any computation in the right son.

Finally, if $\rho \equiv f(\rho_1)$ then there are two possible computation trees:

$$\begin{array}{cc} \multicolumn{2}{c}{\langle f(\rho_1), a, w\rangle} \\ \langle \rho_1, a, v\rangle & \langle \tau, v, w\rangle \\ \cdots t_1 \cdots & \cdots t_2 \cdots \end{array} \qquad\qquad \begin{array}{c} \langle f(\rho_1), a, 0\rangle \\ \langle \rho_1, a, v\rangle \qquad\qquad \\ \cdots t_1 \cdots \qquad\qquad \end{array}$$

In both cases the value v of the argument ρ_1 is computed in the left son. The two cases are determined by the outcome of the test $m(v) < m(a)$. If the measure decreases then the computation tree is shown above on the left. This is when the identity $f(x) = \tau[f; x]$ is used as the computation rule in the form $f(\underline{v}_m) \mapsto \tau[f; \underline{v}_m]$. The value w of the term *tau* is computed in the right son and the value of the recursive application $f(\underline{v}_m)$ is determined as w. If the outcome of the test is negative then the computation tree is shown above on the right where the value of $f(\underline{v}_m)$ is 0. The reader will note that the computation of $f(\rho)$ thus evaluates the guard.

It should be obvious that we can construct a computation tree for any subterm ρ of τ and any assignment a of the value of the variable x because the terms in the labels of the tree are always smaller except in the right sons of recursive applications but then the measure decreases and the initial measure $m(a)$ can decrease only finitely many times.

We arithmetize this computation with the help of an explicitly defined predicate $Ct(t)$ holding iff t codes a computation tree for a subterm ρ of τ. PA proves that we have

$$\exists v \exists t_1 \exists t_2\, Ct\, Nd((\ulcorner \tau \urcorner, x, v), t_1, t_2)$$

and that the value v and the subtrees t_1 and t_2 are unique. We can thus define f by minimalization:

$$f(x) = H\,\mu_t[Ct\,Nd((\ulcorner\tau\urcorner, x, H(t)), H\,T(t), T\,T(t))]\ .$$

UNFINISHED

1.4.17 Definition of predicates through their characteristic functions. UNFINISHED Example

Extensions of PA by Clausal Definitions

1.4.18 Introduction to clausal definitions with an example. Clausal definitions are probably best explained with a concrete example. Suppose that we wish to extend PA with a unary function $[\sqrt{z}]$ satisfying the following specification:

$$[\sqrt{z}]^2 \leq z < ([\sqrt{z}]+1)^2$$

which means that the function should compute the whole part of the square root. We have seen in 1.4.13(1) a definition by minimalization. This was a 'naive' program running in time $\mathcal{O}(z)$ by a brute force search which was exponentially slower than it should have been.

The following clausal definition introduces the same function in a computationally optimal form running in time $\mathcal{O}(\log(z))$:

$$\begin{array}{ll}
[\sqrt{0}] = 0 & \\
[\sqrt{z}] = 1 & \leftarrow z < 4 \land z > 0 \\
[\sqrt{4{\cdot}x+i}] = s\mathbf{0} & \leftarrow 4{\cdot}x+i \geq 4 \land i < 4 \land [\sqrt{x}] = s \land 4{\cdot}x+i < (s\mathbf{1})^2 \\
[\sqrt{4{\cdot}x+i}] = s\mathbf{1} & \leftarrow 4{\cdot}x+i \geq 4 \land i < 4 \land [\sqrt{x}] = s \land 4{\cdot}x+i \geq (s\mathbf{1})^2\ .
\end{array}$$

The clauses are just formulas in the language of PA even though their implications are customarily written in the converse form. The clauses should be completely self-explanatory and the reader should have no difficulties whatsoever to understand the properties of the defined function.

$$\begin{array}{l}
[\sqrt{z}] = y \leftrightarrow \mathbf{case} \\
\qquad z < 4 \rightarrow \mathbf{case} \\
\qquad\qquad z = 0 \rightarrow 0 = y \\
\qquad\qquad z > 0 \rightarrow 1 = y \\
\qquad z \geq 4 \rightarrow \mathbf{let} \\
\qquad\qquad z = 4{\cdot}x + i \land i < 4 \rightarrow_{x,i} \\
\qquad\qquad\ \mathbf{let} \\
\qquad\qquad\quad [\sqrt{x}] = s \rightarrow_s\ \mathbf{case} \\
\qquad\qquad\qquad\qquad 4{\cdot}x+i < (s\mathbf{1})^2 \rightarrow s\mathbf{0} = y \\
\qquad\qquad\qquad\qquad 4{\cdot}x+i \geq (s\mathbf{1})^2 \rightarrow s\mathbf{1} = y
\end{array}$$

Fig. 1.5. The definition of $[\sqrt{z}]$ with case formulas.

1.4.19 Generalized case formulas. The only problem with the clausal definition of the function $[\sqrt{z}]$ in Par. 1.4.18 is to recognize that the clauses constitute a definition at all. We will show that this is indeed the case, and that it is an extension of PA by definition. Toward that end we write the clauses in a form with *case* formulas given in Fig. 1.5 which resembles contextual definitions (albeit recursive). The reader should think of the case formulas as conjucts of their alternatives some of which have universally quantified *local* variables. For instance, he should visualize the following three alternative case formula:

$$
\begin{array}{l}
\textbf{case} \\
\quad \phi_1 \rightarrow \psi_1 \\
\quad \phi_2[x,y] \rightarrow_{x,y} \psi_2[x,y] \\
\quad \phi_3[x] \rightarrow_x \psi_3[x]
\end{array}
$$

as standing for the formula

$$(\phi_1 \rightarrow \psi_1) \wedge \forall x \forall y (\phi_2[x,y] \rightarrow \psi_2[x,y]) \wedge \forall x(\phi_3[x] \rightarrow \psi_3[x]) \ .$$

The assumptions in the alternatives of a case formula should be *complete*, pairwise *exclusive*, and the local variables should be uniquely determined. In the above three alternative case this means that we have:

$$
\begin{gathered}
\phi_1 \vee \exists x! \exists y!\, \phi_2[x,y] \vee \exists x!\, \phi_3[x] \\
\phi_2[x,y] \vee \phi_3[x] \rightarrow \neg\phi_1 \\
\phi_2[x,y] \rightarrow \neg\exists x \phi_3[x] \ .
\end{gathered}
$$

Under those conditions the above case formula is equivalent to the following disjunctive formula:

$$\phi_1 \wedge \psi_1 \vee \exists x \exists y (\phi_2[x,y] \wedge \psi_2[x,y]) \vee \exists x(\phi_3[x] \wedge \psi_3[x]) \ .$$

1.4.20 Let formulas. Some of the case formulas have only one alternative and their sole purpose is to introduce local variables; the reader should vizualize them as a generalization of *let* constructs as known from functional programming languages. For that reason we write **let** instead of **case** as, in for instance:

$$
\begin{array}{l}
\textbf{let} \\
\quad z = 4{\cdot}x + i \wedge i < 4 \rightarrow_{x,i} \phi[x,i]
\end{array}
$$

which splits the argument z by *pattern matching* into the unique values x and i satisfying the shown relation. The local variables x and i can be then referred to in the *body* $\phi[x,i]$ of the alternative.

1.4.21 Unfolding of the contextual definition of $[\sqrt{z}]$. The contextual definition from Fig. 1.5 is transformed to the four clauses for $[\sqrt{z}]$ by *unfolding*. Unfolding, in this case, means the splitting of the alternatives presentend in the disjunctive form where we rely on the fact that $\phi \leftarrow \psi_1 \vee \psi_2$ and

$$(\phi \leftarrow \psi_1) \land (\phi \leftarrow \psi_2)$$

are propositionally equivalent and that $\phi \leftarrow \exists \vec{x}\psi$ and $\forall \vec{x}(\phi \leftarrow \psi)$ are logically equivalent provided the variables $\vec{x}$ do not occur in ϕ. We then split the conjucted clauses, drop the outermost universal quantifiers, and use properties of identity. For instance, the first and the third clauses for $[\sqrt{z}]$ are in the following form just before the properties of identity are applied to them:

$$\begin{array}{l}
[\sqrt{z}] = y \leftarrow z < 4 \land z = 0 \land 0 = y \\
[\sqrt{z}] = y \leftarrow z \geq 4 \land z = 4{\cdot}x + i \land i < 4 \land \\
\quad [\sqrt{x}] = s \land 4{\cdot}x + i < (s\mathbf{1})^2 \land s\mathbf{0} = y \ .
\end{array}$$

1.4.22 Definition of $[\sqrt{z}]$ by generalized course of values definition with measure. We will now transform the contextual recursive formula for $[\sqrt{z}]$ in Fig. 1.5 into a *generalized* course of values definition with measure. The definition is given in Fig. 1.6 and contains *case* terms instead of case formulas. Both definitions are satisfied by the same function and so they are equivalent. Case terms are significantly less readable than the case formulas and require explanation given in Paragraphs 1.4.23 through 1.4.26. We will define the functions applied in the case terms in Fig. 1.6 in Par. 1.4.33.

$$\begin{array}{l}
[\sqrt{z}] = \mathbf{case} \\
\qquad \overline{sgn}(z <_* 4) = 0 \to \mathbf{case} \\
\qquad\qquad\qquad \overline{sgn}(z =_* 0) = 0 \to 0 \\
\qquad\qquad\qquad \overline{sgn}(z =_* 0) = 1 \to 1 \\
\qquad \overline{sgn}(z <_* 4) = 1 \to \mathbf{let} \\
\qquad\qquad\qquad 0, qr(z) = 0, x, i \to_{x,i} \\
\qquad\qquad\qquad\quad \mathbf{let} \\
\qquad\qquad\qquad\quad\quad 0, [\sqrt{x}] = 0, s \to_s \ \mathbf{case} \\
\qquad\qquad\qquad\qquad\qquad\qquad \overline{sgn}(4{\cdot}x + i <_* (s\mathbf{1})^2) = 0 \to s\mathbf{0} \\
\qquad\qquad\qquad\qquad\qquad\qquad \overline{sgn}(4{\cdot}x + i <_* (s\mathbf{1})^2) = 1 \to s\mathbf{1}
\end{array}$$

Fig. 1.6. The definition of $[\sqrt{z}]$ with case terms.

$$\begin{array}{l}
\mathbf{case} \\
\quad \tau = 0 \to \alpha_0 \\
\qquad \vdots \\
\quad \tau = \underline{m-1}_m \to \alpha_{m-1} \\
\quad \tau = \underline{m}_m, x_1, \ldots, x_{n_m} \to_{x_1,\ldots,x_{n_m}} \alpha_m[x_1, \ldots, x_{n_m}] \\
\qquad \vdots \\
\quad \tau = \underline{k-1}_m, x_1, \ldots, x_{n_{k-1}} \to_{x_1,\ldots,x_{n_{k-1}}} \alpha_{k-1}[x_1, \ldots, x_{n_{k-1}}]
\end{array}$$

Fig. 1.7. The general form of a case term.

1.4.23 Case terms. The general form of case terms is given in Fig. 1.7 where $0 \leq m < k$ and all $n_m, \dots n_{k-1}$ are positive numbers. For $m \leq j < k$ we abbreviate the local variables $x_1, \dots x_{n_j}$ to $\vec{x}_j$. The local variables $\vec{x}_j$ may occur in the terms $\alpha_1[\vec{x}_j]$ but not in the term τ. Although all local variables in $\vec{x}_j$ must be pairwise different, the sets $\vec{x}_{j_1}$ and $\vec{x}_{j_2}$ may share variables whenever $j_1 \neq j_2$. The terms τ and α_j may contain additional *non-local* variables.

Before the case term from Fig. 1.7 is admitted as legal it must satisfy the following *completeness* condition

$$\tau = 0 \vee \dots \vee \tau = \underline{m-1}_m \vee \exists \vec{x}_i\, \tau = \underline{m}_m, \vec{x}_m \vee \dots \vee \exists \vec{x}_{k-1}\, \tau = \underline{k-1}_m, \vec{x}_{k-1} \;. \tag{1}$$

We will need more general case terms guarded by a condition which is a formula of PA. The case term from Fig. 1.7 is legal under a *guard* ϕ if PA proves the completeness condition (1) under the assumption ϕ. Note that an *absolute* case term, i.e. a case term without guard, is guarded by any condition.

When the guard of a case term is satisfied then the *discriminator* term τ denotes a *(disjoint) union value determined by* m, k, n_m, $\dots$, n_{k-1}. The *tag* of the union value τ is the denotation of τ if $\tau < \underline{m}_m$ and the denotation of $H(\tau)$ if $\tau \geq \underline{m}_m$.

The reader will note that the alternatives in (1) are pairwise disjoint and, for instance, for $j_1 < m$ and $m \leq j_2 < k$ we have

$$\tau = \underline{j_2}_m, \vec{x}_{j_2} \rightarrow \tau \neq \underline{j_1}_m$$

bcause $j_1 < j_2 < j_2, \vec{x}_{j_2}$ holds.

The tag j of τ determines the meaning (denotation) of the case term as the meaning of the term α_j if $j < m$ and the meaning of $\alpha_j[\vec{x}_j]$ when $m \leq j < k$ with the assignments to the local variables $\vec{x}_j$ uniquely determined from the union value $\tau = \underline{j}_m, \vec{x}_j$. We abbreviate the case term from Fig. 1.7 to

$$\mathit{case}_{m,k}(\tau, \alpha_0, \dots, \alpha_m[\vec{x}_m], \dots) \;. \tag{2}$$

The generalized term (2) is *well-formed under a guard* ϕ if ϕ is a guard for the case term, for every $j < m$ the generalized term α_j is well-formed under the guard $\phi \wedge \tau = \underline{j}_m$, and for every $m \leq j < k$ the generalized term $\alpha_j[\vec{y}_j]$ is well-formed under the guard $\phi \wedge \tau = \underline{j}_m, \vec{y}_j$.

1.4.24 Let terms. *Let* terms are the case terms with $m = 0$ and $k = 1$, i.e. one alternative case terms with local variables. For instance

let
$0, [\sqrt{x}] = 0, s \rightarrow_s \alpha[s]$.

Note that the tag 0 is superfluous and it is included in order to maintain the uniform form of case terms. Also note that the sole purpose of let terms is to introduce local variables.

$$
\begin{array}{l}
\phi \rightarrow \alpha = y \leftrightarrow \textbf{case} \\
\qquad\qquad \phi_0 \rightarrow \alpha_0 = y \\
\qquad\qquad \vdots \\
\qquad\qquad \phi_{m-1} \rightarrow \alpha_{m-1} = y \\
\qquad\qquad \phi_m, x_1, \ldots, x_{n_m} \rightarrow_{x_1,\ldots,x_{n_m}} \alpha_m[x_1, \ldots, x_{n_m}] = y \\
\qquad\qquad \vdots \\
\qquad\qquad \phi_{k-1}, x_1, \ldots, x_{n_{k-1}} \rightarrow_{x_1,\ldots,x_{n_{k-1}}} \alpha_{k-1}[x_1, \ldots, x_{n_{k-1}}] = y
\end{array}
$$

Fig. 1.8. The correspondence between the case terms and formulas.

1.4.25 Annotation of case terms. The connection of case terms to case formulas is established by the *annotation* of a case term with *assumption* formulas. The assumption formulas for the case term in Fig. 1.7 guarded by ϕ are $\phi_0, \ldots, \phi_{m-1}, \phi_m[\vec{y}_m], \ldots, \phi_{k-1}[\vec{y}_{k-1}]$ with the condition that we have

$$\phi \rightarrow \tau = \underline{j}_m \leftrightarrow \phi_j \tag{1}$$

whenever $j < m$ and

$$\phi \rightarrow \tau = \underline{j}_m, \vec{y}_j \leftrightarrow \phi_j[\vec{y}_j] \tag{2}$$

whenever $m \le j < k$. The reader will note that this guarantees the completeness and pairwise exclusivity of the assumption formulas as well as the uniqueness of local variables. This annotated case term is abbreviated to

$$\mathit{case}_{m,k}(\tau, (\phi_0 \rightarrow \alpha_0), \ldots, (\phi \rightarrow_{\vec{y}_m} \alpha_m), \ldots)\ . \tag{3}$$

We can think of all case terms as being annotated because the unannotated term in Fig. 1.7 can be brought into the annotated form (3) by taking as its assumption formulas the corresponding identities on the left-hand-sides of (1) and (2). If we abbreviate the term (3) by α then the connection to the corresponding case formula is given in Fig. 1.8.

$$
\begin{array}{l}
D((\tau =_* \underline{0}_m), \alpha_0^\star, \\
\ \ldots \\
\quad D((\tau =_* \underline{m-1}_m), \alpha_{m-1}^\star, \\
\qquad D(H(\tau =_* \underline{m}_m), \alpha_m^\star[H\,T^1(\tau), \ldots, H\,T^{n_m-1}(\tau), T^{n_m}(\tau)], \\
\qquad\ \ldots \\
\qquad\quad D(H(\tau =_* \underline{k-2}_m), \alpha_{k-2}^\star[H\,T^1(\tau), \ldots, H\,T^{n_{k-2}-1}(\tau), T^{n_{k-2}}(\tau)], \\
\qquad\qquad\qquad \alpha_{k-1}^\star[H\,T^1(\tau), \ldots, H\,T^{n_{k-1}-1}(\tau), T^{n_{k-1}}(\tau)])\ldots))\ldots)
\end{array}
$$

Fig. 1.9. The term of PA which is the translation of the generalized term in Fig. 1.7.

1.4.26 The meaning of case terms. We have informally presented the intended meaning of case terms in Par. 1.4.23. Case terms may bind local variables and so they are instances of *variable binding operators*. Note that lambda terms $\lambda x.\tau$ are another well-known examples of such operators. Because of technical complications of variables bound in the terms we do not introduce the case terms formally into PA and treat them as concretely presented syntactic objects on the level of meta-theory. We use α, β, as syntactic variables to range over *generalized* terms which are built up from the object terms of the language of PA by the case term constructs.

To every generalized term α we associate as its *translation* an object term $\alpha^\star$ in such a way that the denotations of $\alpha^\star$ in the models of PA are the same as the intended denotations of the generalized terms. The translation is defined by recursion on the structure of generalized terms in such a way that the translation of the generalized term 1.4.23(2) (or 1.4.25(3)) is the object term given in Fig. 1.9.

1.4.27 Generalized course of values definition with measure. We call

$$f(\vec{x}) = \alpha[[f]^{\mu}_{\vec{x}}; \vec{x}] \tag{1}$$

a *generalized* course of values definition with measure μ if its translation $f(\vec{x}) = \alpha^*[[f]^{\mu}_{\vec{x}}; \vec{x}]$ is a definition of f by course of values with measure μ. The function f is said to be defined by the generalized definition.

We can drop the guards around recursive applications of formulas if we restrict the recursive applications in α to *regular* applications. The idea is that for every recursive application $f(\vec{\rho})$ occurring in α we have

$$\psi_1 \land \ldots \land \psi_k \to \mu[\vec{\rho}] < \mu[\vec{x}]$$

where $\psi_1, \ldots, \psi_k$ are the annotation formulas *governing* the recursive occurrence in α. This means that if present the generalized definition (1) in an equivalent contextual form with a case formula ϕ:

$$f(\vec{x}) = y \leftrightarrow \phi[f; \vec{x}]$$

then the governing formulas are read off from the assumptions on case formulas enclosing the recursive application. For instance, for the single recursive application $[\sqrt{x}]$ in the definition in Fig. 1.5 we have

$$z \geq 4 \land z = 4{\cdot}x + i \land i < 4 \to x < z$$

and so the measure of the definition is the argument z itself.

The generalized definitions (1) with regular recursive applications are called *regular* definitions. For regular generalized definitions we not only have the extensional property that

$$\alpha^\star[[f]^\mu_{\vec{x}};\vec{x}] = \alpha^\star[f;\vec{x}]$$

holds for all $\vec{x}$ but we also have a stronger intensional property that the recursive applications $f(\vec{\rho})$ can be *strictly* evaluated whenever their governing formulas hold. Strict evaluation (cf. **UNFINISHED**) means that the arguments $\vec{\rho}$ are evaluated to $\vec{\rho}_1$ before the rewrite rule $f(\vec{\rho}_1) \blacktriangleright \alpha[f;\vec{\rho}_1]$ is applied.

1.4.28 Extensions of PA by clausal definitions. Let us designate the current extension of PA by T. We now describe a *clausal* extension of T to S with a new function symbol f. The *clausal definition* of a function f is obtained by the unfolding of a regular generalized course of values definition with measure:

$$f(\vec{x}) = \alpha[f;\vec{x}] \tag{1}$$

with α a well-formed generalized term under the guard $\top$. The translated formula $\alpha^\star$ must be in the language of S and there must be an extension by definition of the theory T to S_1 with a contextual definition $f(\vec{x}) = y\phi[\vec{x},y]$ for some formula ϕ of the language of T. The formula ϕ is obtained from the course of values definition with measure $f(\vec{x}) = \alpha^\star[[f]^\mu_{\vec{x}};\vec{x}]$

We obtain the clauses for f by transforming the generalized definition (1) into an equivalent contextual form with generalized case formulas

$$f(\vec{x}) = y \leftrightarrow \psi[f;\vec{x}]$$

and then by reading off the clauses from it and by using the properties of identity to simplify the clauses. The clauses are then added as new axioms of S together with the single induction formula for $\phi[\vec{x};f(\vec{x})]$. The theory S is equivalent to the theory S_1 and so it proves all induction formulas containing the new function symbol f. Moreover, because S_1 is an extension of T by definition, so is S.

For instance, the clausal definition of the function $[\sqrt{z}]$ given in Par. 1.4.18 is obtained from the regular generalized definition in Fig. 1.6 which is transformed into a form with generalized case formulas in Fig. 1.5. The clauses for $[\sqrt{z}]$ are read off this definition and simplified as described in Par. 1.4.21.

UNFINISHED predicates

1.4.29 Defaults in clausal definitions. UNFINISHED DEFAULTS

1.4.30 $\mathcal{D}$-case terms. In this, and the next two paragraphs, we present three kinds of case terms which are *basic*.

The $\mathcal{D}$-case terms are absolute and come in two forms differing only in annotation:

$$case_{2,2}(\overline{sgn}(x),(x>0 \to \alpha_0),(x=0 \to \alpha_1)) \tag{1}$$
$$case_{2,2}(\overline{sgn}(P_*(\vec{\tau})),(P(\vec{\tau}) \to \alpha_0),(\neg P(\vec{\tau}) \to \alpha_1)) \ . \tag{2}$$

The unary function $\overline{sgn}$ has the following explicit definition:

$$\overline{sgn} = 1 \dot{-} x \ .$$

The reader will note that we have $\overline{sgn}(x+1) = 0$ and $\overline{sgn}(0) = 1$ and so PA proves

$$case_{2,2}(\overline{sgn}(0), \alpha_0, \alpha_1)^\star = case_{2,2}(1, \alpha_0, \alpha_1)^\star = \alpha_1^\star = D(0, \alpha_0^\star, \star_1)$$

and

$$case_{2,2}(\overline{sgn}(x+1), \alpha_0, \alpha_1)^\star = case_{2,2}(0, \alpha_0, \alpha_1)^\star = \alpha_0^\star = D(x+1, \alpha_0^\star, \alpha_1^\star) \ .$$

This means that $\mathcal{D}$-case terms are extensionally applications of the case discrimination (**if-then-else**) function D. However, there is a crucial intensional difference in the way the two are computed. Applications of the function D are computed strictly, i.e. arguments before the application D, while the $\mathcal{D}$-case terms, as all case terms, are computed non-strictly (see Par. 1.6.4).

For the first form of $\mathcal{D}$-case terms we have $\overline{sgn}(x) = 0 \leftrightarrow x > 0$ and $\overline{sgn}(x) = 1 \leftrightarrow x = 0$ and thus the conditions on the assumption formulas are satisfied. The second form of $\mathcal{D}$-case terms is extensionally just an instantiation of the first form with $P_*(\vec{\tau})$ where P_* is the characteristic function of the predicate P. The annotation with assumption formulas is legal because we have $\overline{sgn}\, P_*(\vec{\tau}) = 0 \leftrightarrow P(\vec{\tau})$ and $\overline{sgn}\, P_*(\vec{\tau}) = 1 \leftrightarrow \neg P(\vec{\tau})$.

1.4.31 Binary case terms. *Binary* case terms are absolute and have the annotated form

$$case_{0,2}(b(\tau), (\tau = z\mathbf{0} \rightarrow_z \alpha_0[z]), (\tau = z\mathbf{0} \rightarrow_z \alpha_1[z])) \tag{1}$$

where the unary function b is introduced into PA by a contextual definition:

$$\begin{aligned} b(x) = y \leftrightarrow\ & \exists z(x = z\mathbf{0} \wedge y = 0, z) \vee \\ & \exists z(x = z\mathbf{1} \wedge y = 1, z) \end{aligned}$$

whose existence and uniqueness conditions are easily seen provable.

The function $b(x)$ yields the union values $0, z$ or $1, z$ depending on the parity of the number x. The reader will note that the conditions on the assumption formulas which are $b(x) = 0, z \leftrightarrow x = z\mathbf{0}$ and $b(x) = 1, z \leftrightarrow x = z\mathbf{1}$ are satisfied.

1.4.32 Cartesian case terms. *Cartesian* case (let) terms have the annotated form

$$case_{0,1}(c(\tau), (\tau = v, w \rightarrow_{v,w} \alpha_0[v, w])) \tag{1}$$

where the unary function c is introduced into PA by a contextual definition:

$$c(x) = y \leftrightarrow x = 0 \wedge y = 0 \vee x > 0 \wedge y = 0, x \ .$$

The completeness condition (cf 1.4.23(1)) for cartesian case terms is

$$\exists v \exists w \, c(\tau) = 0, v, w$$

and it is implied by any guard at least as strong as $\tau > 0$. Under such guard the condition on the assumption formula is satisfied because we have $c(\tau) = 0, v, w \leftrightarrow \tau = v, w$.

1.4.33 Derived case terms. *Derived* case terms have all functions applied in their discriminator terms definable by generalized definitions with basic case terms.

For instance, the two let terms used in the generalized definition in Fig. 1.6 are derived terms. The second of them is a let term as used the functional programming languages. The general form of such terms is:

$$case_{0,1}((0, \tau), (\tau = x \rightarrow_x \alpha_0[x])) \ .$$

The first let term of Fig. 1.6 applies the function qr yielding the pair consisting of the quotient and remainder after the division of z by 4. The let term has the form:

$$case_{0,1}((0, qr(\tau)), (\tau = 4{\cdot}q + r \wedge r < 4 \rightarrow_{q,r} \alpha_0[q, r]))$$

with the condition on its assumption formula satisfied because we have:

$$0, qr(\tau) = 0, q, r \leftrightarrow \tau = 4{\cdot}q + r \wedge r < 4 \ .$$

This let term is derived because the function $qr(z)$ can be defined with two nested binary case terms:

$$\begin{array}{lll} qr(z) = \textbf{case} & & \\ \quad b(z) = 0, u \rightarrow_u & \textbf{case} & \\ & \quad b(u) = 0, q \rightarrow_q q, 0 & \\ & \quad b(u) = 1, q \rightarrow_q q, 2 & \\ \quad b(z) = 1, u \rightarrow_u & \textbf{case} & \\ & \quad b(u) = 0, q \rightarrow_q q, 1 & \\ & \quad b(u) = 1, q \rightarrow_q q, 3 \ . & \end{array}$$

The unfolded clausal definition of qr just before the identity optimizations is:

$$\begin{aligned} qr(z) &= q, 0 \leftarrow z = u\mathbf{0} \wedge u = q\mathbf{0} \\ qr(z) &= q, 2 \leftarrow z = u\mathbf{0} \wedge u = q\mathbf{1} \\ qr(z) &= q, 1 \leftarrow z = u\mathbf{1} \wedge u = q\mathbf{0} \\ qr(z) &= q, 3 \leftarrow z = u\mathbf{1} \wedge u = q\mathbf{1} \end{aligned}$$

which becomes after the identity optimizations:

$$
\begin{aligned}
&qr(q\mathbf{00}) = q, 0\\
&qr(q\mathbf{10}) = q, 2\\
&qr(q\mathbf{01}) = q, 1\\
&qr(o\mathbf{01}) = q, 3\ .
\end{aligned}
$$

1.4.34 Pair case terms. *Pair* case terms are another example of derived terms and they have the annotated form

$$case_{1,2}(p(\tau), (\tau = 0 \to \alpha_0), (\tau = v, w \to_{v,w} \alpha_1[v, w]))$$

where the unary function p is introduced into PA by an explicit clausal definition:

$$
\begin{aligned}
&p(0) = 0\\
&p(v, w) = 1, v, w\ .
\end{aligned}
$$

The function $p(x)$ yields the union values 0 or $1, v, w$. The conditions on the assumption formulas are satisfied because we have $p(x) = 0 \leftrightarrow x = 0$ and $p(x) = 1, v, w \leftrightarrow x = v, w$.

The clausal definition of p is unfolded from the generalized definition with basic terms:

$$
\begin{aligned}
p(x) = \mathbf{case}&\\
&\overline{sgn}(x) = 0 \to \mathbf{let}\\
&\qquad\qquad c(x) = 0, v, w \to_{v,w} 1, v, w\\
&\overline{sgn}(x) = 1 \to 0\ .
\end{aligned}
$$

The reader will note that the let term in the definition is well-formed because its cartesian case term has its quard satisfied since we have $\overline{sgn}(x) = 0 \leftrightarrow x > 0$.

A pair case term is, for instance, used in the generalized definition

$$
\begin{aligned}
x \oplus y = \mathbf{case}&\\
&p(x) = 0 \to y\\
&p(x) = 1, v, w \to_{v,w} v, w \oplus y
\end{aligned}
$$

from which the clausal definition of the list concatenation function is unfolded:

$$
\begin{aligned}
&0 \oplus y\\
&(v, w) \oplus y = v, w \oplus y\ .
\end{aligned}
$$

1.4.35 A short discourse on the role of notation in mathematics and in computer programming. We have been always puzzled by the question why, in the age such dazzling computer generated graphics, the theoreticians of computer programming can live with an ancient typewriter style notation for their programs. A glance in most books on programming languages reveals programs like:

```
filter []                   = []
filter (y:ys) | p y         = y : filter ys
filter (y:ys) | otherwise = filter ys  .
```

whereas the same definition in our mathematical notation looks as follows:

$$
\begin{aligned}
&\mathit{filter}(0) = 0\\
&\mathit{filter}(v,w) = v, \mathit{filter}(w) \leftarrow P(v)\\
&\mathit{filter}(v,w) = \mathit{filter}(w) \quad \leftarrow \neg P(v)\ .
\end{aligned}
$$

The reader will note that the test $P(v)$ in our clauses unfolds from a $\mathcal{D}$-case term and so the repeated evaluation of $P(v)$ is avoided. The same must be achieved with an `otherwise` in the first program.

The typewriter style is even more puzzling to us because the readability of programs is one of the most basic dictums of a good programming language design. The situation is similar in the existing automated theorem provers, or rather intelligent proof checkers. We typically see in them formulas like:

```
forall x ( Sqrt(x)^2 <= x and x < ( Sqrt(x) + 1 )^2 )
```

although mathematicians, who in general do not put so much emphasis on the readability as computer scientists, would not dream of presenting the formula in a form different than:

$$\forall x([\sqrt{x}]^2 \leq x \wedge x < ([\sqrt{x}] + 1)^2)\ .$$

Part of the reason for this strange way of presentation lies in the traditionally understood role the syntax analysis should play in the design and presentation of computer programs. Language designers seem to insist on the 'what you see is what you get' approach to the writing of programs. This is because otherwise the parsing of programs would be difficult as e fancy mathematical notation cannot be easily parsed. True, but the same computer scientists use, apparently without any thoughts, a markup language (most often Latex) when writing their papers. They know that they have to enter their formulas in a slightly less readable marked up form and for the price of this minor inconvenience the formulas will be presented in an esthetically pleasing form.

The reader has certainly noticed that we consistently use mathematical notation for function and predicate applications, logical connectives, and quantifiers. CL, our current implementation of the clausal language, has somewhat limited Latex-like possibilities of presenting formulas as

$$\exists y(x \oplus y \prec [\sqrt{x}] \wedge x \neq y)\ .$$

In order to simplify the syntax analysis, the above (somewhat non-sensical) formula is typed in as

```
\e y ( Prec(App(x,y),Sqrt(x)) & x != y) .
```

The cultural gap between what is the standard in the supposedly ultra modern computer science and in the old fashioned mathematics is wide and it is still opening up. Referees of our papers which we submit to computer science conferences almost invariably chide us for the funny looking syntax of our programs without apparently realizing that we do not use anything special, just the language of Peano arithmetic.

The clauses of the present CL system are still syntactically analysed and so we cannot use fancy assumption formulas in our pattern matching presentation of arguments. We plan to change this dramatically with the prepared new version of CL. We plan to limit the syntax analysis to the parsing of simple terms and formulas. The case terms will be prompted in a top-down fashion. This, together with the enormous flexibility of extensible syntax of our case terms, will permit the use of arbitrary assumption formulas in the annotations of our case terms. The reader will note that the 'syntaxless' syntax of our clausal definitions, and the almost unlimited power of extensibility of case terms, will be possible only because the constraints on the case terms will have to be proved in the proof system before a new kind of a case term will be admitted.

The existing version of CL has a builtin set of pattern matching expressions by far surpassing the ones permitted in current functional languages such as Haskell. Patterns in Haskell are expressions (terms) whereas already the current version CL permits also pattern formulas such as $z = 4{\cdot}x + i \land i < 4$. The dramatic difference between the powers of expressibility of patterns as terms and patterns as formulas can be compared to the similarly dramatic difference between the power of explicit definitions $f(\vec{x}) = \tau$ in PA which are limited to applications in τ of previously introduced function symbols and the power of contextual definitions $f(\vec{x}) = y \leftrightarrow \phi$ where one has at disposal in the formula ϕ the full logical apparatus of propositional connectives and quantifiers.

We are convinced that the radical step of abandoning in the planned version of CL of the syntax analysis in favor of top-down prompting, together with the full extensibility of case terms, will unleash dramatically new ways of presentation of programs. The reader will note that this will happen fully within the language of Peano arithmetic without the addition of any reserved words or fancy syntax of current programming languages.

1.5 Limits of Provably Recursive Definitions in PA

1.5.1 Ordinal numbers less than ϵ_0. We wish to give a definition of a function V over $\mathbb{N}$ which is Δ_1-definable and so it is effectively computable (recursive) but not provably recursive in PA. The function V will grow so enormously fast that it will be practically uncomputable for all but the smallest arguments. The function will be defined with a measure into the initial segment of ordinal numbers less than the first *epsilon* number ϵ_0. This number satisfies the identity $\epsilon_0 = \omega^{\epsilon_0}$.

It is well-known that every ordinal number $\prec \epsilon_0$ can be uniquely denoted in the *Cantor's normal form* by a term

$$\omega_1^{\alpha} + \omega^{\alpha_2} \ldots + \omega^{\alpha_n} + 0 \tag{1}$$

where $n \geq 0$, $\alpha_1 \succeq \alpha_2 \succeq \ldots \succeq \alpha_n$, and the terms α_i are constructed similarly.

Let $\alpha \prec \epsilon_0$ be an ordinal whose Cantor's normal form is (1) and $\beta \prec \epsilon_0$ an ordinal whose Cantor's normal form is

$$\omega_1^{\beta} + \omega^{\beta_2} \ldots + \omega^{\beta_m} + 0 \ .$$

The *natural sum* $\alpha \sharp \beta$ of the two ordinals is the ordinal less than ϵ_0 whose Cantor's normal form is

$$\omega_1^{\gamma} + \omega^{\gamma_2} \ldots + \omega^{\gamma_{n+m}} + 0$$

where each γ_i is some α_j or β_j and all latter numbers are some γ_k. It should be clear that we have $\alpha \sharp \beta = \beta \sharp \alpha \succeq \alpha, \beta$.

It is not hard to see that every ordinal number less than ϵ_0 is denoted (but not uniquely) by a term built up from 0 by the binary operation $\alpha \sharp \omega^\beta$. We abbreviate $(\alpha \sharp \omega^\beta) \sharp \omega^\gamma$ to $\alpha \sharp \omega^\beta \sharp \omega^\gamma$. The advantage of this representation is that we do not have to order the exponents in non-increasing order and, for instance, the terms $\alpha \sharp \omega^\beta \sharp \omega^\gamma$ and $\alpha \sharp \omega^\gamma \sharp \omega^\beta$ denote the same ordinals.

1.5.2 Coding of ordinals $\prec\epsilon_0$ in $\mathbb{N}$. We encode the ordinals less than ϵ_0 into natural numbers by encoding the ordinal number 0 by $0 \in \mathbb{N}$ and the ordinal number $\alpha \sharp \omega^\beta$ by the natural number $a \oplus (b, 0)$ where a, b encode α and β respectively. It shuld be clear that every natural number is a code of an ordinal. Note that we have $a \oplus (b, c, 0) \neq a \oplus (c, b, 0)$ whenever $b \neq c$ but both numbers code the same ordinal.

The reader will note that we can have a more optimal 'reverse' encoding where $\alpha \sharp \omega^\beta$ is encoded by b, a but, since we will be dealing with practically non-computable functions, the efficiency of coding does not really matter.

We 'overload' the ordinal function $\alpha \sharp \omega^\beta$ and explicitly introduce it as a binary function over $\mathbb{N}$:

$$a \sharp \omega^b = a \oplus (b, 0) \ .$$

In order to distinguish the two functions we will use variables α, β, γ, ... to range over ordinals and the variables a, b, c, ... to range over the corresponding natural numbers coding ordinals.

The ternary function $a \sharp \omega^b \cdot n$ over $\mathbb{N}$ yielding the code of the ordinal

$$\alpha \sharp \overbrace{\beta \sharp \ldots \sharp \beta}^{n}$$

is introduced into PA by primitive recursion:

$a \sharp \omega^b \cdot 0 = a$
$a \sharp \omega^b \cdot (n{+}1) = a \sharp \omega^b \cdot n \sharp \omega^b$.

The binary function ω^i_k over $\mathbb{N}$ yielding the code of the ordinal designated by the same symbol is introduced into PA by primitive recursion:

$\omega^i_0 = 0 \sharp \omega^0 \cdot i$
$\omega^i_{k+1} = 0 \sharp \omega^{\omega^i_k}$.

We also overload the ordinal relation $\prec$ and use it as a binary relation $a \prec b$ over $\mathbb{N}$ holding of codes if $\alpha \prec \beta$ holds. The relation is provably recursive in $I\Sigma_1$, and although transitive and irreflexive, it is not an order because the law of trichotomy does not hold for it (this is because of the non-unique coding of ordinals). We will need a special case of $\prec$ as a ternary relation $a \prec \omega^i_k$ which is introduced into PA by course of values recursion in a:

$0 \prec \omega^i_k \leftarrow k > 0 \lor i > 0$
$a \sharp \omega^0 \prec \omega^{i+1}_0 \leftarrow a \prec \omega^i_0$
$a \sharp \omega^b \prec \omega^i_{k+1} \leftarrow a \prec \omega^i_{k+1} \land b \prec \omega^i_k$.

1.5.3 Arithmetization of fundamental sequences for limit ordinals. We call the code a of an ordinal less than ϵ_0 a *right successor* code if $a = b \sharp \omega^0$ for some b. A non-zero code a which is not a right successor is a *right limit* code. The code a is a right limit iff $a = b \oplus (c, 0) = b \sharp \omega^c$ for some b and $c > 0$.

We arithmetize the *fundamental sequences* $(\alpha)[n]$ for limit ordinals α (see [18]) by primitive recursion:

$(a \sharp \omega^{b \sharp \omega^0})[n] = a \sharp \omega^b \cdot (n{+}1)$
$(a \sharp \omega^{b \sharp \omega^c})[n] = a \sharp \omega^{(b \sharp \omega^c)[n]} \leftarrow c \neq 0$.

$I\Sigma_1$ proves
$$a \neq 0 \to (a)[n] \prec a \ .$$

1.5.4 A function growing faster than functions provably recursive in PA. Consider the following clauses for the unary function symbol V:

$V(0 \sharp \omega^0 \cdot n) = 0 \sharp \omega^0 \cdot n$
$V(a \sharp \omega^{b \sharp \omega^0} \sharp \omega^0 \cdot n) = V((a \sharp \omega^{b \sharp \omega^0})[n] \sharp \omega^0)$
$V(a \sharp \omega^{b \sharp \omega^c} \sharp \omega^0 \cdot n) = V((a \sharp \omega^{b \sharp \omega^c})[n] \sharp \omega^0 \cdot n) \leftarrow c \neq 0$.

The clauses for V are well-discriminated because every number c can be uniquely written as $c = d \oplus e$ where $\forall x(x \,\varepsilon\, e \to x = 0)$ and
$$d = 0 \lor \exists a \exists b \exists c\, d = a \oplus (b \oplus (c, 0), 0) \ .$$
Note that then e codes a finite ordinal, i.e. $e = 0 \sharp \omega^0 \cdot n$ for $n = L(e)$, and d is either 0 or it codes a transfinite ordinal $d = a \sharp \omega^{b \sharp \omega^c}$. Thus the first clause,

where $d = 0$, is discriminated from the remaining two where $d \neq 0$. The last two clauses are discriminated on whether $d = b \sharp \omega^c$ is a right successor ($c = 0$) or a right limit ($c \neq 0$). We have

$$a \sharp \omega^{b \sharp \omega^c} \sharp \omega^0 \cdot n \succ (a \sharp \omega^{b \sharp \omega^c})[n] \sharp \omega^0 \cdot \max(1, n)$$

and so the recursive argument in the last two clauses decreases in the relation $\prec$. This relation is not an order over $\mathbb{N}$ so it cannot be a well-order. However, the relation is well-founded and so the recursion has to stop after finitely many steps.

The problem is that PA is not strong enough to prove (in the form of a schema of well-founded induction on $\prec$) that the relation $\prec$ is well-founded. This means that the function V, although Δ_1-definable, i.e. recursive, is not provably recursive and so it cannot be introduced into PA by extensions by definitions.

On the other hand, for every $m > 0$, $k > 0$ and any i the fragment $I\Sigma_{m+k-1}$ proves that the restriction of $\prec$ to codes $\prec w^i_k$, i.e. the explicitly defined relation

$$a \prec_{k,i} b \leftrightarrow a \prec b \land b \prec w^{\underline{i}_m}_{\underline{k}_m} \ ,$$

is well-founded. This means that $I\Sigma_k$ proves a schema of well-founded induction on $\prec_{k,i}$ for Σ_m-formulas.

1.5.5 Extended Ackermann-Péter function. We have chosen the above form of definition of the function V for two reasons. The first one is that the function has a close connection to an extension into transfinite codes of the well-known Ackermann-Péter function from which we can define the so called fast growing hierarchy of functions. The second reason is a close connection to the intensional primitive recursive functionals (see **UNFINISHED**).

We define a binary function A over $\mathbb{N}$ by explicit definition:

$$A(a, n) = L\,V(0 \sharp \omega^a \sharp \omega^0 \cdot n) \ .$$

The definition must be done in the standard model of PA because the function A cannot be introduced into PA. The clauses for V imply (in the model) the following recurrences for the function A:

$$\begin{aligned} A(0, n) &= n + 1 \\ A(a \sharp \omega^0, 0) &= A(a, 1) \\ A(a \sharp \omega^0, n + 1) &= A(a, A(a \sharp \omega^0, n)) \\ A(a \sharp \omega^b, n) &= A((a \sharp \omega^b)[n], n) \leftarrow b \neq 0 \ . \end{aligned}$$

The binary Ackermann-Péter function which grows faster than all primitive recursive functions and satisfies:

$$Ack(0,n) = n+1 \tag{1}$$
$$Ack(m+1,0) = Ack(m,1) \tag{2}$$
$$Ack(m+1,n+1) = Ack(m, Ack(m+1,n)) \tag{3}$$

can be now explicitly defined as $Ack(m,n) = A(0 \sharp \omega^0 \cdot m, n)$. The reader will note that we have $0 \sharp \omega^0 \cdot m \prec \omega_1^1$ and so the codes of ordinals used in the computation of Ack do not even start to exploit the incredible rate of growth of the function A applied to the codes of larger ordinals.

1.5.6 Fast growing hierarchy. The extended Ackermann-Péter function can be also used to define a fast growing hierarchy of functions F_α similar to the ones studied by Wainer [25] and Schwichtenberg [19] (see also Rose [18]). To that end we assign to every ordinal $\alpha \prec \epsilon_0$ as its *canonical* code a the code obtained from the Cantor's normal form for α by replacing $+$ by natural sums $\sharp$. We then explicitly define:

$$F_\alpha(x) = A(a,x)$$

and obtain the following properties of functions F_α:

$$\begin{aligned} F_0(x) &= x+1 \\ F_{\alpha+1}(x) &= F_\alpha^{x+1}(1) \\ F_\alpha(x) &= F_{(\alpha)[x]}(x) \qquad \alpha \text{ is a limit ordinal.} \end{aligned}$$

We have chosen the hierarchy functions in such a way that for finite ordinals m we have $F_m(n) = Ack(m,n)$.

1.5.7 Provably recursive restrictions of V. It is well-known that the function F_{ϵ_0} satisfying:

$$\begin{aligned} F_{\epsilon_0}(x) = F_{(\epsilon_0)[x]}(x) = F_{\omega_x^1}(x) = A(\omega_x^1, x) = \\ L\,V(0 \sharp \omega^{\omega_x^1} \sharp \omega^0 \cdot x) = L\,V(\omega_{x+1}^1 \sharp \omega^0 \cdot x) \end{aligned}$$

is not provably recursive in PA. This is another reason why the function V cannot be provably recursive.

Let us now investigate restrictions of V which are provably recursive in PA. The unary function $V_e(a)$ is introduced into PA by explicit clausal definition:

$$\begin{aligned} & V_e(0 \sharp \omega^0 \cdot n) = 0 \sharp \omega^0 \cdot n \\ & V_e(a \sharp \omega^{b \sharp \omega^0} \sharp \omega^0 \cdot n) = a \sharp \omega^b \cdot (n+1) \sharp \omega^0 \\ & V_e(a \sharp \omega^{b \sharp \omega^c} \sharp \omega^0 \cdot n) = a \sharp \omega^{(b \sharp \omega^c)[n]} \sharp \omega^0 \cdot n \leftarrow c \neq 0\ . \end{aligned}$$

and its binary iteration $V_e^n(p)$ is introduced by primitive recursion:

$$\begin{aligned} & V_e^0(p) = p \\ & V_e^{n+1}(p) = V_e\, V_e^n(p) \quad . \end{aligned}$$

The standard model of PA then satisfies:

$$\exists n \exists m\, V_e^n(a) = 0 \sharp \omega^0 \cdot m \tag{1}$$

which is the condition of regularity for an expansion of the standard model of PA by a function V defined by minimalization:

$$V(a) = T\, \mu_p[V_e^{H(p)}(a) = 0 \sharp \omega^0 \cdot T(p)] \tag{2}$$

The clauses for V are then provable in PA extended by the axiom (2). This means that Peano arithmetic is not strong enough to prove the existence condition (1) because otherwise V would be provably recursive.

On the other hand, for $k \geq 1$ and any i the fragment $I\Sigma_k$ proves

$$a \prec \omega_{\underline{k}_m}^{\underline{i}_m} \to \exists n \exists m\, V_e^n(a) = 0 \sharp \omega^0 \cdot m \tag{3}$$

and so the function $V_{k,i}$ satisfying

$$\begin{aligned}
&V_{k,i}(d) = 0 \sharp \omega^0 \cdot n \leftarrow d \prec \omega_{\underline{k}_m}^{\underline{i}_m} \wedge d = 0 \sharp \omega^0 \cdot n \\
&V_{k,i}(d) = V_{k,i}(a \sharp \omega^b \cdot (n{+}1) \sharp \omega^0) \leftarrow d \prec \omega_{\underline{k}_m}^{\underline{i}_m} \wedge d = a \sharp \omega^{b \sharp \omega^0} \sharp \omega^0 \cdot n \\
&V_{k,i}(d) = V_{k,i}(a \sharp \omega^{(b \sharp \omega^c)[n]} \sharp \omega^0 \cdot n) \leftarrow d \prec \omega_{\underline{k}_m}^{\underline{i}_m} \wedge d = a \sharp \omega^{b \sharp \omega^c} \sharp \omega^0 \cdot n \wedge c \neq 0
\end{aligned}$$

is provably recursive in $I\Sigma_k$ and the standard model of PA satisfies

$$a \prec \omega_{\underline{k}_m}^{\underline{i}_m} \to V_{k,i}(a) = V(a)\ .$$

For any $k \geq 1$ and any ordinal $\alpha \prec \omega_k^1$ with the canonical code a we have $\alpha \prec \omega_{k-1}^i$ for some $i > 0$ and so $\omega^\alpha \prec \omega_k^i$. Thus $0 \sharp \omega^a \sharp \omega^0 \cdot x \prec \omega_{\underline{k}_m}^{\underline{i}_m}$ and, since

$$F_\alpha(x) = A(a, x) = L\, V(0 \sharp \omega^a \sharp \omega^0 \cdot x) = L\, V_{k,i}(0 \sharp \omega^a \sharp \omega^0 \cdot x)\ ,$$

the function F_α is provably recursive in $I\Sigma_k$. Hence all functions F_α where $\alpha \prec \epsilon_0$ are provably recursive in PA.

1.6 Intensional Issues of Computability

UNFINISHED Intensional issues have to do with the form of terms and definitions rather than with the functions and predicates defined.

UNFINISHED annotation on case terms plays no role.

Computation Over Mixed Numerals

We have introduced the clausal definitions with the help of generalized terms in such a way that to every clausal definition there is a regular generalized course of values definition with measure. We will now show how to use the latter for effective computation.

1.6.1 Mixed numerals. We will compute over the class of *mixed numerals* which are the least set of terms containing the constant 0, with every terms ρ_1, ρ_2 also the terms $\rho_1\mathbf{1}$ and (ρ_1, ρ_2), and with every term $\rho \not\equiv 0$ also the term $\rho\mathbf{0}$. Binary and pair numerals are thus proper subsets of mixed numerals.

In contrast to monadic, binary, or pair numerals, the mixed numerals do not enjoy the unique representation of natural numbers. For instance, the number three is denoted by four mixed numerals which are all different as terms:

$$0\mathbf{11} \quad (0,0)\mathbf{1} \quad (0\mathbf{1},0) \quad ((0,0),0)\ .$$

1.6.2 Mixed definitions of functions. We will compute functions defined by *mixed definitions* which are certain regular generalized course of values definitions with measure. The generalized definitions use $\mathcal{D}$, binary, cartesian, and case terms derived from these. The object terms in the definitions are built up from the constant 0 and variables by applications of binary successors, pairing, and of previously defined functions. Decimal numerals are abbreviations for the corresponding binary numerals and predicates are computed from the definitions of their characteristic functions.

We distinguish two classes of mixed definitions. Mixed definitions in the *narrow* sense, or *narrow* mixed definitions, are such that the measure terms in recursive generalized definitions apply only functions which are also definable by narrow mixed definitions. Unlimited mixed definitions allow functions in the measures to be introduced into PA by any extension by definition, say by a contextual definition.

The difference in the two classes is substantial. It is easy to see that the narrow mixed definitions define only primitive recursive functions while arbitrary mixed definitions define all provably recursive functions of PA, i.e. the $\prec\epsilon_0$-recursive functions.

1.6.3 Reductions. We will compute well-formed generalized terms α by *reductions*. The terms α will be *closed*, i.e. without free (non-local) variables. Reductions proceed by locating in α, which is not yet a mixed literal, the leftmost and innermost generalized term, called *redex*, and by rewriting the redex with a corresponding generalized term, called *contractum*. The rewriting is repeated until the generalized term being reduced becomes a mixed numeral.

UNFINISHED $\blacktriangleright$ notation **UNFINISHED** it is a good approximation of compilation for simplicity we substitute for local variables and arguments instead of using environments.

UNFINISHED termination

1.6.4 Redexes and their contracta. In the following we list all redex contracta pairs using the notation $\blacktriangleright$. We denote by α closed generalized terms, by τ closed object terms, and ρ the mixed numerals. The reader will note that for all redex contracta pairs $\alpha_1 \blacktriangleright \alpha_2$ the terms α_1 and α_2 denote the same natural number, i.e. we have $\alpha_1^\star = \alpha_2^\star$. The reduction

$$\rho\mathbf{00} \blacktriangleright \rho\mathbf{0}$$

removes one leading zero. Reductions

$$\begin{aligned}
\overline{sgn}(0) &\blacktriangleright 0\mathbf{1} \\
\overline{sgn}(\rho\mathbf{1}) &\blacktriangleright 0 \\
\overline{sgn}(\rho\mathbf{0}) &\blacktriangleright 0 \qquad \text{if } \rho \not\equiv 0 \\
\overline{sgn}(\rho_1, \rho_2) &\blacktriangleright 0
\end{aligned}$$

simplify the discriminators of $\mathcal{D}$-case terms. Reductions

$$\begin{aligned}
b(0) &\blacktriangleright 0, 0 \\
b(\rho\mathbf{0}) &\blacktriangleright 0, \rho \qquad \text{if } \rho \neq 0 \\
b(\rho\mathbf{1}) &\blacktriangleright 0\mathbf{0}, \rho \\
b(\rho_1, \rho_2) &\blacktriangleright 0, \rho \qquad \text{where } \rho\mathbf{0} = \rho_1, \rho_2 && (1) \\
b(\rho_1, \rho_2) &\blacktriangleright 0\mathbf{1}, \rho \qquad \text{where } \rho\mathbf{1} = \rho_1, \rho_2 && (2)
\end{aligned}$$

simplify the discriminators of binary case terms. Reductions

$$c(\rho) \blacktriangleright 0, \rho_1, \rho_2 \qquad \text{where } \rho = \rho_1, \rho_2 \tag{3}$$

simplify the discriminators of cartesian case terms. The reader will note that in any such then we must have $\rho \not\equiv 0$. The reduction

$$f(\vec{\rho}) \blacktriangleright \alpha[f, \vec{\rho}]$$

opens a mixed definition $f(\vec{x}) = \alpha[f; \vec{x}]$.

The final set of reductions involves case terms (both basic and derived)

$$case_{m,k}(\rho, \alpha_0, \ldots, \alpha_m[\vec{y}_m], \ldots) \blacktriangleright \alpha \tag{4}$$

where if $\rho = \underline{j}_b$ with $j < m$ then $\alpha \equiv \alpha_j$ and if $\rho = \underline{j}_b, \vec{\rho}_j$ then $\alpha \equiv \alpha_j[\vec{\rho}_j]$. The reader will note that the well-formedness restrictions on case terms guarantee that the term ρ denotes a union value determined by m, k, n_m, $\ldots$, n_{k-1}.

Reductions (1), (2) involve and reductions (3), (4) may involve conversions between representations of mixed numerals. The no conversion condition for the reduction (3) is $\rho \equiv \rho_1, \rho_2$ and for (4) the condition is $\rho \equiv \underline{j}_b$ with $j < m$ and $\rho \equiv \underline{j}_b, \vec{\rho}_j$ with $m \leq j < k$. Conversions are effectively computable but may be time consuming.

Data Types

Conversions in the marked reductions of Par. 1.6.4 are quite time consuming (although computable in linear space and polynomial time as shown in [24]) and we would like to avoid them. This can be done by means of syntactic restrictions on the form of mixed definitions by means of *typing*. Moreover, well-typed definitions of functions can be efficiently compiled into machine code (or C for that matter).

Types are intuitively certain sets of data values. Since our values are natural numbers, the types are certain subsets of $\mathbb{N}$, and hence can be defined by unary *type* predicates. With a proof system integrated with a programming language we can define arbitrary type predicates and provide proofs that our definitions of functions yield values of certain types when provided with arguments of some types. We, however, feel that the full power of the proof system should be reserved to the proofs of theorems about our functions rather than being used for typing. We think that the type predicates should form a rather weak class so the typing can be performed in a decidable manner. Moreover, as mentioned above, the typing should prevent needless conversion of representation of data values and should enable efficient compilation. For the last, the types should reflect the memory representation of data structures and it seems to us that the Pascal-style typing is a natural choice. Pascal-style type predicates can be then naturally extended to *polymorphic* type predicates in the style of ML.

There are two aspects to typing. The extensional aspect deals with the specification of the class of type predicates. The intensional aspect deals with a decidable typing calculus for deriving assertions about the types of terms, generalized terms, and definitions. Well-typed closed generalized terms then reduce without any conversion of mixed numerals. Well-typed definitions of functions and predicates with the polymorhic types instantiated, can be efficiently translated into machine code.

1.6.5 Pascal-style type predicates. Pascal-style type predicates can be defined by ordinary clausal definitions of predicates whose syntax is severely restricted. We will by convention choose the predicate symbols to be postfix operators whose applications are written as $x : T$ and read as (the value of) x is of type T. The reader should view the combination $: T$ as the symbol of a type predicate rather than to view $:$ as a binary infix operator taking a value and a type. In the folowing we will use S, T as meta-variables ranging over the symbols for types predicates.

The Pascal-style type predicates can be classified as *primitive*, *cartesian*, *list*, and *union* type predicates.

1.6.6 Primitive type predicates. The type of natural numbers is given by the predicate N with the following explicit clausal definition:

$x : N$.

The type N is the type of natural numbers. Values of type N can be represented in computer memory as the bignums of LISP, i.e. as numbers in the unlimited precision.

In a concrete implementation of CL we can choose more kinds of primitive type predicates. Unsigned and signed limited precision numbers represented in memory by, say, 32-bit words come to mind.

1.6.7 Cartesian type predicates. Suppose that $T_1, \ldots T_n$ have been introduced into PA as type predicates. The unary type predicate T explicitly defined by the clausal definition

$$x_1, \ldots, x_n : T \leftarrow x : T_1 \wedge \ldots \wedge x : T_n$$

is the type predicate of *cartesian product* of $T_1, \ldots, T_n$.

For instance, the predicate

$$x, y, z : N_3 \leftarrow x : N \wedge x : N \wedge x : N$$

is the type of triples of natural numbers. The reader will note that the same predicate has a simpler definition

$$x, y, z : N_3$$

which, however, does not have the prescribed syntactic form.

1.6.8 List type predicates. Suppose that T hat been introduced into PA as a type predicate. The predicate

$$0 : \mathit{List}(T)$$
$$x, y : \mathit{List}(T) \leftarrow x : T \wedge y : \mathit{List}(T) \; .$$

is the type predicate of *lists* with elements from S. The reader should read the combination $: \mathit{List}(T)$ as a 'structured' predicate symbol rather than as an operator taking types and yielding types.

Note that in the absence of polymorhism, the Pascal-style typing requires that, for instance, the predicates $\mathit{List}(N)$ and $\mathit{List}(N_3)$ should be introduced as two different predicates. The reader will also note that we have $\forall x\, x : \mathit{List}(N)$.

The memory representation of values of type $\mathit{List}(T)$ can, for intance, be a 32-bit pointer which is either *nil* for empty lists or a pointer to a cartesian pair $T \times \mathit{List}(T)$.

1.6.9 Union type predicates. *Union* type predicates hold of union values. Rather than discussing the general form of union types we illustrate them with an example. Consider the following clausal definition:

$$0 : \mathit{Bt}(T)$$
$$1, n, l, r : \mathit{Bt} \leftarrow n : T \wedge l : \mathit{Bt}(T) \wedge r : \mathit{Bt}(T)$$

where the type predicate T has been previously introduced into PA. A more familiar definition of the same predicate is with the help of two constructor functions $E = 0$ and $Nd(n,l,r) = 1,n,l,r$ as

$$E : Bt(T)$$
$$Nd(n,l,r) : Bt \leftarrow n : T \land l : Bt(T) \land r : Bt(T) \quad .$$

Values of type $Bt(T)$ are union values determined by 1, 2, and 3 (the arity of the value with the tag 1) where the values $1,n,l,r$ have the components appropriately typed.

Values of this type may be represented by pointers. The value E by *nil* and the values with the tag 1 by a pointer to a cartesian quadruple $N{\times}N{\times}Bt(T){\times}Bt(T)$ with the first component holding the tag 1.

The reader will note that we have

$$x : Bt(N) \rightarrow x : Bt(T)$$

for any union type predicate $Bt(T)$.

UNFINISHED general form of representation of union values

UNFINISHED union The type *Ch* is the type of extended ASCII characters and can be represented as bytes.

1.6.10 ML-style type predicates. *Polymorphic* typing in the style of the programming language ML corrects the greatest shortcoming of Pascal-style typing where the symbol T in the application $x : List(T)$ is a part of the predicate symbol rather than a second argument to the binary predicate $x : List(t)$ where the *type parameter* t ranges over all Pascal-style typing predicates. We cannot achieve this without going to the second-order calculus of arithmetic because in PA both arguments x and t must be natural numbers. Hence, the argument t does not range over type predicates but over the codes of type predicates. The polymorphic list predicate is then introduced into PA as a binary predicate by the following clausal definition:

$$0 : List(t)$$
$$x,y : List(t) \leftarrow x \mathbin{\boldsymbol{:}} t \land y : List(t)$$

which applies a binary *universal* typing predicate $x \mathbin{\boldsymbol{:}} t$. The reader will note the bold colon symbol signifying that this is a binary infix predicate rather than a part of the predicate symbol.

The universal predicate, which will be discussed in Par. 1.6.13, is such that PA proves

$$x \mathbin{\boldsymbol{:}} {'T}(t_1,\ldots,t_n) \leftrightarrow x : T(t_1,\ldots,t_n) \tag{1}$$

for every type predicate T with n type parameters, i.e. an $(n+1)$-ary type predicate $x : T(t_1,\ldots,t_n)$, introduced into PA. Here ${'T}(\tau_1,\ldots,\tau_n)$ is an abbreviation for a certain term of PA which denotes the code of $x : T(\tau_1,\ldots,\tau_n)$.

When T has no paramaters, i.e. when $x : T$ is a unary type predicate, then (1) should be read as

$$x \mathbin{\pmb{:}} {'T} \leftrightarrow x : T \ .$$

This style of polymorphism which permits type parameters in the form of variables ranging over (codes of) Pascal-style types but no new types is called *predicative polymorhism* (see, for instance, [15]).

With the polymorphic list type predicate one now takes arbitrary type predicate T and writes $x : \mathit{List}('T)$ instead of having to introduce the type predicate $: \mathit{List}(T)$ separately for each T.

We introduce a convention of writing the *type applications* $'T(\tau_1, \ldots, \tau_n)$ for $n \geq 0$ in an abbreviated form $T(\tau_1, \ldots, \tau_n)$. We can thus write $x : \mathit{List}(T)$ instead of $x : \mathit{List}('T)$. The reader will note that by (1) the last is equivalent to $x \mathbin{\pmb{:}} {'\mathit{List}}('T)$ which can be abbreviated to $x \mathbin{\pmb{:}} \mathit{List}(T)$.

Polymorphic type of binary trees is defined by the type predicate with one type parameter:

$$\begin{aligned} &E : \mathit{Bt}(t) \\ &\mathit{Nd}(n,l,r) : \mathit{Bt}(t) \leftarrow n \mathbin{\pmb{:}} t \land l : \mathit{Bt}(t) \land r : \mathit{Bt}(t) \quad . \end{aligned}$$

We can now, for instance, assert $x : \mathit{Bt}\,\mathit{List}(N_3)$ which is an abbreviation for $x : \mathit{Bt}('\mathit{List}('N_3))$ or equivalently $x \mathbin{\pmb{:}} \mathit{Bt}\,\mathit{List}(N_3)$ which is an abbreviation for $x \mathbin{\pmb{:}} {'\mathit{Bt}}('\mathit{List}('N_3))$.

1.6.11 Polymorphic vector type predicate. Vectors (arrays) are extensionally lists of given length. The importance of vectors lies in their intensional properties of having good memory representations. It would seem that we need two kinds of vector types. The ternary polymorphic type predicate $x : \mathit{Vect}_1(n,t)$ holding of *fixed* vectors is introduced into PA by primitive recursion:

$$\begin{aligned} &0 : \mathit{Vect}_1(0,t) \\ &v,w : \mathit{Vect}_1(n+1,t) \leftarrow v \mathbin{\pmb{:}} t \land w : \mathit{Vect}_1(n,t) \ . \end{aligned}$$

For every positive number n and every type predicate T the fixed vectors $x : \mathit{Vect}_1(\underline{n}_b, 'T)$ are represented in memory just like the Pascal arrays of type $\mathbf{array}[0..(n{-}1)]\,\mathbf{of}\,T$.

The binary polymorphic type predicate $x : \mathit{Vect}(t)$ holding of *flexible* vectors is introduced explicitly into PA by:

$$n,x : \mathit{Vect}(t) \leftarrow x : \mathit{Vect}_1(n,t) \ .$$

For every type predicate T the flexible vectors $x : \mathit{Vect}('T)$ are represented in computer memory as pointers to *dependent* cartesian pairs of type $N \times \mathit{Vect}_1(n,'T)$ where the value of the first component is n. The first component thus hold the length of the vector.

However, the practice of programming in our programming language Trilogy II, in which we have implemented the system CL, shows that fixed vectors are not used at all. For this reason we will work below with the flexible vectors only.

1.6.12 Operations on vectors. Although vectors are extensionally just lists it is of advantage to select some operations on them as basic ones and enforce by means of typing (see **UNFINISHED**) that the vectors are efficiently operated upon through these operations. These restrictions will guararantee an efficient compilation of vector operations into machine code.

There are three operations on vectors: creation of new vectors $New(n, v)$, indexing of vectors $a[i]$, and modification of vectors $a[i := v]$. The operations are introduced into PA with the help of auxiliary operations performing the same tasks with fixed vectors whose clausal definitions are:

$$
\begin{aligned}
&New_1(0, v) = 0\\
&New_1(n+1, v) = v, New_1(n, v)\\
&(v, a)[0]_1 = v\\
&(v, a)[i+1]_1 = a[i]_1\\
&(v, a)[0 := w]_1 = w, a\\
&(v, a)[i+1 := w]_1 = v, a[i := w]_1 \ .
\end{aligned}
$$

The operations for (flexible) vectors are then introduced into PA by explicit clausal definitions:

$$
\begin{aligned}
&New(n, v) = n, New_1(n+1, v)\\
&(n, a)[i] = a[i]_1 \leftarrow i < n\\
&(n, a)[i] = a[0]_1 \leftarrow i \geq n\\
&(n, a)[i := v] = n, a[i := v]_1 \leftarrow i < n\\
&(n, a)[i := v] = n, a \leftarrow i \geq n \ .
\end{aligned}
$$

The reader will note that in the application $Nev(n, v)$ the number n is not the length of the vector but rather its highest index. This means that the result is a vector with at least one component. This arrangment is important for the smooth typing of vector operations where the indexing operation yields an element of its argument vector (rather than the default 0 which is difficult to type properly) even if the index is out of bounds.

1.6.13 The universal typing predicate. By a detour through some auxiliary predicates we can introduce into PA a binary predicate $x \mathbin{\pmb{:}} c$ which acts as a universal typing predicate such that PA proves

$$x \mathbin{\pmb{:}} \boldsymbol{tappl}(\ulcorner T \urcorner, t_1, \ldots, t_n, 0) \leftrightarrow x : T(t_1, \ldots, t_n) \tag{1}$$

for every type predicate T with n type parameters introduced into PA. Here $\ulcorner T \urcorner$ is a mixed numeral denoting the code of T obtained by the arithmetization (see below) of the definition of T. The binary constructor function $\boldsymbol{tappl}$ codes the type application of T to its parameters. When T is without parameters then (1) should be read as

$$x \mathbin{\pmb{:}} \boldsymbol{tappl}(\ulcorner T \urcorner, 0) \leftrightarrow x : T \ .$$

The abbreviation $'T(\rho_1, \dots, \rho_n)$ discussed in Par. 1.6.10 stands for the term $\mathit{papply}(\ulcorner T \urcorner, \rho_1, \dots, \rho_n, 0)$.

The arithmetization of definitions of type predicates needs the following constructors which are explicitly introduced into PA as follows: $\boldsymbol{N} = 0$; $\boldsymbol{tappl}(c,p) = 1,p,s$; $\boldsymbol{vect}(t) = 2,t$; $t_1 \times t_2 = 3, t_1, t_2$; $t_1 \times^* t_2 = 4, t_1, t_2$; $\boldsymbol{Un}(m,s) = 5,m,s$; $\boldsymbol{par}(n) = 6,n$; and $\boldsymbol{rec}(x,c,p) = 7,x,c,p$.

PA proves the following properties of the universal typing predicate:

$$\begin{gathered}
x \mathbin{\pmb{:}} \boldsymbol{N} \\
x \mathbin{\pmb{:}} \boldsymbol{vect}(t) \leftrightarrow \exists n \exists a (x = n, a \land L(a) = n + 1 \land \forall i (i \le n \to (a)_i \mathbin{\pmb{:}} t)) \\
x \mathbin{\pmb{:}} t_1 \times t_2 \leftrightarrow \exists v \exists w (x = v, w \land v \mathbin{\pmb{:}} t_1 \land w \mathbin{\pmb{:}} t_2) \\
x \mathbin{\pmb{:}} t_1 \times^* t_2 \leftrightarrow x = 0 \lor x \mathbin{\pmb{:}} t_1 \times t_2 \\
x \mathbin{\pmb{:}} \boldsymbol{tappl}(c,p) \leftrightarrow x \mathbin{\pmb{:}} \mathit{sb}(c,x,c,p) \\
x \mathbin{\pmb{:}} \boldsymbol{rec}(y,c,p) \leftrightarrow |x|_p < |y|_p \land x \mathbin{\pmb{:}} \boldsymbol{tappl}(c,p) \\
x \mathbin{\pmb{:}} \boldsymbol{Un}(m,s) \leftrightarrow x < m \lor \exists i \exists y (i < L(s) \land x = m + i, y \land y \mathbin{\pmb{:}} (s)_i) \ .
\end{gathered}$$

The constant $\boldsymbol{N}$ denotes the code of the definition of the type predicate N (see Par. 1.6.6), i.e. $\ulcorner N \urcorner \equiv \boldsymbol{N}$, and so

$$'N \equiv \boldsymbol{tappl}(\ulcorner N \urcorner, 0) \equiv \boldsymbol{tappl}(\boldsymbol{N}, 0) \ .$$

The term $\boldsymbol{vect}\,\boldsymbol{par}(0)$ denotes the code of the definition of the one-parameter type predicate *Vect* (see Par. 1.6.11), i.e. $\ulcorner \mathit{Vect} \urcorner \equiv \boldsymbol{vect}\,\boldsymbol{par}(0)$, and so

$$'\mathit{Vect}(\rho) \equiv \boldsymbol{tappl}(\ulcorner \mathit{Vect} \urcorner, \rho, 0) \equiv \boldsymbol{tappl}(\boldsymbol{vect}\,\boldsymbol{par}(0), \rho, 0) \ .$$

For every t_1 and t_2 the term $t_1 \times t_2$ denotes the code of the cartesian product of t_1 and t_2. We abbreviate $t_1 \times (t_2 \times t_3)$ to $t_1 \times t_2 \times t_3$. Thus, for instance, the code $\ulcorner N_3 \urcorner$ of the type predicate N_3 (see Par. 1.6.7) is $'N \times 'N \times 'N$, and so

$$\begin{aligned}
'N_3 \equiv{} & \boldsymbol{tappl}(\ulcorner N_3 \urcorner, 0) \equiv \\
& \boldsymbol{tappl}(\boldsymbol{tappl}(\boldsymbol{N}, 0) \times \boldsymbol{tappl}(\boldsymbol{N}, 0) \times \boldsymbol{tappl}(\boldsymbol{N}, 0), 0) \ .
\end{aligned}$$

For every t_1 and t_2 the term $t_1 \times^* t_2$ codes the 'optional' cartesian product of t_1, t_2 which holds of 0 or of cartesian products $t_1 \times t_2$.

For instance, the code $\ulcorner \mathit{List} \urcorner$ of the polymorphic list type predicate $\mathit{List}(t)$ (see Par. 1.6.10) is as in the following:

$$'\mathit{List}(\rho) \equiv \boldsymbol{tappl}(\ulcorner \mathit{List} \urcorner, \rho, 0) \equiv \boldsymbol{tappl}(\boldsymbol{par}(0) \times^* \boldsymbol{rec}(0,0), \rho, 0) \ .$$

The constructor $\boldsymbol{par}$ codes the type parameters in the codes of type predicates with type parameters such that the i-th parameter is coded by

$\boldsymbol{par}(\underline{i-1}_b)$. The constructor $\boldsymbol{rec}$ codes recursive applications of type predicates in their definitions. The purpose of both constructors can be seen in the following:

$$
\begin{aligned}
&x : {}'List(t) \Leftrightarrow x : \boldsymbol{tappl}(\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),t,0) \Leftrightarrow \\
&\quad x : sb(\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),x,\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),t,0) \Leftrightarrow \\
&\quad x : t\times^{*}\boldsymbol{rec}(x,\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),t,0) \Leftrightarrow \\
&\quad x = 0 \lor x : t\times\boldsymbol{rec}(x,\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),t,0) \Leftrightarrow \\
&\quad x = 0 \lor \exists v \exists w(x = v,w \land v : t \land w : \boldsymbol{rec}(x,\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),t,0) \Leftrightarrow \\
&\quad x = 0 \lor \exists v \exists w(x = v,w \land v : t \land w : \boldsymbol{tappl}(\boldsymbol{par}(0)\times^{*}\boldsymbol{rec}(0,0,0),t,0)) \Leftrightarrow \\
&\quad x = 0 \lor \exists v \exists w(x = v,w \land v : t \land w : {}'List(t)) \Leftrightarrow \\
&\quad x = 0 \lor x : t\times{}'List(t) \Leftrightarrow x : t\times^{*}{}'List(t)\ .
\end{aligned}
$$

The four-place *substitution* function $sb(c,y,d,p)$ yields the code obtained from the code c by substituting in it for every occurrence of parameter $\boldsymbol{par}(i)$ the value $(p)_i$ and for every occurrence of $\boldsymbol{rec}(0,0,0)$ the value $\boldsymbol{rec}(y,d,p)$. Since we have

$$x : \boldsymbol{rec}(y,d,p) \leftrightarrow |x|_p < |y|_p \land x : \boldsymbol{tappl}(d,p)\ ,$$

we can see that after the substitution $\boldsymbol{rec}$ acts as a guarded type application $\boldsymbol{tappl}(d,p)$ which is invoked only if x is structurally simpler than y. This use of guards is similar to that in definitions by course of values recursion with measure and in both cases we enforce by it the termination of recursion. Clausal definitions of recursive type predicates must be regular in the first argument and so the guards are always satisfied for their codes.

The substitution $sb(c,y,d,p)$ is *shallow* in the sense that it does not enter the codes $\boldsymbol{tappl}(e,q)$ embedded in c. This means that we have no non-local parameters and recursion in the codes and as a consequence the predicate $x : c$ is primitive recursive.

The constructor $\boldsymbol{Un}$ codes union type predicates. The idea is that we have $x : \boldsymbol{Un}(m,\rho_m,\ldots,\rho_{k-1},0)$ iff x is a union value determined by m, k, n_m, $\ldots$, n_{k-1} (see Par. 1.4.23). Moreover, for every j s.t. $m \le j < k$ the number n_j is the 'arity' of the code ρ_j, i.e. the code has a form $\sigma_1\times\ldots\times\sigma_{n_j}$, and we have $x = \underline{j}_b, y_1, \ldots, y_{n_j}$ with $y_1 : \sigma_1$, $\ldots$, $y_{n_j} : \sigma_{n_j}$. The reader will note that the last is equivalent with $x = \underline{j}_b, y$ and $y : \rho_j$.

For instance, the code $\ulcorner Bt \urcorner$ of the polymorphic type predicate of labelled binary trees $Bt(t)$ (see Par. 1.6.10) is as in the following:

$$
\begin{aligned}
&{}'Bt(\rho) \equiv \boldsymbol{tappl}(\ulcorner Bt \urcorner,\rho,0) \equiv \\
&\qquad\qquad \boldsymbol{tappl}(\boldsymbol{Un}(\underline{1}_b,(\boldsymbol{par}(0)\times\boldsymbol{rec}(0,0,0)\times\boldsymbol{rec}(0,0,0)),0),\rho,0)\ .
\end{aligned}
$$

1.6.14 Type terms. We will present below a calculus for deriving assertions about well-typed generalized terms and definitions. For that we need a flexible language whose terms ρ denote codes of type predicates. The terms are called *type* terms and they are used in applications $x : \rho$. Type terms are constructed from variables (say t_1, t_2, ...) ranging over type codes (i.e. over $\mathbb{N}$) by constructors $\rho_1 \times \rho_2$, $\rho_1 \times^* \rho_2$,

$$\boldsymbol{Un}(\underline{m}_b, \rho_m, \ldots, \rho_{k-1}, 0) \ ,$$

and by type applications of the form $'T(\rho_1, \ldots, \rho_n)$ where T is a type predicate with n-parameters previously introduced into PA. The reader will recall that the last type application abbreviates the term $\boldsymbol{tappl}(\ulcorner T \urcorner, \rho_1, \ldots, \rho_n, 0)$.

For every type predicate T with n parameters ($n \geq 0$) introduced into PA except N and *Vect* we take its code $\ulcorner T \urcorner$, express it via constructors as a term of PA, shallowly replace in it every subterm $\boldsymbol{par}(\underline{i}_b)$ by the variable t_{i+1}, every subterm $\boldsymbol{rec}(0,0,0)$ by the type term $'T(t_1, \ldots, t_n)$ We obtain thereby a type term $\rho[t_1, \ldots, t_n]$ such that PA proves

$$x : {'T}(t_1, \ldots, t_n) \leftrightarrow x : \rho[t_1, \ldots, t_n] \tag{1}$$

For instance, for the type predicates mentioned in Par. 1.6.13 PA proves

$$\begin{aligned} x : N_3 &\leftrightarrow x : N \times N \times N \\ x : List(t) &\leftrightarrow x : t \times^* List(t) \\ x : Bt(t) &\leftrightarrow x : \boldsymbol{Un}(1, (t \times Bt(t) \times Bt(t)), 0) \end{aligned}$$

where we have consistently used the abbreviations for type applications (see Par. 1.6.10).

1.6.15 Typing calculus. We wish to type a mixed definition of the n-ary function symbol f in the polymorphic style of ML (see [10]) as

$$f :: \rho_1, \ldots, \rho_n \mapsto \rho \tag{1}$$

where ρ, ρ_1, ..., ρ_n are type terms. This extensionally means

$$x_1 : \rho_1 \wedge \ldots x_n : \rho_n \rightarrow f(x_1, \ldots, x_n) : \rho \ , \tag{2}$$

but intensionally the typing (1) is a much stronger assertion because it will be derived in a considerably weaker calculus, indeed a decidable one, than a formal proof system of the first-order theory PA.

Consider for instance, the explicit clausal definition:

$f(x) = 3, x$

for which PA trivially proves

$$x : N \rightarrow f(x) : N$$

but we will not be able to derive $f :: N \mapsto N$ in the type calculus.

The derivation of (1) in the weak type calculus will guarantee the computation by reduction without any conversions of applications $f(\tau_1, \ldots, \tau_n)$ for all mixed numerals τ_1, ..., τ_n for which the typing calculus derives $\tau_1 : \rho_1$, ..., $\tau_n : \rho_n$. A mixed numeral τ such that the typing calculus derives $\tau : \rho$ is called a *canonical* numeral of type ρ. Another advantage of the derivation of (1) in the typing calculus with closed type terms (without free type variables) is that the definition of f can be efficiently compiled into machine code or into the programming language C using the Pascal-like representation of its data types.

The typing calculus will be deriving either assertions of the form (1) or *type sequents* of the form

$$\Delta \Rightarrow \alpha : \rho \tag{3}$$

where α is a generalized term and ρ a type term. Δ is a sequence of finitely many (possibly empty) assumptions (guards). The assumptions are of the form $x : \rho$ or $f :: \rho_1, \ldots, \rho_n \mapsto \rho$. The order of assumptions in Δ is irrelevant and the reader can treat Δ as a finite set or, alternatively, he can enrich the type calculus by *structural* rules permitting interchange, duplication, and removal of duplications in the assumption sequence Δ. We say that the typing calculus derives $\alpha : \rho$ if it derives the sequent $\emptyset \Rightarrow \alpha : \rho$.

Derivations in the typing calculus are trees with roots of the form (1) or (3). The derivation trees are constructed in the usual way by means of *rules of inference* which are of the form $\dfrac{\phi_1 \ \ldots \ \phi_n}{\phi}$ where the *conclusion* ϕ is derived from the *premises* $\phi_1, \ldots \phi_n$. We do not exclude $n = 0$ and such rules are *axioms*.

The typing calculus is extensible in the sense that with every extension by definition of PA the typing calculus is extended with new rules of inference involving the newly introduced symbols.

We leave it to the reader to check that whenever the typing calculus derives the sequent $\Delta \Rightarrow \alpha : \rho$ then PA proves $\Delta^\star \to \alpha^* : \rho$ where $\Delta^\star$ stands for the conjunction of translated assumptions. Here an assumption $x : \rho$ is translated into itself and an assumption $f :: \rho_1, \ldots, \rho_n \mapsto \rho$ into

$$\forall x_1 \ldots \forall x_n (x_1 : \rho_1 \wedge \ldots x_n : \rho_n \to f(x_1, \ldots, x_n) : \rho) \ .$$

Similarly, when (1) is derived in the typing calculus then PA proves (2). These two facts prove the soundness of the typing calculus. The completeness of the calculus is not desirable because of its intensional benefits.

In the following paragraphs we present the inference rules of the typing calculus categorized into groups. **UNFINISHED** metavariables .... α, τ, ρ, σ

1.6.16 Inference rules using assumptions. Only two kinds of inference rules use assumptions (guards) in sequents. The first kind are axioms which type object variables and the second kind are rules with n premises typing applications of n-ary function symbols:

$$\frac{}{\Delta, x : \rho \Rightarrow x : \rho}$$

$$\frac{\Delta, f :: \rho_1, \ldots, \rho_n{\mapsto}\rho \Rightarrow \tau_1 \mathbin{\boldsymbol{:}} \rho_1 \quad \ldots \quad \Delta, f :: \rho_1, \ldots, \rho_n{\mapsto}\rho \Rightarrow \tau_n \mathbin{\boldsymbol{:}} \rho_n}{\Delta, f :: \rho_1, \ldots, \rho_n{\mapsto}\rho \Rightarrow f(\tau_1, \ldots, \tau_n) \mathbin{\boldsymbol{:}} \rho}$$

1.6.17 Axioms typing the constant 0**.** The constant 0 can be typed in three ways. This kind of multiple typing is often called *ad hoc polymorhism*. The first two kinds are given by the following axioms and the third kind is discussed in Par. 1.6.20:

$$\frac{}{\Delta \Rightarrow 0 \mathbin{\boldsymbol{:}} {'N}} \qquad \frac{}{\Delta \Rightarrow 0 \mathbin{\boldsymbol{:}} \rho_1 \times^* \rho_2}$$

1.6.18 Axioms typing the binary successor functions. The binary successor functions $\cdot\mathbf{0}$ and $\cdot\mathbf{1}$ have the following typing:

$$\frac{}{\cdot\mathbf{0} :: {'N}{\mapsto}{'N}} \qquad \frac{}{\cdot\mathbf{1} :: {'N}{\mapsto}{'N}}$$

The reader will note that this, the typing of 0 as $'N$, and the typing of function applications (see Par. 1.6.16) permits to derive the sequents $\Delta \Rightarrow \tau \mathbin{\boldsymbol{:}} {'N}$ where τ are binary numerals. The assumptions about the types of binary successor functions can be eliminated from Δ by the rules discussed in Par. 1.6.25. This enables the derivation of $\tau \mathbin{\boldsymbol{:}} {'N}$ for all binary numerals. As it happens, these are the only mixed numerals which can be typed as N. Compare this with a trivial proof of $\tau \mathbin{\boldsymbol{:}} {'N}$ in PA for arbitrary terms τ.

1.6.19 Inference rules typing applications of the pairing function. Pairs can be typed in three ways. The first two kinds type pairs as cartesian products:

$$\frac{\Delta \Rightarrow \tau_1 \mathbin{\boldsymbol{:}} \rho_1 \quad \Delta \Rightarrow \tau_2 \mathbin{\boldsymbol{:}} \rho_2}{\Delta \Rightarrow \tau_1, \tau_2 \mathbin{\boldsymbol{:}} \rho_1 \times \rho_2} \qquad \frac{\Delta \Rightarrow \tau_1, \tau_2 \mathbin{\boldsymbol{:}} \rho_1 \times \rho_2}{\Delta \Rightarrow \tau_1, \tau_2 \mathbin{\boldsymbol{:}} \rho_1 \times^* \rho_2}$$

and the third kind as union values (see Par. 1.6.20).

1.6.20 Inference rules typing union values. Union values are typed by two kinds of inference rules:

$$\frac{}{\Delta \Rightarrow \underline{j}_b \mathbin{\boldsymbol{:}} \boldsymbol{Un}(\underline{m}_b, \rho_m, \ldots, \rho_{k-1}, 0)} \quad \text{where } j < m$$

$$\frac{\Delta \Rightarrow \tau \mathbin{\boldsymbol{:}} \rho_j}{\Delta \Rightarrow \underline{j}_b, \tau \mathbin{\boldsymbol{:}} \boldsymbol{Un}(\underline{m}_b, \rho_m, \ldots, \rho_{k-1}, 0)} \quad \text{where } m \le j < k$$

The reader will note that the binary numerals $\underline{j}_b$ can be typed either as $'N$ (see Par. 1.6.18) or as union values of suitable union types. Binary numerals are included as tags also in union value pairs typed by the inference rules of the second kind. Pairs can be thus typed either as (optional) cartesian products or as union values.

1.6.21 Axioms typing operations on vectors. The three operations on vectors introduced in Par. 1.6.12 have the following polymorphic typing:

$$\frac{}{\mathit{New} :: {}'N, t \mapsto {}'\mathit{Vect}(t)} \qquad \frac{}{\cdot[\cdot] :: {}'\mathit{Vect}(t), {}'N \mapsto t}$$

$$\frac{}{\cdot[\cdot := \cdot] :: {}'\mathit{Vect}(t), {}'N, t \mapsto {}'\mathit{Vect}(t)}$$

These are the only inference rules for the typing of vectors. Thus every well-typed function definition with the vector type must be built up from the three operations and/or auxiliary functions applying the operations.

1.6.22 Axioms typing the discriminators of basic case terms. The discriminators of case terms (both basic and derived) yield union-values. For the typing of case terms we wish the union values to be typed by union types. This is achieved for the discriminators of the three basic case terms by the following typing axioms

$$\begin{array}{cc} \overline{sgn} :: {}'N \mapsto {}'\mathit{Bool} & \overline{sgn} :: {}'\mathit{Bool} \mapsto {}'\mathit{Bool} \\ b :: {}'N \mapsto \boldsymbol{Un}(0, {}'N, {}'N, 0) & c :: t_1 \times t_2 \mapsto \boldsymbol{Un}(0, (t_1 \times t_2), 0) \end{array}$$

where the union type predicate Bool is introduced into PA as follows:

$\mathit{Bool}(0)$
$\mathit{Bool}(1)$.

It should be clear that we have

$$x \mathbin{\boldsymbol{:}} {}'\mathit{Bool} \leftrightarrow x \mathbin{\boldsymbol{:}} \boldsymbol{Un}(\underline{2}_b, 0)$$

but the reader should not associate the value 0 with truth and 1 with falsehood because the characteristic functions of predicates yield 1 for truth and 0 for falsehood. The type Bool should be understood simply as holding of 0 or 1.

The function $\overline{sgn}$ is typed in two ways in a form of ad hoc polymorhism. The first typing is intended to be used with the first form 1.4.30(1) of $\mathcal{D}$-terms which test for zero. The second typing is intended for the second form 1.4.30(2) where the arguments of $\overline{sgn}$ are results of characteristic functions of predicates. The reader will recall that we treat the clausal definitions of characteristic functions of predicates as defining the predicates themselves and we wish the functions to be typed as $\ldots \mapsto {}'\mathit{Bool}$.

1.6.23 Inference rules typing case terms. The idea of typing of a case term

$$\mathit{case}_{m,k}(\tau, \alpha_0, \ldots, \alpha_{m-1}, \alpha_m[y_1, \ldots, y_{n_m}], \ldots, \alpha_{k-1}[y_1, \ldots, y_{n_{k-1}}])$$

under assumptions Δ by a type term ρ is to type its discriminator by a union type

$$\boldsymbol{Un}(\underline{m}_b, (\sigma_1^{(m)} \times \ldots \times \sigma_{n_m}^{(m)}), \ldots (\sigma_1^{(k-1)} \times \ldots \times \sigma_{n_{k-1}}^{(k-1)}), 0) \tag{1}$$

and all of its terms α_i by ρ. Note that the assumption formulas in case terms do not play any role. We can type only such guarded case terms whose guards are implied by the assumptions Δ. However, the implication is not to be proved in PA but rather in the typing caluclus with its limited means. The sole purpose of guards is to act as assumptions for the proof of the completeness condition 1.4.23(1). Note that the property is satisfied under assumptions Δ by the typing under the same assumptions of the discriminator term τ by the union type (1). These considerations lead to the following inference rule:

$$\frac{\begin{array}{l} \Delta \Rightarrow \tau : \boldsymbol{Un}(\underline{m}_b, (\sigma_1^{(m)} \times \ldots \times \sigma_{n_m}^{(m)}), \ldots (\sigma_1^{(k-1)} \times \ldots \times \sigma_{n_{k-1}}^{(k-1)}), 0) \\ \Delta \Rightarrow \alpha_0 : \rho \\ \quad\vdots \\ \Delta \Rightarrow \alpha_{m-1} : \rho \\ \Delta, y_1 : \sigma_1^{(m)}, \ldots, y_{n_m} : \sigma_{n_m}^{(m)} \Rightarrow \alpha_m : \rho \\ \quad\vdots \\ \Delta, y_1 : \sigma_1^{(k-1)}, \ldots, y_{n_{k-1}} : \sigma_{n_{k-1}}^{(k-1)} \Rightarrow \alpha_{k-1} : \rho \end{array}}{\Delta \Rightarrow \mathit{case}_{m,k}(\tau, \alpha_0, \ldots, \alpha_{m-1}, \alpha_m[y_1, \ldots, y_{n_m}], \ldots, \alpha_{k-1}[y_1, \ldots, y_{n_{k-1}}]) : \rho}$$

1.6.24 Inference rules introducing defined type predicates. Every type predicate T other than N or *Vect* can be presented by a typed term in the form 1.6.14(1). For such predicates we have the following typing rules:

$$\frac{\Delta \Rightarrow \alpha : \rho[\rho_1, \ldots, \rho_n]}{\Delta \Rightarrow \alpha : {'T}(\rho_1, \ldots, \rho_n)}$$

As an example of such rules we show in Fig. 1.10 the derivation of $0, 1, 0 : \mathit{List}(\mathit{Bool})$ where the reader will recall that 1 stands for the binary numeral $\underline{1}_b$.

1.6.25 Inference rules eliminating assumptions on function types. For the typing of function applications (see Par. 1.6.16) we need assumptions

$$
\frac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\emptyset \Rightarrow 0 : \boldsymbol{Un}(\underline{2}_b, 0)}}{0 : \mathit{Bool}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\emptyset \Rightarrow 1 : \boldsymbol{Un}(\underline{2}_b, 0)}}{\emptyset \Rightarrow 1 : \mathit{Bool}} \quad \dfrac{\dfrac{}{\emptyset \Rightarrow 0 : \mathit{Bool}\times^* \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 0 : \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 1, 0 : \mathit{Bool}\times \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 1, 0 : \mathit{Bool}\times^* \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 1, 0 : \mathit{Bool}\times \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 0, 1, 0 : \mathit{Bool}\times \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 0, 1, 0 : \mathit{Bool}\times^* \mathit{List}(\mathit{Bool})}}{\emptyset \Rightarrow 0, 1, 0 : \mathit{List}(\mathit{Bool})}
$$

Fig. 1.10. Example of a derivation in the typing calculus.

of the form 1.6.15(1). The assumptions can be eliminated by the followoing inference rules:

$$
\frac{\Delta, f :: \rho_1, \ldots, \rho_n \mapsto \rho \Rightarrow \alpha : \rho \qquad f :: \sigma_1, \ldots, \sigma_n \mapsto \sigma}{\Delta \Rightarrow \alpha : \rho}
$$

where the assumption $f :: \rho_1, \ldots, \rho_n \mapsto \rho$ is an instance of the polymorphic typing $f :: \sigma_1, \ldots, \sigma_n \mapsto \sigma$ in the second premise. The instance is obtained by a possible simultaneous substitution of suitable type terms for some (or all) type variables occurring in the type terms σ, σ_1, ..., σ_n.

1.6.26 Inference rules typing mixed definitions of functions. We can derive the typing of a form 1.6.15(1) for a mixed definition $f(x_1, \ldots, x_n) = \alpha[f; x_1, \ldots, x_n]$ with $n \geq 1$ by typing the body $\alpha[f; x_1, \ldots, x_n]$ under assumptions about the types of its free variables and about the type of f (this is needed for possible recursive applications). This is captured by the following inference rules:

$$
\frac{x_1 : \rho_1, \ldots, x_n : \rho_n, f :: \rho_1, \ldots, \rho_n \mapsto \rho \Rightarrow \alpha : \rho}{f :: \rho_1, \ldots, \rho_n \mapsto \rho}
$$

If f is a constant, i.e. a nullary function, and it has an explicit mixed definition $f = \alpha$ then we type it by the following inference rules

$$
\frac{\emptyset \Rightarrow \alpha : \rho}{f :: \rho} .
$$

1.6.27 Example of typing. UNFINISHED Reverse

1.6.28 Type inference. Type inference is the general problem of deriving a type assertion about an untyped or partially typed program. Clausal definitions are untyped. Even when a type definition is well-typed, i.e. typable, it can happen that it can be typed in an ad hoc polymorphism by more than one unrelated types. For instance

$f(x) = x, 0, 0$

can be typed as $f :: t \mapsto t \times N \times N$, $f :: t_1 \times^* t_2 \to List(t_1 \times^* t_2)$, or $f :: N \mapsto List(N)$. There are many more typings when one considers union types. It is probably the case that any typeable definition can be typed by a finite number of *principal*, i.e. most general typings, such that any typing is an instance of one of the typings.

What is important is that for any sequent $\Delta \Rightarrow \alpha : \rho$ we can decide the formula

$$\exists \vec{t}(\Delta^\star \to \alpha^\star : \rho)$$

by finding the type witnesses for $\vec{t}$. This is done by adaptation of the unification algorithm for polymorphic typing of Milner [14]. We can thus decide whether function definitions are well-typed.

1.6.29 Computation of well-typed mixed definitions. All closed generalized terms used in mixed definitions reduce to mixed numerals. We claim that the well-typed ones reduce without taking the reductions marked in Par. 1.6.4. We note first of all, that all reductions preserve the types and so all terms in a chain of reductions are well-typed.

Reductions 1.6.4(1) or (2) are taken when the discriminator of a binary case term is $b(\rho_1, \rho_2)$ with ρ_1 and ρ_2 mixed numerals. Since the case term is well-typed, we have $b :: N \mapsto \boldsymbol{Un}(0, N, N, 0)$, the argument of b must be typed as N. However, all mixed numerals of type N are binary numerals and so the situation cannot happen.

Reductions 1.6.4(3) are taken when reducing the discriminator of a cartesian case term $c(\rho)$ with ρ a mixed numeral. Since the only typing for c is $c :: t_1 \times t_2 \mapsto \boldsymbol{Un}(0, (t_1 \times t_2), 0)$, we must have $\rho : t_1 \times t_2$ for some t_1 and t_2. The only way this can happen is when $\rho \equiv \rho_1, \rho_2$. But then there is no conversion.

Reductions 1.6.4(4) are taken when the mixed term discriminator ρ of a case term denotes a union value. Since the case term is well-typed, ρ must be of an union type 1.6.23(1). But the mixed numerals of this type are of the form either $\underline{j}_b$ or $\underline{j}_b, \vec{\rho}_j$ and so the reduction takes place without conversion.

If a mixed definition of f is typed as $f :: \sigma_1, \ldots, \sigma_n \mapsto \sigma$ then its application $f(\rho_1, \ldots, \rho_n)$ to mixed numerals s.t. $\rho_1 : \sigma_1$, $\ldots$, $\rho_1 : \sigma_1$ is typed as ρ and the application reduces to a mixed numeral without conversions.

1.6.30 Compilation of well-typed mixed definitions. If a mixed definition of a function f is non-polymorphically typed, i.e. typed as $f :: \sigma_1, \ldots, \sigma_n \mapsto \sigma$ without variables in the type terms σ, σ_1, $\ldots$, σ_n, then the types are Pascal-like. Since all applications of auxiliary functions needed by the definition of f must go through inference rules in Par. 1.6.25, also the types of the auxiliary functions are Pascal-like. There is no conversion in the computation of any well-typed application of f and so the definition of f and of its auxiliary functions can be compiled into machine code (or C) with the standard Pascal-like representation of all types used. True, the auxiliary functions can be polymorphically typed and applied with different instantiations but there is only a finite number of such. Thus the auxiliary functions can be compiled in multiple copies with different Pascal-like types. An objection that this is be memory consuming is not a serious one because the machine (or C) code is compact, memories of modern computers are large, and the additional storage is nothing compared with the storage needed by pictures, music, or video.

1.7 Intensional Functionals

It is often said that LISP is a programming language based on the lambda calculus of functionals, i.e. functions operating on functions. It seems to us quite surprising that this characterization was not seriously questioned before because the domain of LISP are S-expressions. and so there can be no *extensional* functionals in LISP. Functionals of LISP are only coded into S-expressions in the form of *intensional* functionals. This is done by a universal partial function *Apply*. Since S-expressions can be embedded into natural numbers by the pairing function, it suffices for us to analyze the situation in the domain $\mathbb{N}$.

We hasten to state here that although intensional functionals have been studied in logic, for instance by Tait [**?**], the author does not know of an analysis similar to ours done on such a large scale. We mean here that we analyze a real typing system, which is moreover a polymorphic one, and definitions of functions expressed in a real programming language such as the extensible language of clausal definitions. The analysis by Tait was of a simple type system whose types have been generated from N by $s \mapsto t$, and of a simple language of primitive recursive functionals of Gödel. Moreover, our proposal for the introduction of functionals into a programming language leads to a very useful extension of mixed definitions. The proposed language is very simple to understand and use.

1.7.1 Universal function. To every Σ_1-definition of a unary partial function f we can assign its code c. The reader will note that such an f does not have a Π_1-definition unless it is total, i.e. recursive. We can then find a Σ_1-definition (but not a Π_1) of a binary partial *universal* function $U(c,x)$. The universal function is such that $U(c,x) \simeq f(x)$ holds for all x. This should be read as that either both $U(c,x)$ and $f(x)$ are defined and the results are identical, or neither is defined.

The assignment of codes can be extended to n-ary partial Σ_1-definable functions f to which we assign the same codes c as to their unary contractions $\langle f \rangle$. We then have

$$f(x_1,\ldots,x_n) \simeq \langle f \rangle(x_1,\ldots,x_n) \simeq U(c,x_1,\ldots,x_n) \ .$$

The universal function U has a code because its contraction $\langle U\rangle$ is Σ_1-definable. Applications $U(c,x)$ are in the Computability theory usually written as $\{c\}(x)$. Functional programming languages would use the notation $c(x)$ or even $c\,x$. We will write $c{\bullet}x$ in order to make visible that the application operator is a binary function over $\mathbb{N}$. The operator associates to the left and we let $c{\bullet}x{\bullet}y$ to stand for $(c{\bullet}x){\bullet}y$.

We work in PA with total functions only and so we can introduce the universal function $\bullet$ into PA as the Δ_2-definable completion of the partial function. Any definition of a partial function f with an argument c passed in the body of f to the first argument of $\bullet$ can be viewed as an intensional functional where the argument c is the code of a function rather than a function directly. Intensional functionals are thus Δ_2-definable as completed partial functions.

We are interested in a characterization of **decidable** constraints on arguments under which the intensional functionals can be computed. Decidable constraints will allow us to turn the Δ_2-definition of $\bullet$ into a Δ_1-definition of its restriction $\bullet_1$.

One of the possibilities for the constraints on arguments is to use a syntactic scheme of stratification of arguments in order to prevent the self-application $c{\bullet}c$ of which we cannot decide in general whether its computation terminates or not.

1.7.2 Hereditarily recursive operations. The simplest stratification of arguments of functionals is by *function types* $s{\mapsto}t$ which are called in logic *finite* types. The ground type is N and when the types s and t have been defined then we can define the type $s{\mapsto}t$ by explicit definition:

$$c : s{\mapsto}t \leftrightarrow \forall x(x : s \rightarrow \exists y(c{\bullet}x \simeq y \land y : t)) \;.$$

The function type $s{\mapsto}t$ thus holds of all intensional functionals c which are defined and yield functionals of type t if applied to functionals of type s. Such functionals are known as *hereditarily recursive operations* [6, 23]. This is a perfectly feasible approach except that it does not integrate well-with our data types. The reason is that the function types are of increasing quantifier complexity. While the predicate $c : \mathbb{N}{\mapsto}\mathbb{N}$ can be defined by a Π_2-definition, the definition of $c : (\mathbb{N}{\mapsto}\mathbb{N}){\mapsto}\mathbb{N}{\mapsto}\mathbb{N}$ requires a Π_3-formula and the definition of

$$c : ((\mathbb{N}{\mapsto}\mathbb{N}){\mapsto}\mathbb{N}{\mapsto}\mathbb{N}){\mapsto}(\mathbb{N}{\mapsto}\mathbb{N}){\mapsto}\mathbb{N}{\mapsto}\mathbb{N}$$

a Π_4-formula etc. The increasing quantifier complexity of function types means that we cannot introduce into PA the predicate $x : t$ with t admitting besides data types also the function types.

In order to stay within PA we substantially weaken the function types where we intuitively let $c : s{\mapsto}t$ to hold iff c codes a mixed definition of a unary function f s.t. $f :: s{\mapsto}t$ is derivable in the typing calculus. This is discussed in more detail below.

1.7.3 Bland intensional functionals. We will investigate first a rather limited class of intensional functionals which we call *bland* as opposed to a substantially larger class of *curried* functionals which will be introduced in Par. 1.7.13.

The idea of bland functionals is simple enough. Suppose for a moment that we have managed to introduce into PA the application operator $\bullet$ and that we have suitably extended the definition of the universal typing predicate $x :: t$ (see Par. 1.6.13) to function types $t = s_1 {\mapsto} s_2$ by treating the symbol $\mapsto$ as a new constructor function: $s {\mapsto} t = 8, s, t$. PA will prove

$$x : s{\mapsto}t \wedge y : s \rightarrow x{\bullet}y : t \; . \tag{1}$$

In order to be able to derive this also in the typing calculus we extend it with the axiom:

$$\frac{}{\cdot{\bullet}\cdot :: (s{\mapsto}t), s{\mapsto}t} \; . \tag{2}$$

We also extend the **narrow** mixed definitions by allowing in them applications of the operator $\bullet$ and call them *bland* definitions. Suppose now that we have introduced into PA by a bland definition an n-ary function symbol f. Suppose further that the definition is well-typed and that we have derived in the (extended) typing calculus $f :: s_1, \ldots, s_n {\mapsto} t$. The function f will have assigned a code $'f$ such that PA will prove:

$$'f : s_1 \times \ldots \times s_n {\mapsto} t \tag{3}$$

$$x_1 : s_1 \wedge \ldots \wedge x_n : s_n \rightarrow {'f}{\bullet}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \; . \tag{4}$$

Whenever, the *index property* (4) holds we say that the function f has an *index* $'f$. We will see below that in the case of bland functionals the sufficient condition for f to have an index is that we have a well-typed bland definition of f.

The typing property (3) is derivable in PA but not in the typing calculus. For that we add to the typing calculus new axioms:

$$\frac{}{\Delta, f :: s_1, \ldots, s_n{\mapsto}t \Rightarrow {'f} : s_1 \times \ldots \times s_n{\mapsto}t} \; . \tag{5}$$

1.7.4 Computation of bland definitions. We compute bland functionals by adding to the mixed numerals as new irreducible terms also the codes $'f$ of bland functionals f with indices. We call this extended class the *bland* numerals. Note that unlike the mixed numerals, the class of bland numerals is defined relatively to the current extension of PA. The new reductions are

$$'f{\bullet}(\vec{\rho}) \blacktriangleright f(\vec{\rho}) \tag{1}$$

where $\vec{\rho}$ are bland numerals and $f(\vec{\rho})$ is well-typed.

It can be shown that the reductions of all well-typed terms terminate with bland terminals. Note that while terms typed by function types are obtained from the indices of bland functionals by the operator $\bullet$, the only irreducible numerals of function types are the codes $'f$ of functions with bland definitions.

1.7.5 Example: The bland functional ***Map*****.** The canonical example of use of functionals is in the functional programming the binary functional *Map* which can be defined by

$$Map(f,0) = 0$$
$$Map(f,v,w) = f\bullet v, Map(f,w) \ .$$

The function is polymorphically typable as

$$f :: s{\mapsto}t, List(s){\mapsto}List(t)$$

is function can be polymorphically typed as and so it has an index $'Map$ such that $'Map : (s{\mapsto}t){\times}List(s){\mapsto}List(t)$ and PA proves:

$$f : s{\mapsto}t \wedge x : List(s) \rightarrow {'Map}\bullet(f,x) = Map(f,x) \ . \tag{1}$$

UNFINISHED Example of use

1.7.6 Comment on the introduction of bland functionals. The reader will probably agree with us that the idea and use of (bland) intensional functionals is simple. The description of their computation is straightforward because it takes just one additional easy to understand type of reduction 1.7.4(1). This should be contrasted with the following outline of the hard work needed to introduce the function types and the application operator into PA and to prove the indexing properties 1.7.3(4). The hard work involves the arithmetization of both the typing calculus and of the computation process. The later is needed for the definition of the application operator $\bullet$. We stress here that the difficult introduction of $\bullet$ and its inefficient definition has to do only with the semantics of proving that the reduction 1.7.4(1) preserves meaning, i.e. that PA proves $'f\bullet(\vec{\rho}) = f(\vec{\rho})$. The simplicity and the efficiency of computation with bland functionals is not affected by this.

1.7.7 Arithmetization of generalized terms. We now arithmetize the generalized terms as used in bland definitions.
UNFINISHED

1.7.8 Arithmetization of the typing calculus. UNFINISHED

1.7.9 Type levels. An important measure of complexity of a recursive typed definition is its *type level* which counts the complexity of its function types. We introduce into PA the unary function $lev(t)$ yielding the type level of the (code of the) type t to satisfy the following:

$$
\begin{gathered}
lev(\boldsymbol{N}) = lev\,\boldsymbol{rec}(a,b,c) = lev\,\boldsymbol{par}(i) = 0 \\
lev\,\boldsymbol{vect}(t) = lev(t) \\
lev(s{\times}t) = lev(s{\times}^{*}t) = \max(lev(s), TL(t)) \\
lev(\boldsymbol{tapply}(c,p) = lev\,\boldsymbol{sb}(c,0,\boldsymbol{N},p) \\
lev(\boldsymbol{Un}(m,s) = \max_{t\varepsilon s} lev(t) \\
lev(s{\mapsto}t) = \max(lev(s)+1, lev(t)) \ .
\end{gathered}
$$

Type level of a value x s.t. $x : t$ is $lev(x)$. Note that the type level of a function definition with index $'f : s{\mapsto}t$ is thus $lev(s{\mapsto}t) > 0$. Values with type level 0 are therefore the data structures typed by types not containing any function types. We for instance, have $lev\ List\ Vect(N{\times}N) = 0$ and $lev\ List\ Vect(N{\times}(s{\mapsto}t)) = lev(s{\mapsto}t) > 0$. Functions over data structures with type level 0 are of type level 1 and functions taking such functions as arguments are at least of type level 2.

$$
\begin{array}{l}
Ct(\boldsymbol{x}_i, c, x, x[i], 0) \\
Ct(\boldsymbol{z}, c, x, 0) \\
Ct(\boldsymbol{S}_0(a), c, x, v\boldsymbol{0}, (a,c,x,v), 0) \\
Ct(\boldsymbol{S}_1(a), c, x, v\boldsymbol{1}, (a,c,x,v), 0) \\
Ct(\boldsymbol{P}(a,b), c, x, (v,w), (a,c,x,v), (a,c,x,v), 0) \\
Ct(\overline{\boldsymbol{sgn}}(a), c, x, 0, (a,c,x,v+1), 0) \\
Ct(\overline{\boldsymbol{sgn}}(a), c, x, 1, (a,c,x,0), 0) \\
Ct(\boldsymbol{b}(a), c, x, (0,v), (a,c,x,v\boldsymbol{0}), 0) \\
Ct(\boldsymbol{b}(a), c, x, (1,v), (a,c,x,v\boldsymbol{1}), 0) \\
Ct(\boldsymbol{c}(a), c, x, (0,v,w), (a,c,x,(v,w)), 0) \\
Ct(\boldsymbol{cs}(a,m,t), c, x, w, (a,c,x,v), ((t)_v, c, x, w), 0) \leftarrow v < m \\
Ct(\boldsymbol{cs}(a,m,t), c, x, w, (a,c,x,v), ((t)_j, c, (x,y), w), 0) \leftarrow v \geq m \wedge v = j, y \\
Ct(\boldsymbol{cd}(a,n,m,e), c, x, \boldsymbol{cd}(a,n,m,e), 0) \\
Ct(a\underline{\bullet}b, c, x, z, (a,c,x,v), (b,c,x,w), (d,v,w,z), 0) \leftarrow v = \boldsymbol{cd}(d,n,m,e) \\
Ct(\boldsymbol{rec}(a), c, x, w, (a,c,x,v), (d,m,v,y_1), (d,m,x,y_2), (b,c,v,w), 0) \leftarrow \\
\quad c = \boldsymbol{cd}(b,n,m,e) \wedge m = \boldsymbol{cd}(d,n_1,m_1,e_1) \wedge y_1 < y_2 \\
Ct(\boldsymbol{rec}(a), c, x, w, (a,c,x,v), (d,m,v,y_1), (d,m,x,y_2), (e,\boldsymbol{cd}(e,n,0,0),v,w), 0) \leftarrow \\
\quad c = \boldsymbol{cd}(b,n,m,e) \wedge m = \boldsymbol{cd}(d,n_1,m_1,e_1) \wedge y_1 \geq y_2 \ .
\end{array}
$$

Fig. 1.11. Computation trees for bland functionals

1.7.10 Definition of the application operator.

1.7.11 Ackerman. UNFINISHED

$$
\begin{array}{l}
F(f,0) = f(1) \\
F(f,m+1) = f{\bullet}F(f,m)
\end{array}
$$

typed as $F :: (N{\mapsto}N), N{\mapsto}N$ and so it has an index $'F$ typed as $'F : (N{\mapsto}N){\times}N{\mapsto}N$. We would like to define a function

$$A(0) = {}'S$$
$$A(n+1) = \lambda m.{}'F\bullet(A(n), m) \ .$$

Then $Ack(n, m) = A(n)\bullet m$.

1.7.12 Function types. Suppose that f is an n-ary function with a definition which can be typed as

$$t_1 \times \ldots \times t_n \mapsto s \tag{1}$$

and c is the code of this definition. Although f can be a Δ_2-definable function because it can apply directly or indirectly the universal function $\bullet$, it can be computed for arguments of correct types and we have in the standard model of PA:

$$x_1 : t_1 \wedge \ldots \wedge x_1 : t_n \rightarrow \{c\}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \ . \tag{2}$$

We say that the function f has an *index* c. We will designate the index c by ${}'f$. If (2) can be proved in a fragment T of PA, we say that f has a *T-provable* index. The index c of the function f can be now used as an intensional functional of type (1).

1.7.13 Curried intensional functionals. UNFINISHED For curried functionals:

$$Ct(a\underline{\bullet}b, c, x, v\underline{\bullet}w, (a, c, x, v), (b, c, x, w), 0) \leftarrow Red(1, v, w) = 0$$
$$Ct(a\underline{\bullet}b, c, x, z, (a, c, x, v), (b, c, x, w), (f, d, y, z), 0) \leftarrow$$
$$\quad Red(1, v, w) = d, y \wedge d = \boldsymbol{cd}(f, n, m, e)$$

$$Red(i, cd(a, n, m, e), y) = cd(a, n, m, e), y \leftarrow n = i$$
$$Red(i, cd(a, n, m, e), y) = 0 \leftarrow n > i$$
$$Red(i, a\underline{\bullet}b, y) = Red(i+1, a, b, y) \ .$$

UNFINISHED Computation trees, this is real language rather than for a minimal scheme.

UNFINISHED The idea is that n-ary functions are assigned function types $t_1 \times \ldots \times t_n \mapsto s$. If a function f is of the latter type then we have:

$$x_1 : t_1 \wedge \ldots x_n : t_n \rightarrow f(x_1, \ldots, x_n) : s$$

Note that this is to be the same as

$$x : t_1 \times \ldots \times t_n \rightarrow \langle f \rangle(x) : s \ .$$

The universal function U is assigned the polymorphic function type $(s \mapsto t) \times s \mapsto t$ and we would like to have

$$c : s \mapsto t \wedge x : t \rightarrow \{c\}(x) : t \ .$$

In order to stay within PA we substantially weaken the typing predicate and we let $c : t \mapsto s$ hold iff c codes a syntactically well-typed definition of a unary function f taking values of type t to values of type s.

1.7.14 Currying. Instead of letting the binary application symbol $\bullet$ to stand for the universal function U, as was the case in the scheme of intensional functionals discussed in Par. 1.7.12, we can assign the codes to typed definitions in a more refined way and obtain more powerful intensional functionals. If an n-ary function symbol f has a definition typed as

$$t_1 \times \ldots \times t_n \mapsto s$$

we can treat its code c as typed in the *curried* form:

$$c : t_1 \mapsto \ldots \mapsto t_n \mapsto s \ .$$

This is done by defining the application symbol $\bullet$ as

$$c \bullet x = \begin{cases} c_1 & c \text{ codes } f(y_1, y_2 \ldots, y_n) \simeq \tau[f; y_1, y_2 \ldots, y_n],\ n > 1, \text{ and} \\ & c_1 \text{ codes } g(y_2, \ldots, y_n) \simeq \tau[g; x, y_2, \ldots, y_n] \\ U(c, x) & \text{otherwise.} \end{cases}$$

The standard model of PA thus satisfies

$$x_1 : t_1 \land \ldots \land x_1 : t_n \rightarrow c \bullet x_1 \bullet \ldots \bullet x_n = f(x_1, \ldots, x_n)$$

and we call c the *(currried) index* of f.

In the next two paragraph we will show that curried intensional functionals are much more powerful than the ones from Par. 1.7.12 which we might call *bland* functionals.

1.7.15 Fast growing intensional functionals. UNFINISHED The ternary *iteration* intensional functional $I(n, a, b)$ of polymorphic type $\mathbb{N} \times (t \mapsto t) \times t \mapsto t$, which we abbreviate to $a^{(n)}(b)$, is defined by primitive recursion:

$$\begin{aligned} a^{(0)}(b) &= b \\ a^{(n+1)}(b) &= a \bullet (a^{(n)}(b)) \ . \end{aligned}$$

An infinite sequence of types T^k is defined as:

$$\begin{aligned} T^0 &= \mathbb{N} \\ T^{k+1} &= T^k \mapsto T^k \ . \end{aligned}$$

An infinite sequence of $(k+1)$-ary intensional functionals K_0^{k+1} of type

$$T^k \times T^{k-1} \times \ldots \times T^1 \times T^0 \mapsto T^0$$

is explicitly defined by:

$$
\begin{aligned}
K_0^1(n) &= n \\
K_0^2(a_1,n) &= a_1{\bullet}(n{+}1) \\
K_0^3(a_2,a_1,n) &= a_2^{(n+1)}(a_1){\bullet}1 \\
K_0^{k+4}(a_{k+3},a_{k+2},a_{k+1},\ldots,a_1,n) &= a_{k+3}^{(n+1)}(a_{k+2}){\bullet}a_{k+1}{\bullet}\ldots{\bullet}a_1{\bullet}n\ .
\end{aligned}
$$

The definitions are well-typed and the functionals have indices ${}'K_0^{k+1}$ such that

$$
a_k \mathbin{:} T^k \wedge \ldots a_1 \mathbin{:} T^1 \rightarrow {}'K_0^{k+1}{\bullet}a_k{\bullet}\ldots{\bullet}a_1{\bullet}n = K_0^{k+1}(a_k,\ldots,a_1,n)
$$

is satisfied in the standard model. Unfortunately, this can be proved in PA only for numerals:

$$
\underline{a_k}_m \mathbin{:} T^k \wedge \ldots \underline{a_1}_m \mathbin{:} T^1 \rightarrow {}'K_0^{k+1}{\bullet}\underline{a_k}_m{\bullet}\ldots{\bullet}\underline{a_1}_m{\bullet}\underline{n}_m = K_0^{k+1}(\underline{a_k}_m,\ldots,\underline{a_1}_m,\underline{n}_m)\ .
$$

We can define a binary meta-theoretical function $\underline{K}^{k+1}(a)$ yielding terms of PA such that:

$$
\begin{aligned}
\underline{K}^{k+1}(0) &\equiv {}'K_0^{k+1} \\
\underline{K}^{k+1}(a \sharp \omega^b) &\equiv \underline{K}^{k+2}(b){\bullet}\underline{K}^{k+1}(a)\ .
\end{aligned}
$$

The fast growing function V from Par. 1.5.4, although Δ_1-definable, can be introduced into PA only as a completed partial function by a Δ_2 definition and PA proves:

$$
V(\underline{a}_m) = 0 \sharp \omega^0 \cdot (\underline{K}^1(a){\bullet}0)\ . \tag{1}
$$

This follows by the meta-theoretical $\prec$-induction from the following theorems of PA:

$$
\begin{aligned}
\underline{K}^{k+1}(a \sharp \omega^b \cdot n) &= (\underline{K}^{k+2}(b))^{(n)}(\underline{K}^{k+1}(a)) \\
\underline{K}^1(a \sharp \omega^0 \cdot n){\bullet}m &= \underline{K}^1(a){\bullet}(m{+}n) \\
\underline{K}^{k+2}(a \sharp \omega^{b \sharp \omega^c}){\bullet}\underline{K}^{k+1}(a_{k+1}){\bullet}\ldots{\bullet}\underline{K}^1(a_1){\bullet}n &= \\
&\underline{K}^{k+2}((a \sharp \omega^{b \sharp \omega^c})[n]){\bullet}\underline{K}^{k+1}(a_{k+1}){\bullet}\ldots{\bullet}\underline{K}^1(a_1){\bullet}n\ .
\end{aligned}
$$

We can also introduce into PA a binary function $K^{k+1}(a)$ by course of values recursion in a:

$$
\begin{aligned}
&K^{k+1}(0) = {}'K_0^{k+1} \\
&K^{k+1}(a \sharp \omega^b) = K^{k+2}(b)\underline{\bullet}K^{k+1}(a)\quad .
\end{aligned}
$$

The function $K^{k+1}(a)$ yields the code of a functional of type T^{n+1} such that if $K^{k+2}(b)$ yields the code c and $K^{k+1}(a)$ the code d, the application $c\underline{\bullet}d$ yields the code of $c{\bullet}d$. The definition of $K^{k+1}(a)$ is not well-typed although PA proves

$$\underline{a_n}_m : T^k \to K^{k+1}(\underline{a}_m)\bullet\underline{a_n}_m = \underline{K}^{k+1}(a)\bullet\underline{a_n}_m \ .$$

From this and from (1) we can see that standard model of PA satisfies:

$$V(a) = 0 \sharp \omega^0 \cdot (K^1(a)\bullet 0)$$

but this is unprovable in PA because, otherwise we could introduce the function V into PA.

UNFINISHED codes of functionals are clausal definitions with measures and $\bullet$.

UNFINISHED what is U **UNFINISHED** well-typed codes.

We wish a programming comfort not the largest possible class of provably recursive functions. Primitive recursive functions are by far more that can be feasibly computed. Thus we wish indices but not for all functions.

We have seen in the previous paragraph that curried intensional functionals very soon reach the limits of provability in PA and so they cannot be worked comfortably with. The situation is actually even worse Map

Example:

Strengthening by V makes the typing possible, although provably recursive are much more but they do not have provable indices.

It is possible to strengthen PA, basically by asserting that well-typed definitions of functionals have indices but the question is whether it is worth it? Although the proponents of functional programming in the style of Haskell will not agree with us, we think that the full power of curried intensional functionals is not needed and the bland functionals introduced in Par. 1.7.12 are sufficient for the the needs of programming.

What does the currying gives us.

Similar argument for Ack as above for V.

What does the currying gives us. So this is a C-style programming

Characterization.

Ackermann is definable but does not have an index.

1.7.16 Infinite lists. UNFINISHED Functional languages as Haskell can operationally deal with infinite lists by the device of lazy evaluation. Infinite lists must be denotationally added to the domain of Haskell. Our schema of intensional functionals has significant advantage of semantic simplicity over functional languages and we can deal with infinite sequences (even with eager evaluation) in a mathematically clean way. Infinite sequences can be coded by indices p of their enumerating functions where $p \mapsto n$ denotes the n-th element of the sequence.

Infinite lists of natural numbers are thus of type $N \mapsto N$. We present the standard example of infinite lists where the primitive recursive function p_n yielding the n-th prime is defined by detour through three intensional functionals whose indices are typed as follows:

$$\begin{aligned} {}'\mathit{Tl} &: (\mathbb{N}\mapsto\mathbb{N})\mapsto\mathbb{N}\mapsto\mathbb{N} \\ {}'\mathit{Mults} &: \mathbb{N}\mapsto(\mathbb{N}\mapsto\mathbb{N})\mapsto\mathbb{N}\mapsto\mathbb{N} \\ {}'[2..] &: \mathbb{N}\mapsto\mathbb{N}\ . \end{aligned}$$

The binary function Sv is typed as $(\mathbb{N}\mapsto\mathbb{N})\times\mathbb{N}\mapsto\mathbb{N}$ and the unary function p_n as $\mathbb{N}\mapsto\mathbb{N}$. The functionals and functions are defined as:

$$\begin{aligned} & \mathit{Tl}(s,n) = s\bullet(n+1) \\ & \mathit{Mults}(k,s,n) = \mathit{Mults}(k,\mathit{Tl}(s),n) \leftarrow s\bullet 0 = h \wedge k \mid h \\ & \mathit{Mults}(k,s,0) = h \leftarrow s\bullet 0 = h \wedge k \nmid h \\ & \mathit{Mults}(k,s,n+1) = \mathit{Mults}(k,\mathit{Tl}(s),n) \leftarrow s\bullet 0 = h \wedge k \nmid h \\ & Sv(s,0) = h \leftarrow s\bullet 0 = h \\ & Sv(s,n+1) = Sv({}'\mathit{Mults}\bullet h\bullet(\mathit{Tl}\bullet s),n) \leftarrow s\bullet 0 = h \\ & [2..](n) = n+2 \\ & p_n = Sv({}'[2..],n)\ . \end{aligned}$$

$\mathit{Mults}(k,s)$ transforms an infinite list s into another infinite list by deleting all elements of s divisible by k. $Sv(s,n)$ implements the sieve of Erasthothenes by yielding the n-th element of the infinite list obtained from s by the process of sieving s. Although Sv is a total function, it can transform a total infinite list into a partial one if s does not contain infinitely many primes. The infinite sequence $2,3,4,\ldots$ with an index ${}'[2..]$ has infinitely many primes and so ${}'Sv\bullet{}'[2..]$ yields an index of the infinite sequence of all primes.

The definition of the elementary function p_n by a detour through level two partial functionals may be illustrating the power of functional languages but it is hardly the right way of defining the function. The proof that the function does what it should is difficult because one has to deal with partial functions.

1.8 Second-Order Issues of Modularity

Conservative Second-Order Calculus of Extensions

1.8.1 Tree of extensions. UNFINISHED

UNFINISHED existential instantiation of functions by proofs as a generalization of extraction of programs.

Abstract Data Types

1.8.2 Abstraction Types. UNFINISHED

1.8.3 Representants. UNFINISHED Let $\sim$ be an equivalence over T:

$$\begin{gathered} x \sim y \to T(x) \wedge T(y) \\ T(x) \to x \sim x \\ x \sim y \to y \sim x \\ x \sim y \wedge y \sim z \to x \sim z \ . \end{gathered}$$

We define a predicate provably recursive in $\sim$:

$$\mathit{Isr}(x) \leftrightarrow \forall y(y \sim x \to y \geq x)$$

and a function provably recursive in $\sim$:

$$\begin{aligned} & r(0) = 0 \\ & r(x+1) = y + 1 \leftarrow \mathit{Isr}(x+1) \wedge r(x) = y \wedge \mathit{Isr}(y) \\ & r(x+1) = y \leftarrow \mathit{Isr}(x+1) \wedge r(x) = y \wedge \neg \mathit{Isr}(y) \\ & r(x+1) = r(x) \leftarrow \neg \mathit{Isr}(x+1) \ . \end{aligned}$$

If T is infinite, i.e. if

$$\exists y(y \geq x \wedge T(y))$$

then

$$\begin{gathered} x \sim y \to r(x) = r(y) \\ T(x) \wedge T(y) \wedge r(x) = r(y) \to x \sim y \\ \exists y(x = r(y) \wedge T(y)) \ . \end{gathered}$$

1.8.4 Finite Sequences. Sequences and three specializations: lists, arrays, queues, first typeless, then typed.

1.8.5 Finite Sets. Language: $\emptyset$ empty set, $s \cup \{a\}$ insert into set, ch choice function, $|s|_s$ size of the set, Set predicate of being a set. SET is abbreviation for the formulas of the following groups:

Properties of ch, $\emptyset$, and Set:

$$ch(\emptyset) = 0 \ .$$

Clausal property of set size (there is no measure which goes down):

$$\begin{aligned} & |s|_s = 0 \leftarrow ch(s) = 0 \\ & |s|_s = |t|_s + 1 \leftarrow ch(s) = x, t \ . \end{aligned}$$

Clausal definition of predicate $x : Set$ ($|s|_s$ is the measure):

$$\begin{aligned} & \emptyset : Set \\ & s : Set \leftarrow ch(s) = y, t \wedge t : Set \ . \end{aligned}$$

Clausal definition of set membership ($|s|_s$ is the measure):

$x \in s \leftarrow ch(s) = y, t \wedge (x = y \vee x \in t)$.

Extensionality:

$$s : Set \wedge t : Set \rightarrow (s = t \leftrightarrow \forall x (x \in s \leftrightarrow x \in t)) \ .$$

Properties of insert:

$$s : Set \rightarrow s \cup \{x\} : Set$$
$$s \cup \{x\} : Set \rightarrow (y \in s \cup \{x\} \leftrightarrow y = x \vee y \in s) \ .$$

1.8.6 Typing of sets. Every implementation of SET can be typed for every type T by defining:

$$s : Set(T) \leftrightarrow s : Set \wedge \forall x (x \in s \rightarrow x : T) \ .$$

We can then prove the typing properties:

$$\emptyset : Set(T)$$
$$s : Set(T) \wedge ch(s) = x, t \rightarrow x : T \wedge t : Set(T)$$
$$x : T \wedge s : Set(T) \rightarrow s \cup \{x\} : Set(T) \ .$$

1.8.7 Finite Sets II. Language: $\emptyset$ empty set, $s \cup \{a\}$ insert into set, ch choice function, Axioms: Properties of ch:

$$ch(\emptyset) = 0$$
$$ch(s) = x, t \rightarrow t < s \ .$$

Clausal definition of set membership

$x \in s \leftarrow ch(s) = y, t \wedge (x = y \vee x \in t)$.

Extensionality:

$$s = t \leftrightarrow \forall x (x \in s \leftrightarrow x \in t) \ .$$

Basic property of insert:

$$y \in s \cup \{x\} \leftrightarrow y = x \vee y \in s \ .$$

UNFINISHED three implementations, bitmap, ordered list, binary search tree, Note that membership can be faster than through choice.

1.8.8 Abstract binary trees. Language: $\emptyset$, $Nd(n, s, t)$. Axioms:

$$x = \emptyset \vee \exists n \exists s \exists t \, x = Nd(n, s, t) \tag{1}$$
$$\emptyset \neq Nd(n, s, t) \tag{2}$$
$$Nd(n_1, s_1, t_1) = Nd(n_2, s_2, t_2) \rightarrow n_1 = n_2 \wedge s_1 = s_2 \wedge t_1 = t_2 \tag{3}$$
$$s < Nd(n, s, t) \wedge t < Nd(n, s, t) \ . \tag{4}$$

1.9 Issues Open to Further Research

In-place Modification

UNFINISHED The analysis is intensional, but it can be extensionalized with dag type.

$$Dag = V(\mathbb{N}) \mid P(\mathbb{N}) \mid (Dag, Dag) \mid Dag \,\mathrm{wh}\, List(\mathbb{N}, Dag)\ .$$

Functions are then rewriten to take and yield: $w \,\mathrm{wh}\, b$.

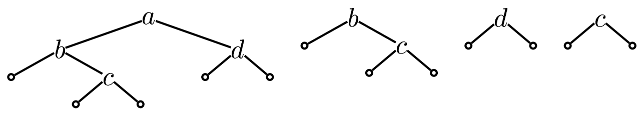
Optimization by Computer-Aided Transformations

Some ten years ago there was a considerable research into the techniques of computer-assisted program transformations in order to optime programs. This was before the semantics of programming languages was sufficiently simplified so the languages could be designed together with formal proof systems. The following problem shows how a rather deep knowledge of properties of underlying data structures is required before programs can be transformed in computer assisted way.

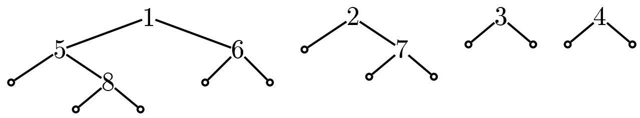
1.9.1 Breadth-first Numbering. We present a so called *functional programming pearl* posed by John Launchberry and discussed by Chris Okasaki in [16]:

> Given a tree, create a new tree of the same shape, but with the values at the nodes replaced by the numbers 1, 2,. . . in breadth-first order.

Okasaki's solution in the programming language ML can be formulated for our binary trees (see Par. 1.3.19) by designing an auxiliary function $B(n, a) = b$ taking a number n and a forest a of type $List\, Bt(t)$ into the forest b of type $List\, Bt(N)$, such that $L(a) = L(b)$, the trees of b are of the same shape as the corresponding trees in a, and the entire forest is numbered starting with n in a breadth-first order. For instance, if a is the forest:



Then $b = B(1, a)$ should be the forest:



The function B looks at its second argument as a queue and yields and works with the output forest as a backward queue to which one adds in the front and removes from the end:

$B(n, 0) = 0$
$B(n, [E] \oplus a) = [E] \oplus B(n, a)$
$B(n, [Nd(x, t, s)] \oplus a) = [Nd(n, t_1, s_1)] \oplus a_1 \leftarrow$
$\quad B(n + 1, a \oplus [t] \oplus [s]) = a_1 \oplus [t_1] \oplus [s_1]$.

In the third clause of B, the subtrees t and s are placed at the end of the argument queue and after the recursive application $B(n+1, a \oplus [t] \oplus [s]) = b$ they will be correctly numbered as t_1 and s_1 respectively in the output forest b which is destructed from the end as $b = a_1 \oplus [t_1] \oplus [s_1]$. The forest a_1 is now correctly numbered to follow the tree $Nd(n, t_1, s_1)$ in the forest yielded by $B(n, [Nd(x, t, s)] \oplus a)$.

The clausal definition of $B(n, a)$ is regular in the measure $\sum_{s \varepsilon a} 2 \cdot |t|_t + 1$ where $|s|_t$ is the *size* of the tree s clausally defined as:

$|E|_t = 0$
$|Nd(x, s_1, s_2)|_t = |s_1|_t + |s_2|_t + 1$.

This is because **UNFINISHED**

The function $Bf(t)$ breadth-first numbering the tree t is now explicitly defined as:

$Bf(t) = t_1 \leftarrow B(1, [t]) = [t_1]$

because the breadth-first numbering of t is the same as the breadth-first numbering of the single element forest $[t]$.

1.9.2 Turning the backwards queue into a normal one. Okasaki notes that the output backwards queue yielded by B can be turned into an ordinary queue in a function $B_1(n, a)$ yielding the same forest as $B(n, a)$ but in the reversed order. We can view the problem of designing the function B_1 as a program transformation problem where we are looking for a recursive clausal definition of the function B_1 given its explicit 'definition'

$$B_1(n, a) = Rev B(n, a) \tag{1}$$

which should be viewed as the desired property of B_1 rather than as a definition. The clausal definition of B_1 can be semi-mechanically obtained from the clasuses for B when we note that we have $a = b \leftrightarrow Rev(a) = Rev(b)$. We accordingly modify the clauses of B to obtain:

$Rev\, B(n, 0) = Rev(0)$
$Rev\, B(n, [E] \oplus a) = Rev(E \oplus B(n, a))$
$Rev\, B(n, [Nd(x, t, s)] \oplus a) = Rev([Nd(n, t_1, s_1)] \oplus a_1) \leftarrow$
$\quad Rev\, B(n + 1, a \oplus [t] \oplus [s]) = Rev(a_1 \oplus [t_1] \oplus [s_1])$.

We now use the obvious properties

$$Rev(0) = 0 \tag{2}$$
$$Rev([a]) = [a] \tag{3}$$
$$Rev(a \oplus b) = Rev(b) + Rev(a) \tag{4}$$

of the list reversal function *Rev* and obtain:

$$\begin{aligned}
&\mathit{Rev}\,B(n,0) = 0\\
&\mathit{Rev}\,B(n,[E]\oplus a) = \mathit{Rev}\,B(n,a)\oplus[E]\\
&\mathit{Rev}\,B(n,[\mathit{Nd}(x,t,s)]\oplus a) = \mathit{Rev}(a_1)\oplus[\mathit{Nd}(n,t_1,s_1)] \leftarrow\\
&\quad \mathit{Rev}\,B(n+1,a\oplus[t]\oplus[s]) = [s_1]\oplus[t_1]\oplus\mathit{Rev}(a_1)\ .
\end{aligned}$$

As the final step, we replace the auxiliary result $\mathit{Rev}(a_1)$ by a_1 and use the property (1) to get the desired clausal definition of the function B_1:

$$\begin{aligned}
&B_1(n,0) = 0\\
&B_1(n,[E]\oplus a) = B_1(n,a)\oplus[E]\\
&B_1(n,[\mathit{Nd}(x,t,s)]\oplus a) = a_1\oplus[\mathit{Nd}(n,t_1,s_1)] \leftarrow\\
&\quad B_1(n+1,a\oplus[t]\oplus[s]) = [s_1]\oplus[t_1]\oplus a_1\ .
\end{aligned}$$

Both input and output queues are now standard where we add at the end and remove from the front. The new breadth-first numbering function Bf_1 has an explicit definition:

$$\mathit{Bf}_1(t) = t_1 \leftarrow B_1(1,[t]) = [t_1]\ .$$

1.9.3 Speeding up the en-queuing. We note that our function $B_1(t)$ operates in time $\mathcal{O}(|t|_s^2)$ because of the naive implementation of the en-queuing operation $q\oplus[x]$ by concatenation. Okasaki improves this naive solution by using a fast implementation of the ADT queue. One such implementation represents a queue $q = a\oplus\mathit{Rev}(b)$ as a pair of lists (a,b). The en-queuing and de-queing functions have the following definitions:

$$\begin{aligned}
&\mathit{Enq}(x,(a,b)) = a,x,b\\
&\mathit{Deq}(0,0) = 0\\
&\mathit{Deq}(0,b) = x,a,0 \leftarrow b>0 \wedge \mathit{Rev}(b) = [x]\oplus a\\
&\mathit{Deq}((x,a),b) = x,a,b\ .
\end{aligned}$$

The reader will note that the de-queuing function yields a pair consisting of the removed element and the new shortened queue provided that the queue is not empty. For empty queues the function yields 0.

Instead of modifying B_1 for the ADT queue, we transform it into a ternary function $B_2(n,a,b)$ where (a,b) represents the input queue $a\oplus\mathit{Rev}(b)$ and B_2 yields the pair (b_1,a_1) representing the output queue $b_1\oplus\mathit{Rev}(a_1)$. In other words, we are looking for a recursive clausal definition of the function B_2 satisfying:

$$B_2(n,a,b) = b_1,a_1 \leftrightarrow B_1(n,a\oplus\mathit{Rev}(b)) = b_1\oplus\mathit{Rev}(a_1)\wedge L(a) = L(a_1)\ . \tag{1}$$

Towards that end we rewrite the clauses of B_1 in an equivalent homogeneous form:

$$
\begin{aligned}
&B_1(n,a) = 0 \leftarrow a = 0\\
&B_1(n,a) = b \oplus [E] \leftarrow a = [E] \oplus a_1 \wedge B_1(n,a_1) = b\\
&B_1(n,a) = a_2 \oplus [Nd(n,t_1,s_1)] \leftarrow a = [Nd(x,t,s)] \oplus a_1 \wedge\\
&\quad B_1(n+1, a_1 \oplus [t] \oplus [s]) = [s_1] \oplus [t_1] \oplus a_2 \ .
\end{aligned}
$$

Substituting $a_0 \oplus Rev$ for a yields:

$$
\begin{aligned}
&B_1(n, a_0 \oplus Rev(b)) = 0 \leftarrow a_0 \oplus Rev(b) = 0 && (2)\\
&B_1(n, a_0 \oplus Rev(b)) = c \oplus [E] \leftarrow a_0 \oplus Rev(b) = [E] \oplus a_1 \wedge B_1(n,a_1) = c && (3)\\
&B_1(n, a_0 \oplus Rev(b)) = a_2 \oplus [Nd(n,t_1,s_1)] \leftarrow a_0 \oplus Rev(b) = [Nd(x,t,s)] \oplus a_1 \wedge\\
&\quad B_1(n+1, a_1 \oplus [t] \oplus [s]) = [s_1] \oplus [t_1] \oplus a_2 \ . && (4)
\end{aligned}
$$

Clause (2) can be equivalently written as

$$B_1(n, 0 \oplus Rev(0)) = 0 \oplus Rev(0)$$

and then by property (1) as

$$B_2(n,0,0) = 0,0 \ . \qquad (5)$$

We will now transform the clause (4) under the assumption that $a_0 > 0$, i.e. $a_0 = [x] \oplus a$ for some x and a. We then have

$$a_0 \oplus Rev(b) = [Nd(x,t,s)] \oplus a_1 \leftrightarrow x = Nd(x,t,s) \wedge a \oplus Rev(b) = a_1$$

and so we can simplify the clause (4) to

$$
\begin{aligned}
&B_1(n, ([Nd(x,t,s)] \oplus a) \oplus Rev(b)) = a_2 \oplus [Nd(n,t_1,s_1)] \leftarrow\\
&\quad B_1(n+1, a \oplus Rev(b) \oplus [t] \oplus [s]) = [s_1] \oplus [t_1] \oplus a_2 \quad .
\end{aligned}
$$

Since

$$a \oplus Rev(b) \oplus [t] \oplus [s] = a \oplus Rev([s] \oplus [t] \oplus b) \ ,$$

we further get

$$
\begin{aligned}
&B_1(n, ([Nd(x,t,s)] \oplus a) \oplus Rev(b)) = a_2 \oplus [Nd(n,t_1,s_1)] \leftarrow\\
&\quad B_1(n+1, a \oplus Rev([s] \oplus [t] \oplus b)) = [s_1] \oplus [t_1] \oplus a_2 \quad .
\end{aligned}
$$

We always have $a_2 = b_1 \oplus Rev(a_1)$ for some b_1 and a_1 and, since

$$L(a_2){+}2 = L\,B_1(n{+}1, a{\oplus}Rev([s]{\oplus}[t]{\oplus}b)) = L(a{\oplus}Rev([s]{\oplus}[t]{\oplus}b)) = L(a){+}L(b){+}2 \ ,$$

we can also assume that $L(a_1) = L(a)$ (and $L(b_1) = L(b)$). The last clause can be then written as

$$
\begin{aligned}
&B_1(n, ([Nd(x,t,s)] \oplus a) \oplus Rev(b)) = (b_1 \oplus Rev(a_1)) \oplus [Nd(n,t_1,s_1)] \leftarrow\\
&\quad B_1(n+1, a \oplus Rev([s] \oplus [t] \oplus b)) = [s_1] \oplus [t_1] \oplus (b_1 \oplus Rev(a_1)) \wedge L(a) = L(a_1)
\end{aligned}
$$

which simplifies to:

$$
\begin{aligned}
&B_1(n, ([Nd(x,t,s)] \oplus a) \oplus Rev(b)) = b_1 \oplus Rev([Nd(n,t_1,s_1)] \oplus a_1) \leftarrow\\
&\quad B_1(n+1, a \oplus Rev([s] \oplus [t] \oplus b)) = ([s_1] \oplus [t_1] \oplus b_1) \oplus Rev(a_1) \wedge L(a) = L(a_1) \quad .
\end{aligned}
$$

Using the property (1) we get from this a clause for B_2:

$$B_2(n, [Nd(x,t,s)] \oplus a, b) = b_1, [Nd(n,t_1,s_1)] \oplus a_1 \leftarrow$$
$$B_2(n+1, a, [s] \oplus [t] \oplus b) = [s_1] \oplus [t_1] \oplus b_1, a_1 \ . \tag{6}$$

By similar transformations we obtain under the assumption $a_0 > 0$ from the clause (3) the clause

$$B_2(n, [E] \oplus a, b) = b_1, [E] \oplus a_1 \leftarrow B_2(n, a, b) = b_1, a_1 \ . \tag{7}$$

We now transform the clauses (3) and (4) under the assumption that $a_0 = 0$. The clauses simplify to:

$$B_1(n, 0 \oplus Rev(b)) = c \oplus [E] \leftarrow Rev(b) = [E] \oplus a_1 \wedge B_1(n, a_1) = c$$
$$B_1(n, 0 \oplus Rev(b)) = a_2 \oplus [Nd(n,t_1,s_1)] \leftarrow Rev(b) = [Nd(x,t,s)] \oplus a_1 \wedge$$
$$B_1(n+1, a_1 \oplus [t] \oplus [s]) = [s_1] \oplus [t_1] \oplus a_2 \ .$$

Both clauses have in their antecedents $Rev(b) \neq 0$ from which we get $b \neq 0$ and we can collapse both clauses into one 'trivial' clause:

$$B_1(n, 0 \oplus Rev(b)) = c \leftarrow b \neq 0 \wedge B_1(n, Rev(b)) = c \ .$$

We substitute $c := Rev(b_1)$ to get:

$$B_1(n, 0 \oplus Rev(b)) = Rev(b_1) \leftarrow b \neq 0 \wedge B_1(n, Rev(b)) = Rev(b_1) \ .$$

We have

$$L(b) = L\,Rev(b) = L\,B_1(n, Rev(b)) = L\,Rev(b_1) = L(b_1)$$

and so we can equivalently write the clause as:

$$B_1(n, 0 \oplus Rev(b)) = Rev(b_1) \oplus Rev(0) \leftarrow b \neq 0 \wedge$$
$$B_1(n, Rev(b) \oplus Rev(0)) = 0 \oplus Rev(b_1) \wedge L\,Rev(b) = L\,Rev(b_1) \ .$$

Using the property (1) we get from this a clause for B_2:

$$B_2(n, 0, b) = Rev(b_1), 0 \leftarrow b \neq 0 \wedge B_2(n, Rev(b), 0) = 0, b_1 \ . \tag{8}$$

The clauses (5), (8), (7), and (6) constitute a clausal definition for the function B_2 which we write with the list notation x, y instead of the identical sequence notation $[x] \oplus y$ as follows:

$$B_2(n, 0, 0) = 0, 0$$
$$B_2(n, 0, b) = Rev(b_1), 0 \leftarrow b \neq 0 \wedge B_1(n, Rev(b), 0) = 0, b_1$$
$$B_2(n, (E, a), b) = b_1, E, a_1 \leftarrow B_2(n, a, b) = b_1, a_1$$
$$B_2(n, (Nd(x,t,s), a), b) = b_1, Nd(n, t_1, s_1), a_1 \leftarrow$$
$$B_2(n+1, a, s, t, b) = (s_1, t_1, b_1), a_1 \ .$$

It remains to explicitly define the function Bf_2 numbering one tree as

$$Bf_2(t) = t_1 \leftarrow B_2(1, (t, 0), 0) = (t_1, b), a \ .$$

The function $Bf_2(s)$ performs in time $\mathcal{O}(|s|_t)$ because the second clause for B_2 is taken once for each level of the tree s with the corresponding forest of children of t as b. This means that the function Rev performs total $2 \cdot |s|_t$ applications and the maximal length.

is probably one the fastest functional algorithms for the breadth 3 times through.

Concurrency

Part I

First-Order Logic and Peano Arithmetic

2. First-Order Languages

2.1 Language of First-Order Logic

2.1.1 First order languages. A *first-order language* $\mathcal{L}$ is given by at most countable sets of *function symbols* and *predicate symols*. Every function and predicate symbol has *arity* $n \geq 0$ which is the number of arguments the symbol expects. We require that there are effective procedures to decide whether p is an n-ary function or predicate symbol of $\mathcal{L}$.

Expressions in $\mathcal{L}$ will be *terms* and *formulas* and they will be finite sequences of symbols. Expressions will be *metamathematical* objects in contrast to mathemathical objects such as natural numbers, real numbers, topological spaces, etc. The expressions of $\mathcal{L}$ will have have no meaning by themselves. They will be defined in such a way that it will be effectively decidable whether an expression is correctly formed.

We write $\tau_1 \equiv \tau_2$ to mean that the expressions τ_1 and τ_2 are identical sequences of symbols.

In these notes we will deal exclusively with first order languages logic so from now on we will use the term *language* to denote a first order language.

2.1.2 Definition of terms of $\mathcal{L}$. The set of *terms* of a language $\mathcal{L}$ is the smallest set of finite sequences of symbols satisfying:

1. variables v_0, v_1, v_2, ... are terms,
2. if $\tau_1, \ldots, \tau_n$ are terms and f is an n-ary function symbol of $\mathcal{L}$ then also $f(\tau_1, \ldots, \tau_n)$ is a term called *function application*.

Nullary function symbols are *constant* symbols and their applications $f()$, which will be abbrevaited to f, are *constants*.

We will use possibly subscripted symbols x, y, z as *syntactic* (meta) variables ranging over variables, symbols f, g as syntactic variables ranging over function symbols, and τ, ρ as syntactic variables ranging over terms.

Some binary function symbols, such as $+$, are customarily written in the *infix* form $\tau_1 + \tau_2$ as an abbreviation for $+(\tau_1, \tau_2)$.

2.1.3 Definition of formulas of $\mathcal{L}$. The set of *formulas* of a language $\mathcal{L}$ is the smallest set of finite sequences of symbols satisfying:

1. if τ_1 and τ_2 are terms of $\mathcal{L}$ then $\tau_1 = \tau_2$ is a formula called *identity*,
2. if $\tau_1, \ldots, \tau_n$ are terms and P is an n-ary predicate symbol of $\mathcal{L}$ then $P(\tau_1, \ldots, \tau_n)$ is a formula called *predicate application*,
3. the symbol $\top$, called the *truth symbol*, is a formula,
4. the symbol $\bot$, called *falsehood symbol*, is a formula,
5. if ϕ is a formula so is $\neg\phi$ called *negation*,
6. if ϕ_1 and ϕ_2 are formulas so is $(\phi_1 \vee \phi_2)$, (called *disjunction*), $(\phi_1 \wedge \phi_2)$ (called *conjunction*), $(\phi_1 \rightarrow \phi_2)$ (called *implication*), and $(\phi_1 \leftrightarrow \phi_2)$ (called *equivalence*),
7. if ϕ is a formula and x a variable then so are $\forall x \phi$ (called *universal quantification*) and $\exists x \phi$ (called *existential quantification*).

Formulas formed by the rules (1) and (2) are *atomic formulas.* Formulas formed by the rules (3) though (6) are *propositional* formulas. Formulas formed by the rule (7) are *quantifier* formulas.

The formula ϕ_1 in the implication $(\phi_1 \rightarrow \phi_2)$ is called *antecedent* and ϕ_2 *consequent*. The symbols used in propositional formulas are *propositional connectives*. Nullary predicate symbols are *propositional constants* and their applications $P()$, which will be abbreviated to P, are *propositional constants.*

We use the possibly subscripted symbols ϕ, ψ as syntactic variables ranging over formulas.

In order to increase the readability of formulas we can drop the topmost pair of parentheses around a formula. All binary propositional connectives associate to the right, for instance $\phi_1 \rightarrow \phi_2 \rightarrow \phi_3$ abbreviates $\phi_1 \rightarrow (\phi_2 \rightarrow \phi_3)$. Negations and quantification have larger precedence (bind stronger) than conjunctions, which have larger precedence than disjunctions, which have larger precedence than implications and equivalences. We often abbreviate $\neg\tau_1 = \tau_2$ to $\tau_1 \neq \tau_2$.

2.1.4 Propositional atoms. Atomic and quantified formulas of $\mathcal{L}$ are called the *propositional atoms* of $\mathcal{L}$. The metamathematical function $FPA(\alpha)$ is defined to yield the set of *free* propositional atoms of α, i.e. propositional atoms of α outside of quantifiers. The function is defined for formulas $\alpha \equiv \phi$ and sets of formulas $\alpha \equiv T$ to satisfy the identities given in Fig. 2.1.

2.1.5 Extension of languages. The language $\mathcal{L}_1$ is an *extension* of the language $\mathcal{L}$ if every function and predicate symbol of $\mathcal{L}$ is a symbol of $\mathcal{L}_1$. It should be clear that every term or formula of $\mathcal{L}$ is a term or formula of $\mathcal{L}_1$. Note that every $\mathcal{L}$ is an extension of itself.

2.1.6 Metamathematical implication and equivalence. In order to shorten the metamathematical discursion in English we will use the symbol $\Rightarrow$ in context $\cdots \Rightarrow \cdots$ as abbreviation for *if* $\cdots$ *then* $\cdots$ and the symbol $\Leftrightarrow$ in context $\cdots \Leftrightarrow \cdots$ as abbreviation for $\cdots$ *if and only if* $\cdots$. Sometimes we will write the last also as $\cdots$ *iff* $\cdots$. We use the metamathematical sym-

$$
\begin{aligned}
FPA(\tau_1 = \tau_2) &= \{\tau_1 = \tau_2\} \\
FPA(P(\tau_1, \ldots, \tau_n)) &= \{P(\tau_1, \ldots, \tau_n)\} \\
FPA(\forall x \phi) &= \{\forall x \phi\} \\
FPA(\exists x \phi) &= \{\exists x \phi\} \\
FPA(\top) &= \emptyset \\
FPA(\bot) &= \emptyset \\
FPA(\neg \phi) &= FPA(\phi) \\
FPA(\phi_1 \vee \phi_2) &= FPA(\phi_1) \cup FPA(\phi_2) \\
FPA(\phi_1 \wedge \phi_2) &= FPA(\phi_1) \cup FPA(\phi_2) \\
FPA(\phi_1 \rightarrow \phi_2) &= FPA(\phi_1) \cup FPA(\phi_2) \\
FPA(\phi_1 \leftrightarrow \phi_2) &= FPA(\phi_1) \cup FPA(\phi_2) \\
FPA(T) &= \bigcup \{FPA(\phi) \mid \phi \in T\} \ .
\end{aligned}
$$

Fig. 2.1. Function yielding sets of propositional atoms

bols $\Rightarrow$ and $\Leftrightarrow$ in order to distinguish them from the logical symbols $\rightarrow$ and $\leftrightarrow$ wchich are from the *object*, i.e. first order, language.

3. Propositional Logic

3.1 Tautologies

In this section we investigate formulas which are always true only on the strength of their propositional connectives.

3.1.1 Propositional interpretations. A *propositional interpretation* $\mathcal{I}$ for $\mathcal{L}$ is a subset of propositional atoms of $\mathcal{L}$. $\mathcal{I}$ is *finite* or *infinite* if the set $\mathcal{I}$ is finite or infinite. The intention is that a propositional atom ϕ is true in the propositional interpretation $\mathcal{I}$ iff $\phi \in \mathcal{I}$.

We denote by $\mathcal{I}^T$ the *restriction of* $\mathcal{I}$ *to the free propositional atoms of the set* T: $\mathcal{I}^T = \mathcal{I} \cap FPA(T)$.

3.1.2 Satisfaction relation for propositional interpretations. For a given propositional interpretation $\mathcal{I}$ for $\mathcal{L}$ and a formula ϕ we define the unary relation $\mathcal{I}$ *satisfies* ϕ, written as $\mathcal{I} \vDash \phi$, as shown in Fig. 3.1 where ϕ, ϕ_1 and ϕ_2 are arbitrary formulas and ψ are propositional atoms of $\mathcal{L}$:

$$\begin{aligned}
\mathcal{I} \vDash \psi &\Leftrightarrow \psi \in \mathcal{I} \\
\mathcal{I} &\vDash \top \\
\mathcal{I} &\nvDash \bot \\
\mathcal{I} \vDash \neg\phi &\Leftrightarrow \mathcal{I} \nvDash \phi \\
\mathcal{I} \vDash \phi_1 \vee \phi_2 &\Leftrightarrow \mathcal{I} \vDash \phi_1 \text{ or } \mathcal{I} \vDash \phi_2 \\
\mathcal{I} \vDash \phi_1 \wedge \phi_2 &\Leftrightarrow \mathcal{I} \vDash \phi_1 \text{ and } \mathcal{I} \vDash \phi_2 \\
\mathcal{I} \vDash \phi_1 \rightarrow \phi_2 &\Leftrightarrow \mathcal{I} \nvDash \phi_1 \text{ or } \mathcal{I} \vDash \phi_2 \\
\mathcal{I} \vDash \phi_1 \leftrightarrow \phi_2 &\Leftrightarrow \mathcal{I} \vDash \phi_1 \rightarrow \phi_2 \text{ and } \mathcal{I} \vDash \phi_2 \rightarrow \phi_1 \ .
\end{aligned}$$

Fig. 3.1. Propositional satisfaction relation

Note that the propositional atoms obtain meaning directly from $\mathcal{I}$ whereas the meaning of other kinds of propositional formulas is uniquely determined by the meaning of its subformulas.

We write $\mathcal{I} \vDash T$ as an abbreviation for $\mathcal{I} \vDash \phi$ *for all* $\phi \in T$ and say that T *is satisfied in* $\mathcal{I}$.

Two (propositional) interpretations $\mathcal{I}$ and $\mathcal{J}$ for $\mathcal{L}$ are (elementarily) T-*equivalent*, in writing $\mathcal{I} \equiv_T \mathcal{J}$, if

$$\mathcal{I} \vDash T \Leftrightarrow \mathcal{J} \vDash T \ .$$

$\mathcal{I}$ and $\mathcal{J}$ are (elementarily) *equivalent*, in writing $\mathcal{I} \equiv \mathcal{J}$, if they are $\{\phi \mid \phi \in \mathcal{L}\}$-equivalent, i.e. $\mathcal{I} \vDash \phi \Leftrightarrow \mathcal{J} \vDash \phi$ holds for all formulas ϕ.

3.1.3 Sequents. Fix a language $\mathcal{L}$. For a finite sequence of formulas Λ: ϕ_1, $\ldots$, ϕ_n we write $\bigwedge\Lambda$ as an abbreviation for the conjunction $\phi_1 \wedge \cdots \wedge \phi_n$ if $n \geq 1$ and for $\top$ if $n = 0$. For any propositional interpretation $\mathcal{I}$ we clearly have $\mathcal{I} \vDash \bigwedge\Lambda$ iff $\mathcal{I} \vDash \phi$ for all $\phi \in \Lambda$. Note that this holds also for $\Lambda \equiv \emptyset$ because $\bigwedge\emptyset \equiv \top$ for which $\mathcal{I} \vDash \top$ holds just as $\mathcal{I} \vDash \phi$ vacuously holds for all $\phi \in \emptyset$.

For the same sequence Λ we write $\bigvee\Lambda$ as an abbreviation for the disjunction $\phi_1 \vee \cdots \vee \phi_n$ if $n \geq 1$ and for $\bot$ if $n = 0$. For any propositional interpretation $\mathcal{I}$ we clearly have $\mathcal{I} \vDash \bigvee\Lambda$ iff $\mathcal{I} \vDash \phi$ for some $\phi \in \Lambda$.

For two finite sequences of formulas Λ and Γ we call the formula $\bigwedge\Lambda \rightarrow \bigvee\Gamma$ a *sequent*. For any propositional interpretation $\mathcal{I}$ we clearly have $\mathcal{I} \vDash \bigwedge\Lambda \rightarrow \bigvee\Gamma$ iff $\mathcal{I} \nvDash \phi$ for some $\phi \in \Lambda$ or $\mathcal{I} \vDash \phi$ for some $\phi \in \Gamma$. Thus $\mathcal{I} \nvDash \bigwedge\Lambda \rightarrow \bigvee\Gamma$ iff $\mathcal{I} \vDash \phi$ for all $\phi \in \Lambda$ and $\mathcal{I} \nvDash \phi$ for all $\phi \in \Gamma$. We have $\mathcal{I} \nvDash \bigwedge\emptyset \rightarrow \bigvee\emptyset$ because this stands for $\mathcal{I} \nvDash \top \rightarrow \bot$.

3.1.4 Tautologies. A formula ϕ of $\mathcal{L}$ is a *tautology*, in symbols $\vDash_p \phi$, if $\mathcal{I} \vDash \phi$ holds for all propositional interpretations $\mathcal{I}$ for $\mathcal{L}$.

We say that two formulas ϕ_1 and ϕ_2 are *propositionally equivalent* if we have $\mathcal{I} \vDash \phi_1 \Leftrightarrow \mathcal{I} \vDash \phi_2$ for all propositional interpretations $\mathcal{I}$. But this means that $\mathcal{I} \vDash \phi_1 \leftrightarrow \phi_2$ holds for all propositional interpretations $\mathcal{I}$ and so $\phi_1 \leftrightarrow \phi_2$ is a tautology. Note that we then also have $\vDash_p \phi_1$ iff $\vDash_p \phi_2$.

Because $\mathcal{I} \vDash \phi_1 \wedge \phi_2$ holds iff $\mathcal{I} \vDash \phi_1$ and $\mathcal{I} \vDash \phi_2$ hold we have $\vDash_p \phi_1 \wedge \phi_2$ iff $\vDash_p \phi_1$ and $\vDash_p \phi_2$.

3.1.5 Equivalence lemma.

$$\mathcal{I}^T = \mathcal{J}^T \Rightarrow \mathcal{I} \equiv_T \mathcal{J} \ .$$

Proof. Assume $\mathcal{I}^T = \mathcal{J}^T$ and for any $\phi \in T$ prove $\mathcal{I} \vDash \phi \Leftrightarrow \mathcal{J} \vDash \phi$ by a straightforward induction on the construction of ϕ because for every $\phi \in FPA(\phi)$ we have $\phi \in \mathcal{I} \Leftrightarrow \phi \in \mathcal{J}$. □

3.1.6 Decidability of tautologies. Fix a language $\mathcal{L}$. We call a set S of formulas of $\mathcal{L}$ *decidable* if we can effectively decide for every formula ϕ whether or not $\phi \in S$ holds. Finite sets S are clearly decidable.

For every decidable propositional interpretation $\mathcal{I}$ and for every formula ϕ of $\mathcal{L}$ we can effectively decide whether $\mathcal{I} \vDash \phi$ holds by simply using the properties Par. 3.1.2 of propositional truth.

We can effectively decide whether a formula ϕ is a tautology because the set $FPA\phi$ of all of its free propositional atoms contains finitely many, say n, atoms. We claim that $\vDash_p \phi$ holds iff $\mathcal{I} \vDash_p \phi$ holds for all 2^n subsets $\mathcal{I}$ of $FPA(\phi)$ and the last is clearly effectively decidable. The claim holds because if ϕ is a tautology then it is true in all subsets of $FPA(\phi)$. On the other hand, if ϕ is true in all subsets of $FPA(\phi)$ then if $\mathcal{I}$ is any propositional interpretation for $\mathcal{L}$ then so is $\mathcal{I}^\phi \subseteq FPA(\phi)$ and we have $\mathcal{I}^\phi \vDash \phi$ and hence $\mathcal{I} \vDash \phi$ by Lemma 3.1.5. Thus ϕ is a tautology.

The just described method of deciding whether ϕ is a tautology is called the *truth table method* because every propositional interpretation $\mathcal{I} \subseteq FPA(\phi)$ can be viewed as a row in a table containing t or f according to whether $\mathcal{I} \vDash \phi$ holds or not.

3.2 Propositional Tableaux

We now introduce a method of testing for tautologies by propositional *tableau* proofs. Tableaux were first used by Beth [2] and refined by R. Smullyan [21]. We use the signed tableaux of Smullyan but in a positive way which proves goals rather than refuting them. We will show that tableau proofs prove exactly the tautologies. We introduce the tableaux because they can be extended to deal with identity and quantifiers whereas the truth table method cannot, at least not directly.

3.2.1 Signed formulas. A formula ϕ of a language $\mathcal{L}$ is *signed* if it is written in one of two forms: ϕ or $\phi*$. The signed formula of the first form is called *assumption* and of the second form *goal*. We will use ϕ^+ as a syntactic variable ranging over signed formulas. We will denote by Δ finite nonempty sequences of signed formulas. Every sequence Δ of signed formulas can be associated with a sequent $\bigwedge\Lambda \to \bigvee\Gamma$ where the sequence Λ contains exactly the assumptions in Δ and the sequence Γ contains exactly the goals in Δ (with the signs $*$ deleted).

3.2.2 Propositional tableaux. Fix a language $\mathcal{L}$. Propositional tableaux for $\mathcal{L}$ are finitely branching trees built by to two kinds of expansion rules. A *unary tableau expansion* is of the form

$$\frac{\Delta_1}{\phi_1^+} \tag{1}$$

where Δ_1 is a possibly empty sequence of signed formulas and ϕ_1^+ a signed formula. A *binary tableau expansion rule* is of the form

$$\frac{\Delta_1}{\phi_1^+ \mid \phi_2^+} \tag{2}$$

where also ϕ_2^+ is a signed formula. The signed formulas of Δ are called *premises* and the signed formulas ϕ_1^+ and ϕ_2^+ *conclusions* of the expansion rules.

Let Δ be a non-empty sequence of signed formulas and $\bigwedge\Lambda \to \bigvee\Gamma$ a sequent associated with Δ. A binary tree π with signed formulas as labels is a *tableau for Δ*:

$$\frac{\Delta}{\pi}$$

if the tree π is either empty or it is obtained by an expansion rule. In the graphical representation we place the tableau π under the sequence of signed formulas Δ. The tableau is separated from the sequence by a solid line.

If the tableau π for Δ is empty then it has the form

$$\frac{\Delta}{\circ}$$

If the tableau π for Δ is obtained by a unary rule (1) then it has the form

$$\begin{array}{c} \Delta \\ \hline \phi_1^+ \\ \pi_1 \end{array} \quad \text{where } \Delta_1 \subseteq \Delta \text{ and } \quad \begin{array}{c} \Delta \\ \phi_1^+ \\ \hline \pi_1 \end{array}$$

Note that π_1 is a tableau for the sequence Δ, ϕ_1^+. The unary propositional rules will be such that

$$\models_p (\bigwedge\Lambda \to \bigvee\Gamma) \leftrightarrow (\bigwedge\Lambda_1 \to \bigvee\Gamma_1) \tag{3}$$

where the sequent on the right is associated with Δ, ϕ_1^+.

If the tableau π for Δ is obtained by a binary rule (2) then it has the form

$$\begin{array}{cc} \multicolumn{2}{c}{\Delta} \\ \hline \phi_1^+ & \phi_2^+ \\ \pi_1 & \pi_2 \end{array} \quad \text{where } \Delta_1 \subseteq \Delta, \quad \begin{array}{c} \Delta \\ \phi_1^+ \\ \hline \pi_1 \end{array} \quad \text{, and} \quad \begin{array}{c} \Delta \\ \phi_2^+ \\ \hline \pi_2 \end{array}$$

Note that π_1 is a tableau for the sequence Δ, ϕ_1 and π_2 a tableau for the sequence Δ, ϕ_2. The binary rules will be such that

$$\models_p (\bigwedge\Lambda \to \bigvee\Gamma) \leftrightarrow (\bigwedge\Lambda_1 \to \bigvee\Gamma_1) \land (\bigwedge\Lambda_2 \to \bigvee\Gamma_2) \tag{4}$$

where the two sequents on the right are associated with Δ, ϕ_1^+ and Δ, ϕ_2^+ respectively.

3.2.3 Propositional tableau expansion rules. Fix a language $\mathcal{L}$. The following unary propositional tableau expansion rules are called *flatten rules*:

$$\frac{\phi_1 \wedge \phi_2}{\phi_1}\,(\wedge_1) \quad \frac{\phi_1 \wedge \phi_2}{\phi_2}\,(\wedge_2) \quad \frac{\phi_1 \leftrightarrow \phi_2}{\phi_1 \rightarrow \phi_2}\,(\leftrightarrow_1) \quad \frac{\phi_1 \leftrightarrow \phi_2}{\phi_2 \rightarrow \phi_1}\,(\leftrightarrow_2)$$
$$\frac{\phi_1 \rightarrow \phi_2 *}{\phi_1}\,(\rightarrow_1 *) \quad \frac{\phi_1 \rightarrow \phi_2 *}{\phi_2 *}\,(\rightarrow_2 *) \quad \frac{\phi_1 \vee \phi_2 *}{\phi_1 *}\,(\vee_1 *) \quad \frac{\phi_1 \vee \phi_2 *}{\phi_2 *}\,(\vee_2 *)\ .$$

The following binary propositional tableau expansion rules are called *split rules*:

$$\frac{\phi_1 \vee \phi_2}{\phi_1 \mid \phi_2}\,(\vee) \quad \frac{\phi_1 \rightarrow \phi_2}{\phi_2 \mid \phi_1 *}\,(\rightarrow) \quad \frac{\phi_1 \wedge \phi_2 *}{\phi_1 * \mid \phi_2 *}\,(\wedge *) \quad \frac{\phi_1 \leftrightarrow \phi_2 *}{\phi_1 \rightarrow \phi_2 * \mid \phi_2 \rightarrow \phi_1 *}\,(\leftrightarrow *)\ .$$

The following unary propositional tableau expansion rules are called *inversion rules*:

$$\frac{\neg\phi}{\phi *}\,(\neg) \quad \frac{\neg\phi *}{\phi}\,(\neg *)\ .$$

Note that we have for each propositional connective two rules, one when the connective is the premise formula as an assumption and one as a goal.

We will now convince ourselves by the truth table method that, for instance, the rule $\rightarrow$ satisfies 3.2.2(4) which has the form:

$$\models_p ((\phi_1 \rightarrow \phi_2) \wedge \bigwedge \Lambda \rightarrow \bigvee \Gamma) \leftrightarrow (\phi_2 \wedge \bigwedge \Lambda \rightarrow \bigvee \Gamma) \wedge (\bigwedge \Lambda \rightarrow \phi_1 \vee \bigvee \Gamma)\ .$$

Indeed, for every propositional interpretation $\mathcal{I}$ we have

$$\mathcal{I} \models (\phi_1 \rightarrow \phi_2) \wedge \bigwedge \Lambda \rightarrow \bigvee \Gamma$$

iff $\mathcal{I} \not\models \phi_1 \rightarrow \phi_2$ or $\mathcal{I} \models \bigwedge\Lambda \rightarrow \bigvee\Gamma$ iff ($\mathcal{I} \models \phi_1$ and $\mathcal{I} \not\models \phi_2$) or $\mathcal{I} \models \bigwedge\Lambda \rightarrow \bigvee\Gamma$ iff $\mathcal{I} \models \bigwedge\Lambda \rightarrow \phi_1 \vee \bigvee\Gamma$ and $\mathcal{I} \models \phi_2 \wedge \bigwedge\Lambda \rightarrow \bigvee\Gamma$ iff

$$\mathcal{I} \models (\phi_2 \wedge \bigwedge \Lambda \rightarrow \bigvee \Gamma) \wedge (\bigwedge \Lambda \rightarrow \phi_1 \vee \bigvee \Gamma)\ .$$

3.2.4 Proofs with propositional tableaux. Fix a language $\mathcal{L}$. Let Δ be a non-empty finite sequence of signed formulas of $\mathcal{L}$, and π a propositional tableau for Δ.

A *branch* of the tableau π is a sequence of signed formulas Δ, Δ_1 where Δ_1 is read off some branch of the tree π. We say that the branch is *closed on* ϕ if both ϕ and $\phi*$ are in the branch Δ, Δ_1. The branch is *closed* if Δ, Δ_1 contains either the goal $\top *$, or the assumption $\bot$, or the branch is closed on some ϕ different from $\top$ and $\bot$. The tableau π is *closed* if all of its branches are closed.

We write $\pi\colon \vdash_p [\Delta]$ when π is a closed propositional tableau for Δ. We write $\vdash_p [\Delta]$ if there is a propositional tableau π such that $\pi\colon \vdash_p [\Delta]$. By a simple induction proof on the structure of π we can show:

$$\pi : \vdash_p [\Delta] \text{ and } \Delta \subseteq \Delta_1 \Rightarrow \pi : \vdash_p [\Delta_1]$$

where by $\Delta \subseteq \Delta_1$ we mean $\phi^+ \in \Delta \Rightarrow \phi^+ \in \Delta_1$ *for all* ϕ^+.

For a formula ϕ we say that the tableau π *proves* ϕ, in symbols $\pi\colon \vdash_p \phi$, if $\pi\colon \vdash_p [\phi*]$ holds. The same conventions as for sequences Δ apply also to formulas ϕ. In particular, we say that ϕ *is provable* if $\vdash_p \phi$ holds. For a set of of formulas S we write $\vdash_p S$ if $\vdash_p \phi$ holds for all $\phi \in S$.

3.2.5 Lemma (Soundness of propositional tableaux). *If* $\bigwedge\Lambda \to \bigvee\Gamma$ *is associated to* Δ *then*

$$\pi\colon \vdash_p [\Delta] \Rightarrow \;\vDash_p \bigwedge\Lambda \to \bigvee\Gamma \;.$$

Proof. By induction on the structure of π. So assume that the tableau π for Δ is closed:

$$\begin{array}{c}\Delta \\ \hline \cdots\pi\cdots\end{array}$$

and perform a case analysis on π. If π is empty then either $\top* \in \Delta$, i.e. $\top \in \Gamma$, or $\bot \in \Delta$, i.e. $\bot \in \Lambda$, or else $\psi, \psi* \in \Delta$, i.e. $\psi \in \Lambda$ and $\psi \in \Gamma$ for some propositional atom ψ. For any propositional interpretation $\mathcal{I}$ we then have $\mathcal{I} \vDash \bigwedge\Lambda \to \bigvee\Gamma$ and so the sequent is a tautology.

If the first expansion in π is by a unary rule 3.2.2(1) such that $\Delta_1 \subseteq \Delta$ then we have

$$\begin{array}{c}\Delta \\ \hline \phi_1^+ \\ \cdots\pi_1\cdots\end{array} \quad \text{i.e.} \quad \begin{array}{c}\Delta \\ \phi_1^+ \\ \hline \cdots\pi_1\cdots\end{array}$$

for some tableau π_1 such that $\pi_1\colon \vdash_p [\Delta, \phi_1^+]$. Let $\bigwedge\Lambda_1 \to \bigvee\Gamma_1$ be a sequent associated with Δ, ϕ_1^+. We get $\vDash_p \bigwedge\Lambda_1 \to \bigvee\Gamma_1$ by IH and so $\vDash_p \bigwedge\Lambda \to \bigvee\Gamma$ by 3.2.2(3).

If the first expansion in π is by a binary rule 3.2.2(2) such that $\Delta_1 \subseteq \Delta$ then we have

$$\begin{array}{cc}\multicolumn{2}{c}{\Delta} \\ \hline \phi_1^+ & \phi_2^+ \\ \cdots\pi_1\cdots & \cdots\pi_2\cdots\end{array} \quad \text{i.e.} \quad \begin{array}{c}\Delta \\ \phi_1^+ \\ \hline \cdots\pi_1\cdots\end{array} \quad \text{and} \quad \begin{array}{c}\Delta \\ \phi_2^+ \\ \hline \cdots\pi_2\cdots\end{array}$$

for some tableaux π_1 and π_2 such that $\pi_1\colon \vdash_p [\Delta, \phi_1^+]$ and $\pi_2\colon \vdash_p [\Delta, \phi_2^+]$. Let $\bigwedge\Lambda_1 \to \bigvee\Gamma_1$ and $\bigwedge\Lambda_2 \to \bigvee\Gamma_2$ be sequents associated with Δ, ϕ_1^+ and

Δ, ϕ_2^+ respectively. We get $\models_p \bigwedge \Lambda_1 \to \bigvee \Gamma_1$ and $\models_p \bigwedge \Lambda_2 \to \bigvee \Gamma_2$ by two IH's. Hence $\models_p \bigwedge \Lambda \to \bigvee \Gamma$ by 3.2.2(4). $\square$

3.2.6 Lemma (Completeness of propositional tableaux). *If $\bigwedge \Lambda \to \bigvee \Gamma$ is associated with Δ then*

$$\models_p \bigwedge \Lambda \to \bigvee \Gamma \Rightarrow \ \vdash_p [\Delta] \ .$$

Proof. Assume $\models_p \bigwedge \Lambda \to \bigvee \Gamma$ and prove $\vdash_p [\Delta]$ by induction on the total number n of propositional connectives in the formulas of Δ (not counting those within quantifiers).

If $n = 0$ then Δ consists at most of propositional atoms $\bot$ and $\top$. If $\bot \in \Lambda$ or $\top \in \Gamma$ then the branch Δ is closed. If neither of the two cases applies and the sequences Λ and Γ have no propositional atom in common then we have a contradiction because $\mathcal{I} \not\models \bigwedge \Lambda \to \bigvee \Gamma$ for $\mathcal{I} = \{\phi \mid \phi \in \Lambda\}$. Thus Δ must be closed on some ϕ. Hence, in both cases it suffices to take π empty.

If $n > 0$ then select a signed propositional formula ϕ^+ of Δ which is not $\top$ or $\bot$ and denote by Δ_1 the sequence obtained from Δ by omitting the selected formula from it. Denote by Λ_1 the sequence obtained from Λ by deleting ϕ if the selected signed formula is an assumption and the sequence Λ otherwise and denote by Γ_1 the sequence obtained from Γ by deleting ϕ if the selected formula is a goal and the sequence Γ otherwise. Thus if the selected formula is a goal then $\bigwedge \Lambda_1 \to \phi \vee \bigvee \Gamma_1$ is a tautology and if the selected formula is an assumption then $\phi \wedge \bigwedge \Lambda_1 \to \bigvee \Gamma_1$ is a tautology. We wish to prove $\vdash_p [\Delta]$ by the case analysis of the signed formula ϕ^+.

If $\phi^+ \equiv \neg \phi_1 * \in \Delta$ then, since $\models_p \bigwedge \Lambda_1 \to \neg \phi_1 \vee \bigvee \Gamma_1$, we also have $\models_p \phi_1 \wedge \bigwedge \Lambda_1 \to \bigvee \Gamma_1$. The associated sequence Δ_1, ϕ_1 has $n - 1$ connectives and so $\pi_1 \colon \vdash_p [\Delta_1, \phi_1]$ for some π_1 by IH. This is shown on the left and the constructed tableau is shown on the right:

$$\begin{array}{c} \Delta_1 \\ \phi_1 \\ \hline \cdots \pi_1 \cdots \end{array} \quad \Rightarrow \quad \begin{array}{cc} \Delta & \\ \hline \phi_1 & (\neg *) \\ \cdots \pi_1 \cdots & \end{array}$$

The constructed tableau is closed and so $\vdash_p [\Delta]$.

If $\phi^+ \equiv \phi_1 \vee \phi_2 * \in \Delta$ then, since $\models_p \bigwedge \Lambda_1 \to (\phi_1 \vee \phi_2) \vee \bigvee \Gamma_1$, we also have

$$\models_p \bigwedge \Lambda_1 \to \phi_1 \vee \phi_2 \vee \bigvee \Gamma_1 \ .$$

The associated sequence $\Delta_1, \phi_1 *, \phi_2 *$ has $n-1$ propositional connectives and so $\pi_1 \colon \vdash_p [\Delta_1, \phi_1 *, \phi_2 *]$ for some π_1 by IH. This is shown in the following on the left and the constructed tableau is shown on the right:

$$
\begin{array}{c}
\Delta_1 \\
\phi_1 * \\
\phi_2 * \\
\hline
\cdots \pi_1 \cdots
\end{array}
\quad \Rightarrow \quad
\begin{array}{cc}
\Delta & \\
\hline
\phi_1 * & (\vee_1 *) \\
\phi_2 * & (\vee_2 *) \\
\cdots \pi_1 \cdots &
\end{array}
$$

The constructed tableau is closed and so $\vdash_p [\Delta]$.

If $\phi^+ \equiv \phi_1 \to \phi_2 \in \Delta$ then, since $\models_p (\phi_1 \to \phi_2) \wedge \bigwedge \Lambda_1 \to \bigvee \Gamma_1$, we also have

$$\models_p \phi_2 \wedge \bigwedge \Lambda_1 \to \bigvee \Gamma_1 \text{ and } \models_p \bigwedge \Lambda_1 \to \phi_1 \vee \bigvee \Gamma_1 \ .$$

The sequences Δ_1, ϕ_2 and Δ_1, ϕ_1* have $n-1$ propositional connectives each and so $\pi_2 \colon \vdash_p [\Delta_1, \phi_2]$ and $\pi_1 \colon \vdash_p [\Delta_1, \phi_1*]$ for some π_2 and π_1 by two IH's. The two tableaux are shown on the left and the constructed tableau is shown on the right:

$$
\begin{array}{c}
\Delta_1 \\
\hline
\phi_2 \\
\cdots \pi_2 \cdots
\end{array}
\quad \text{and} \quad
\begin{array}{c}
\Delta_1 \\
\hline
\phi_1 * \\
\cdots \pi_1 \cdots
\end{array}
\quad \Rightarrow \quad
\begin{array}{ccc}
 & \Delta & \\
\hline
 & & (\to) \\
\phi_2 & & \phi_1 * \\
\cdots \pi_2 \cdots & & \cdots \pi_1 \cdots
\end{array}
$$

The constructed tableau is closed and so $\vdash_p [\Delta]$. The remaining cases are similar. □

3.2.7 Theorem (Soundness and completeness of propositional tableaux).

$$\vdash_p \phi \Leftrightarrow \models_p \phi \ .$$

Proof. We have $\vdash_p \phi$ iff by definition $\vdash_p [\phi*]$ iff by Lemmas 3.2.5 and 3.2.6 $\models_p \top \to \phi$ iff $\models_p \phi$. □

3.2.8 Falsification of open branches in propositional tableaux. A branch Δ of a propositional tableau π for $\phi*$ is *propositionally complete* if with every expansion rule with a premise in Δ the branch contains also at least one of its conclusions.

If a tableau for $\phi*$ does not close then it contains an open branch Δ and this can be clearly propositionally completed by finitely many expansions because the conclusions of expansion rules are formulas with a lesser number of propositional connectives than the premises.

For every propositionally complete and not closed branch Δ of a tableau for ϕ we can construct a propositional interpretation $\mathcal{I}$ by collecting all propositional atoms in assumptions:

$$\mathcal{I} = \{\psi \mid \psi \in \Delta \text{ and } \psi \text{ is a propositional atom}\} \ .$$

We prove by induction on the number of connectives in ψ that the following holds:

$$(\psi \in \Delta \Rightarrow \mathcal{I} \models \psi) \text{ and } (\psi{*} \in \Delta \Rightarrow \mathcal{I} \not\models \psi)\ .$$

If ψ is a propositional atom then the claim holds directly from the definition of $\mathcal{I}$. If $\psi \equiv \neg\psi_1$ then if $\neg\psi_1 \in \Delta$ we have $\psi_1{*} \in \Delta$ because the branch is propositionally complete and so $\mathcal{I} \not\models \psi_1$ by IH, i.e. $\mathcal{I} \models \neg\psi_1$. The case $\neg\psi_1{*} \in \Delta$ is similar.

If $\psi \equiv \psi_1 \wedge \psi_2$ then if $\psi_1 \wedge \psi_2 \in \Delta$ we have $\psi_1, \psi_2 \in \Delta$ because of saturation and $\mathcal{I} \models \psi_1$, $\mathcal{I} \models \psi_2$ by two IH's. Hence $\mathcal{I} \models \psi_1 \wedge \psi_2$. If $\psi_1 \wedge \psi_2{*} \in \Delta$ then one of the subformulas is a goal in Δ, say $\psi_1{*} \in \Delta$. Thus $\mathcal{I} \not\models \psi_1$ by IH and hence $\mathcal{I} \not\models \psi_1 \wedge \psi_2$. The remaining cases for ψ are similar.

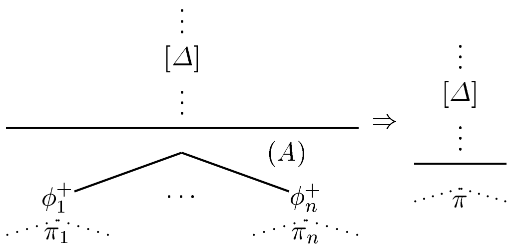
The goal $\phi{*}$ cannot be a tautology because we have $\mathcal{I} \not\models \phi$ by the just proved property.

3.3 Admissible Expansion Rules

3.3.1 Admissible expansion rules. We can often considerably shorten a tableau proof by the use of *admissible* expansion rules. Admissible rules can be reduced to the *basic* expansion rules, which are in the propositional case given in Par. 3.2.3), and so they do not add any strength to the proof system. Precisely, the n-ary expansion rule ($n \geq 1$)

$$\frac{\Delta}{\phi_1^+ \mid \cdots \mid \phi_n^+}\ (A)$$

is *admissible* if for all sequences of signed formulas Δ_1 s.t. $\Delta \subseteq \Delta_1$ and all tableaux $\pi_1, \ldots, \pi_n$ s.t. π_1: $\vdash_p [\Delta_1, \phi_1^+]$, …, π_n: $\vdash_p [\Delta_1, \phi_n^+]$ we can effectively construct a basic tableau π such that π: $\vdash_p [\Delta_1]$. The situation can be visualized as follows:



where we have indicated by $[\Delta]$ that the premises of A are in the branch above. An application of the admissible rule and the subsequent closure by tableaux $\pi_1, \ldots, \pi_n$ on the left can be effectively replaced by the tableau π.

The reader will note that we can permit in the tableau π also expansions by previously justified admissible rules of inference because they can be always replaced by basic inferences. After we have demonstrated the effective reduction of tableaux $\pi_1, \ldots, \pi_n$ to the tableau π we may freely use the admissible rule (A) as if it were a basic rule.

3.3.2 Theorem (Generalized flatten rules). *Following* generalized flatten *rules are admissible in propositional tableaux for any* $n \geq 2$ *and* $1 \leq i \leq n$*:*

$$\frac{\phi_1 \wedge \cdots \wedge \phi_i \wedge \cdots \wedge \phi_n}{\phi_i}\ (G\wedge_i)$$
$$\frac{\phi_1 \vee \cdots \vee \phi_i \vee \cdots \vee \phi_n *}{\phi_i *}\ (G\vee_i *)\ .$$

Proof. We prove the admissibility of the rule $(G\wedge_i)$ by induction on i; the admissibility of $(G\vee_i *)$ is proved similarly. In the base case when $i = 1$ there is nothing to prove as $(G\wedge_1)$ is the basic flatten rule $(\wedge_1)$. For $2 \leq i+1 \leq n$ we consider an expansion by the rule:

$$\begin{array}{c} \vdots \\ \phi_1 \wedge \phi_2 \wedge \cdots \wedge \phi_n \\ \vdots \\ \hline \phi_{i+1} \qquad (G\wedge_{i+1}) \\ \pi \end{array}$$

If $n = 2$ then this is the basic $(\wedge_2)$ rule and we are done. If $n > 2$ then we replace the rule $(G\wedge_{i+1})$ by the basic rule $(\wedge_2)$ followed by the $(G\wedge_i)$ rule which is admissible by IH. The new tableau is as follows:

$$\begin{array}{c} \vdots \\ \phi_1 \wedge \phi_2 \wedge \cdots \wedge \phi_n \\ \vdots \\ \hline \phi_2 \wedge \cdots \wedge \phi_n \qquad (\wedge_2) \\ \phi_{i+1} \qquad (G\wedge_i) \\ \pi \end{array}$$

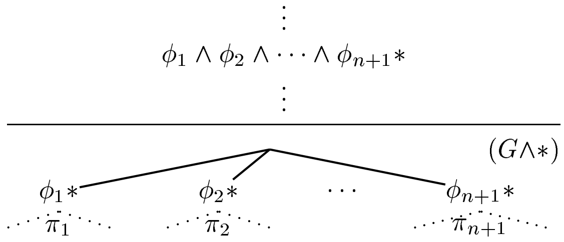
$\square$

3.3.3 Theorem (Generalized split rules). *The following generalizations of rules* $(\vee)$ *and* $(\wedge *)$ *are admissible in propositional tableaux for any* $n \geq 1$*:*

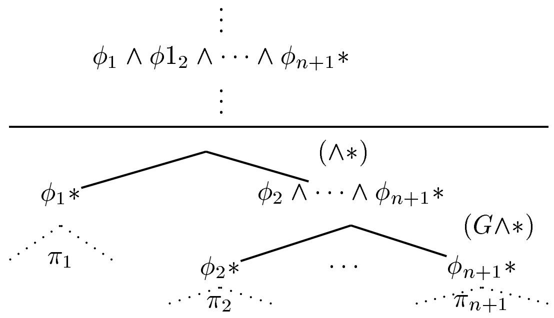
$$\frac{\phi_1 \vee \cdots \vee \phi_n}{\phi_1 \mid \cdots \mid \phi_n} \quad (G\vee)$$

$$\frac{\phi_1 \wedge \cdots \wedge \phi_n *}{\phi_1 * \mid \cdots \mid \phi_n *} \quad (G\wedge *)$$

Proof. We prove here only $(G\wedge *)$ by induction on n. In the base case when $n = 1$ there is nothing to prove as $(G\wedge *)$ is the basic split rule $(\wedge)$. In the inductive case when $n + 1 \geq 2$ we consider an expansion by the rule:



We replace the rule $(G\wedge *)$ by $(\wedge *)$ followed on the right by an n-ary $(G\wedge *)$ rule which is admissible by IH. The new tableau is as follows:



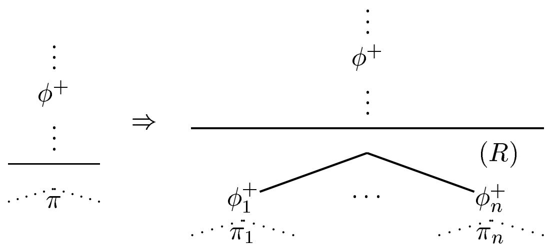
□

3.3.4 Inversion of expansion rules. Let

$$\frac{\phi^+}{\phi_1^+ \mid \cdots \mid \phi_n^+} \quad (R)$$

be an expansion rule with $n \geq 1$. The rule R can be an inversion or split rule as well as an identity or quantifier rule which will be introduced later. We say that the rule (R) is *invertible* if for every sequence of signed formulas Δ such that $\pi : \vdash_p [\Delta, \phi^+]$ there are tableaux π_i for $1 \leq i \leq n$ such that

$\pi_i : \vdash_p [\Delta, \phi_i^+]$. Moreover the rule (R) is not applied with ϕ^+ as a premise, and the formula ϕ^+ is not used for the closing of a branch, in neither of tableaux π_i. The inversion of the rule R can be visualized as follows:

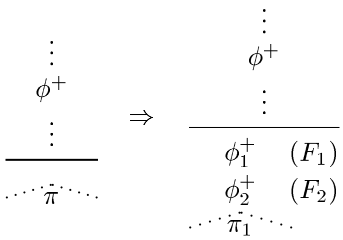


where we can in effect assume that the first expansion in the closed tableau on the right is by the rule (R) and that the premise ϕ^+ is used only once as indicated. This also means that the premise ϕ^+ is not used to close a branch.

Propositional flatten rules have the following schematic form:

$$\frac{\phi^+}{\phi_1^+}\,(F_1) \qquad \frac{\phi^+}{\phi_2^+}\,(F_2)\ .$$

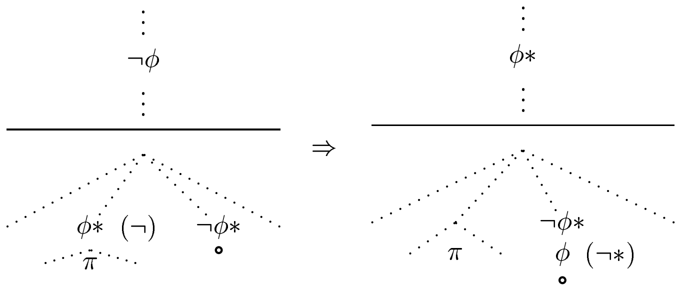
We say that the flatten rules (F_1) and (F_2) are *invertible* if from $\pi\colon \vdash_p [\Delta, \phi^+]$ we can form a tableau π_1 such that $\pi_1\colon \vdash_p [\Delta, \phi_1^+, \phi_2^+]$ where the rules (F_1) and (F_2) are not used in π_1 with ϕ^+ as a premise and neither is the formula ϕ^+ used for closing of a branch. The inversion can be visualized as follows:



where we can in effect assume that the first two expansions in the closed tableau on the right are by the rules (F_1) and (F_2) and that the premise ϕ^+ is used only once as indicated. This also means that the premise ϕ^+ is not used to close a branch.

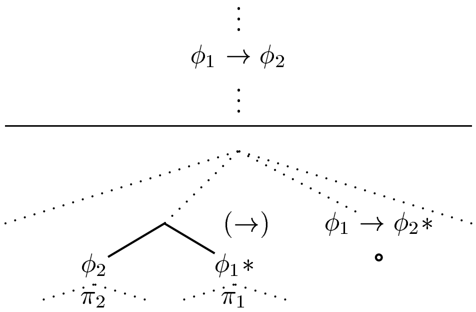
3.3.5 Inversion theorem. *Inversion, split, and flatten rules are invertible in propositional tableaux.*

Proof. The following diagram illustrates the inversion of a $(\neg)$ inversion rule:

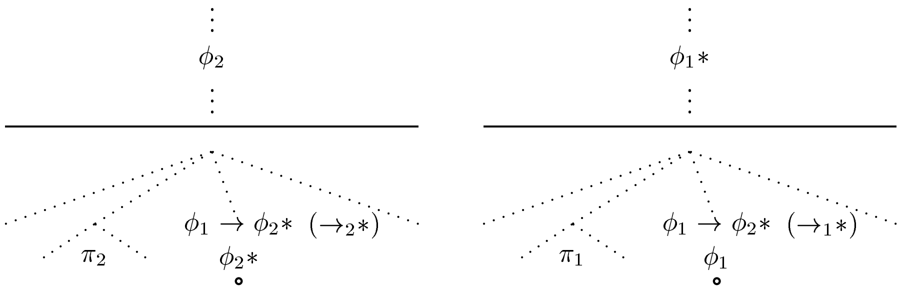


The closed tableau on the left shows just two of possibly many uses of the premise $\neg\phi$. The first one uses the premise in a $(\neg)$ rule and the second one closes the branch with $\neg\phi*$. The closed tableau on the right shows the inversion where the first used formula has been removed (because it is now in the top sequence) and the second one is now used as a premise of a $(\neg*)$ rule after which the branch closes. The two indicated transformations should be applied to all uses of the premise $\neg\phi$. The inversion of $\neg*$ inversion rules is similar.

The following diagram shows a closed tableau before the inversion of a $(\rightarrow)$ split rule:

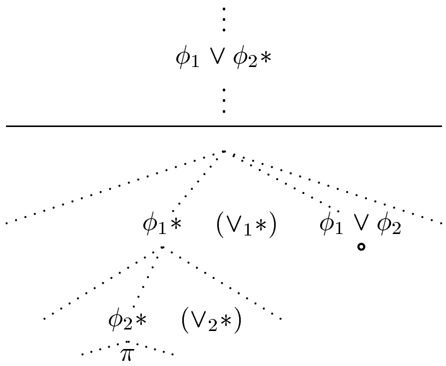


We have indicated two possible uses of the premise $\phi_1 \rightarrow \phi_2$. The first use is in a $(\rightarrow)$ rule and the second use is in the closure of a branch. We form the two inverted tableux as follows:

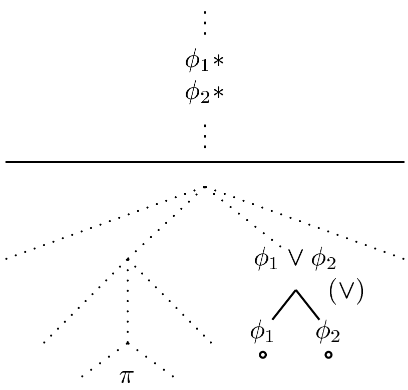


The expansions by the $(\to)$ rule have been replaced in the inverted tableau by tableaux π_2 and π_1 respectively and the closing formulas $\phi_1 \to \phi_2*$ have been expanded by the corresponding flatten rules after which the branches close. The inversion of other split rules is similar.

The following diagram shows a tableau before the inversion of a $(\vee_i*)$ flatten rules:



We have indicated three possible uses of the premise $\phi_1 \vee \phi_2*$. The first use is in a $(\vee_1*)$ rule after which there is a use in a $(\vee_2*)$ rule and third use is in the closure of a branch. We form the closed inverted tableau as follows:



In the inverted tableau the expansions by the $(\vee_i)$ rules have been removed and the closing formulas $\phi_1 \vee \phi_2$ have been expanded by $(\vee)$ split rules after which the branches close. The inversion of other flatten rules is similar. $\square$

3.3.6 Cut rules. For any formula π the following is a *cut rule on* ϕ:

$$\frac{}{\phi \mid \phi*} \quad (C)\ .$$

That cut rules are admissible in propositional tableaux, i.e. that

$$\pi_1\colon \vdash_p [\Delta, \phi] \text{ and } \pi_2\colon \vdash_p [\Delta, \phi*] \Rightarrow \vdash_p [\Delta]\ .$$

holds can be proved by the following semantic argument. Assume $\pi_1\colon \vdash_p [\Delta, \phi]$ and $\pi_2\colon \vdash_p [\Delta, \phi*]$ and let $\bigwedge\Lambda \to \bigvee\Gamma$ be a sequent associated with Δ. By the Soundness lemma (3.2.5) we have $\vDash_p \phi \wedge \bigwedge\Lambda \to \bigvee\Gamma$ and $\vDash_p \bigwedge\Lambda \to \phi \vee \bigvee\Gamma$. By the truth table method we can see that also

$$\vDash_p (\phi \wedge \bigwedge\Lambda \to \bigvee\Gamma) \wedge (\bigwedge\Lambda \to \phi \vee \bigvee\Gamma) \to \bigwedge\Lambda \to \bigvee\Gamma$$

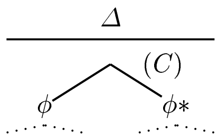
holds and hence $\vDash_p \bigwedge\Lambda \to \bigvee\Gamma$. By the Completeness lemma (3.2.6) we then get $\vdash_p [\Delta]$.

Unfortunately, this argument, which depends on the soundness and completeness of propositional tableaux, cannot be extended to tableaux with quantifier rules without first proving the soundness and completeness theorem for such tableaux. Our intention is to reduce the quantificational logic to the propositional logic and to obtain the soundness and completeness of quantificational tableaux through the reduction and so the above semantical argument proving the admissibility of cut rules cannot be used.

We will now prove the admissibility of cuts by a syntactic (proof-theoretic) argument in a way which extends to the quantificational case.

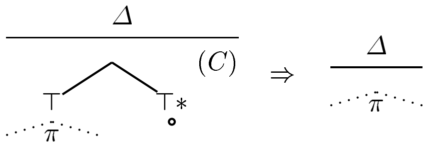
3.3.7 Lemma (Admissibility of cuts on propositional formulas). *If the cut rules on all propositional atoms in a formula ϕ are admissible in propositional tableaux then also the cut rule on ϕ is admissible.*

Proof. Assume that the cuts on the propositional atoms in $FPA(\phi)$ are admissible and prove by induction on the structure of ϕ that the cut on ϕ is admissible. We perform the case analysis of ϕ used in a cut as follows:



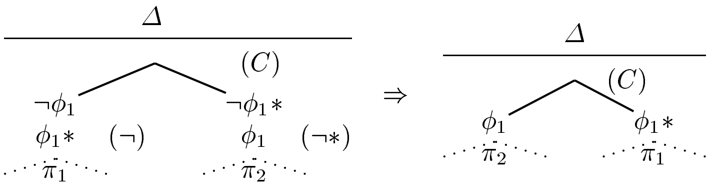
If ϕ is a propositional atom then the cut on ϕ is admissible from the assumption.

If $\phi \equiv \top$ then the expansion by the cut on $\top$ is shown in the following on the left:



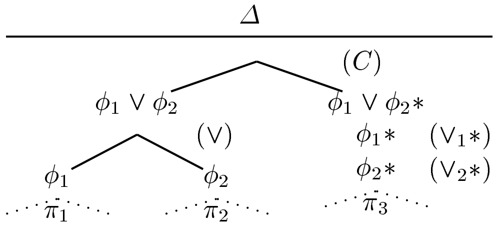
The assumption $\top$ is not used for anything in π and so the tableau π for Δ is closed as shown on the right. The case $\phi \equiv \bot$ is similar.

If $\phi \equiv \neg\phi_1$ then the expansion by the cut on $\neg\phi_1$ is shown in the following on the left:

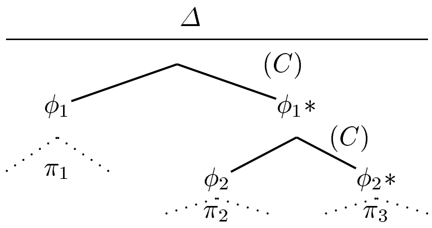


where we may assume without loss of generality that both inversion rules have been inverted. As a consequence the assumption $\neg\phi_1$ is not used for anything in π_1 and the goal $\neg\phi_1*$ is not used in π_2. We transform the tableau as shown on the right where the cut on $\neg\phi_1$ has been removed and the inversion rules replaced by a cut on ϕ_1 which is admissible by IH.

If $\phi \equiv \phi_1 \vee \phi_2$ then the expansion by the cut on $\phi_1 \vee \phi_2$ is as follows:



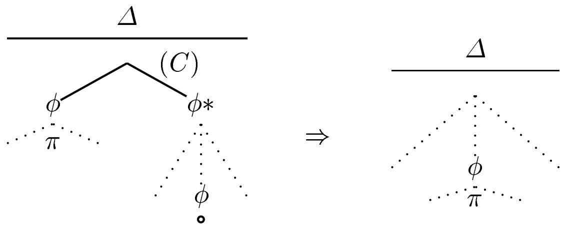
where we may assume without loss of generality that the $(\vee)$ split rule on the left and the $(\vee_i*)$ flatten rules on the right have been inverted. As a consequence the assumption $\phi_1 \vee \phi_2$ is not used for anything in π_1 and π_2 and the goal $\phi_1 \vee \phi_2*$ is not used in π_3. We transform the tableau as follows:



where the formula ϕ has been removed and the disjunctive rules replaced by two cuts on ϕ_1 and ϕ_2 respectively which are admissible by IH. The cases when the main propositional connective of ϕ is $\wedge$, $\rightarrow$, or $\leftrightarrow$ are similar. $\square$

3.3.8 Lemma (Admissibility of cut rules on propositional atoms). *Cut rules on propositional atoms are admissible in propositional tableaux.*

Proof. Consider a closed propositional tableaux with a cut on a propositional atom ϕ shown in the following on the left:



We have shown in the tableau for $\Delta, \phi*$ one of possibly many branches closed on the pair of propositional atoms $\phi, \phi*$. Because the goal $\phi*$ cannot be used in propositional tableaux for anything else we can form a closed tableau for Δ shown on the right where we perform the indicated transformation for all branches closed on $\phi, \phi*$. $\square$

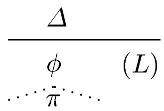
3.3.9 Theorem (Admissibility of cuts). *Cut rules are admissible in propositional tableaux on arbitrary formulas.*

Proof. This is a direct consequence of Lemmas 3.3.7 and 3.3.8. $\square$

3.3.10 Theorem (Lemma rule). *If $\vdash_p \phi$ then the following unary* lemma *rule*

$$\frac{}{\phi} \quad (L)$$

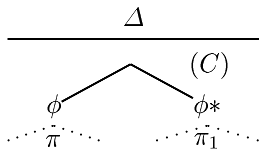
is admissible in propositional tableaux, i.e. for any closed propositional tableau for Δ such that



(1)

we have $\vdash_p [\Delta]$.

Proof. Assume $\pi_1 \colon \vdash_p \phi$ and that the tableau (1) is closed and form the following closed tableau witnessing $\vdash_p [\Delta]$:



$\square$

3.4 Tautological Consequence

Important extension of the notion of tautology is the notion of *tautological consequence* where we ask whether a formula ϕ follows from a finite or infinite set of formulas T by the laws of propositional logic alone.

3.4.1 Tautological consequence. Fix a language $\mathcal{L}$ and let T be a set of formulas from $\mathcal{L}$. We define the relation *formula ϕ is a tautological consequence of T*, in symbols $T \models_p \phi$ as follows:

$$T \models_p \phi \Leftrightarrow (\mathcal{I} \models T \Rightarrow \mathcal{I} \models \phi) \text{ for all propositional interpretations } \mathcal{I}.$$

From this we can see that for $T = \emptyset$ we have $\emptyset \models_p \phi \Leftrightarrow \models_p \phi$.

Tautological consequence is a generalization of implication where we so to speak permit infinite many formulas in antecedent. If T is finite then we have $T \models_p \phi \Leftrightarrow \models_p \bigwedge T \to \phi$ by Lemma 3.4.2. If the set T is infinite then it can contain infinitely many propositional atoms and we cannot replace infinite propositional interpretations by finite ones as we did in the truth table method. Thus it seems that that the testing of $T \models_p \phi$ is a hard problem having to do with quantification over uncountably many propositional interpretations. Fortunately, this kind of quantification can be replaced by existential quantification over countably many finite sets of formulas. This is a consequence of the fundamental theorem 3.4.4.

3.4.2 Semantic deduction lemma. *For every finite set S of formulas we have:*

$$S \models_p \phi \Leftrightarrow \models_p \bigwedge S \to \phi \ .$$

Proof. We have $\mathcal{I} \models S$ iff $\mathcal{I} \models \psi$ for all $\psi \in S$ iff $\mathcal{I} \models \bigwedge S$. Thus $S \models_p \phi$ iff $\mathcal{I} \models S \Rightarrow \mathcal{I} \models_p \phi$ for all $\mathcal{I}$ iff $\mathcal{I} \models \bigwedge S \Rightarrow \mathcal{I} \models_p \phi$ for all $\mathcal{I}$ iff $\models_p \bigwedge S \to \phi$. □

3.4.3 Semantic weakening lemma. *If $S \subseteq T$ then*

$$S \models_p \phi \Rightarrow T \models_p \phi \ .$$

Proof. Assume $S \models_p \phi$ and take any propositional interpretation such that $\mathcal{I} \models T$ holds. Since this means $\mathcal{I} \models \phi$ for all $\phi \in T$ we also have $\mathcal{I} \models S$ and thus $\mathcal{I} \models \phi$ from the assumption. □

3.4.4 Compactness theorem.

$$T \models_p \phi \Rightarrow S \models_p \phi \text{ for a finite } S \subseteq T.$$

Proof. Assume $T \models_p \phi$. T is a set of formulas of a first order language $\mathcal{L}$ which has countably many formulas. Thus the set T is at most countable and we can write it in a form $T = \bigcup_{i \in N} S_i$ where each of the sets S_i is finite and we have $S_0 = \emptyset$ and $S_i \subseteq S_{i+1}$ (This is trivial if T is finite; otherwise, for instance, enumerate T and define S_i to be the set of the first i formulas in the enumeration).

We assign by the function $W(\mathcal{I})$ to every propositional interpretation $\mathcal{I}$ one of the finite sets S_i by:

$$W(\mathcal{I}) = S_i \quad \text{where } i \text{ is the least such that } \mathcal{I} \models S_i \Rightarrow \mathcal{I} \models \phi.$$

This is a legal definition because if $\mathcal{I} \models \phi$ then we have $\mathcal{I} \models S_0 \Rightarrow \mathcal{I} \models \phi$ and if $\mathcal{I} \not\models \phi$ then we have $\mathcal{I} \not\models T$. Thus $\mathcal{I} \not\models \psi$ for some $\psi \in T$ and, since then $\psi \in S_i$ for some i, we have $\mathcal{I} \not\models S_i$ for some i and there is a least such i. Define the set S to satisfy:

$$S := \bigcup \{W(\mathcal{I}) \mid \mathcal{I} \text{ is a propositional interpretation.}\}$$

We clearly have $S \subseteq T$. We also have $S \models_p \phi$ because for any propositional interpretation $\mathcal{I}$ such that $\mathcal{I} \models S$ we have $W(\mathcal{I}) \subseteq S$ and so $\mathcal{I} \models W(\mathcal{I})$. We then obtain $\mathcal{I} \models \phi$ from the definition of $W(\mathcal{I})$. Thus the theorem will be proved if we demonstrate by an indirect proof that the set S is finite.

So suppose that S is infinite. We will construct an increasing chain of propositional interpretations $\mathcal{I}_i$ in which the infiniteness of S will be propagated. Enumerate towards that end all propositional atoms of $\mathcal{L}$ in an infinite sequence $\psi_1, \psi_2, \psi_3, \ldots$ and define the finite sets of propositional atoms A_i for $i \in \mathbb{N}$ by

$$A_i = \bigcup_{1 \le j \le i} \{\psi_j\} .$$

Note that $A_0 = \emptyset$. Define an infinite sequence $\{\mathcal{I}_i\}_{i \in \mathbb{N}}$ of finite propositional interpretations $\mathcal{I}_i$ to satisfy:

$$\mathcal{I}_0 = \emptyset$$
$$\mathcal{I}_{i+1} = \begin{cases} \mathcal{I}_i & \text{if } \bigcup \{W(\mathcal{I}) \mid \mathcal{I} \cap A_{i+1} = \mathcal{I}_i\} \text{ is infinite} \\ \mathcal{I}_i \cup \{\psi_{i+1}\} & \text{otherwise.} \end{cases}$$

We clearly have $\mathcal{I}_i \subseteq \mathcal{I}_{i+1}$. Define the sets I_i for $i \in \mathbb{N}$ to satisfy:

$$I_i = \bigcup \{W(\mathcal{I}) \mid \mathcal{I} \cap A_i = \mathcal{I}_i\}$$

and prove by induction on i:

$$M_i \subseteq A_i \text{ and } I_i \text{ is infinite.}$$

In the base case we have $\mathcal{I}_0 = \emptyset = A_0$ and the set

$$I_0 = \bigcup\{W(\mathcal{I}) \mid \mathcal{I} \cap A_0 = \mathcal{I}_0\} = \bigcup\{W(\mathcal{I}) \mid \emptyset = \emptyset\} = S\ .$$

is infinite. In the inductive case we have

$$\mathcal{I}_{i+1} \subseteq \mathcal{I}_i \cup \{\psi_{i+1}\} \overset{\text{IH}}{\subseteq} A_i \cup \{\psi_{i+1}\} = A_{i+1}\ .$$

We note that if $\mathcal{I} \cap A_i = \mathcal{I}_i$ then

$$\begin{aligned}\mathcal{I} \cap A_{i+1} =& \mathcal{I} \cap (A_i \cup \{\psi_{i+1}\}) = (\mathcal{I} \cap A_i) \cup (\mathcal{I} \cap \{\psi_{i+1}\}) = \\ & \mathcal{I}_i \cup (\mathcal{I} \cap \{\psi_{i+1}\}) = \begin{cases}\mathcal{I}_i & \text{if } \psi_{i+1} \notin \mathcal{I} \\ \mathcal{I}_i \cup \{\psi_{i+1}\} & \text{if } \psi_{i+1} \in \mathcal{I}\end{cases}\end{aligned}$$

and so

$$\begin{aligned}I_n =& \bigcup\{W(\mathcal{I}) \mid \mathcal{I} \cap A_i = \mathcal{I}_i\} = \\ & \bigcup\{W(\mathcal{I}) \mid \mathcal{I} \cap A_{i+1} = \mathcal{I}_i\} \cup \bigcup\{W(\mathcal{I}) \mid \mathcal{I} \cap A_{i+1} = \mathcal{I}_i \cup \{\psi_{i+1}\}\}\ .\end{aligned}$$

One of the two sets on the right must be infinite because I_n is by IH. We consider two cases. If the first set is infinite then $\mathcal{I}_{i+1} = \mathcal{I}_i$ by definition and the first set is I_{n+1}. If the first set is finite then $\mathcal{I}_{i+1} = \mathcal{I}_i \cup \{\psi_{i+1}\}$ and so the second set, which must be infinite, is I_{n+1}. Thus in both cases I_{n+1} is an infinite set.

We construct a propositional interpretation $\mathcal{I} = \bigcup\{\mathcal{I}_i \mid i \in \mathbb{N}\}$ and we have $W(\mathcal{I}) = S_k$ for the least k such that $\mathcal{I} \vDash S_k \Rightarrow \mathcal{I} \vDash \phi$. Let i be the least number such that $\mathit{FPA}(S_k \cup \{\phi\}) \subseteq A_i$ and let $\mathcal{J}$ be any propositional interpretation such that $\mathcal{J} \cap A_i = \mathcal{I}_i$. We have

$$\begin{aligned}\mathcal{J}^{S_k \cup \{\phi\}} =& \mathcal{J} \cap \mathit{FPA}(S_k \cup \{\phi\}) = \mathcal{J} \cap A_i \cap \mathit{FPA}(S_k \cup \{\phi\}) = \\ & \mathcal{I}_i \cap \mathit{FPA}(S_k \cup \{\phi\}) = \mathcal{I}_i^{S_k \cup \{\phi\}}\end{aligned}$$

and so $\mathcal{J}$ and $\mathcal{I}_i$ are $S_k \cup \{\phi\}$-equivalent by the Equivalence lemma (see 3.1.5). From this we get $W(\mathcal{J}) = W(\mathcal{I}_i)$ and hence

$$I_i = \bigcup\{W(\mathcal{J}) \mid \mathcal{J} \cap A_i = \mathcal{I}_i\} = \bigcup\{W(\mathcal{I}_i) \mid \mathcal{J} \cap A_i = \mathcal{I}_i\} = W(\mathcal{I}_i)$$

which is a contradiction because the set $W(\mathcal{I}_i)$ is finite (the set is actually equal to S_k). □

3.4.5 Corollary (Tautological reduction).

$$T \vDash_p \phi \Leftrightarrow\ \vDash_p \bigwedge S \to \phi$$

for a finite subset S of T.

Proof. From $T \vDash_p \phi$ we obtain $S \vDash_p \phi$ for a finite subset S of T by Thm. 3.4.4. The opposite direction follows from Lemma 3.4.3 and we have $S \vDash_p \phi$ iff $\vDash_p \bigwedge S \to \phi$ by Lemma 3.4.2. □

3.4.6 Remark. The reader familiar with set theory will recognize the construction of the sequence $\{\mathcal{I}_i\}_{i\mathbb{N}}$ in the proof of the Compactness theorem as the construction of an infinite branch of an infinite tree with finitely branching nodes in the proof of the König's lemma. The lemma says that in every finitely branching tree with an infinite number of nodes there is an infinite branch.

3.4.7 Semidecidability of tautological consequence. Let $\mathcal{L}$ be a language and T an infinite decidable set of its formulas. We have noted in Par. 3.4.1 that in order to decide the unary relation ϕ *is a tautological consequence of* T, i.e. $T \vDash_p \phi$, one would expect to test $\mathcal{I} \vDash T \Rightarrow \mathcal{I} \vDash \phi$ for uncountably many propositional interpretations $\mathcal{I}$. By the Compactness theorem and Lemma 3.4.3 we however know that it is sufficient to decide whether $S \vDash_p \phi$ holds for a finite subset S of T. As there are countably many finite subsets S of the countable T we have to test by Lemma 3.4.2 countably many times whether $\bigwedge S \to \phi$ is a tautology.

One of the ways to organize the tests is as follows. We encode all formulas of $\mathcal{L}$ into $\mathbb{N}$. Starting from 0 we then successively test for all natural numbers i whether i is a list such that for every $j \in i$ (there are finitely many such j's) the number j codes a formula ϕ (this can be effectively done). If so, then we test whether $\phi \in T$. If this holds for all $j \in i$ we can effectively form the finite set S of all formulas of $\mathcal{L}$ coded by i. We then test whether $\bigwedge S \to \phi$ is a tautology. If this is the case we stop the testing and we know that ϕ is a tautological consequence of T. If not then we have to continue with the next number $i+1$ and if ϕ is not a tautological consequence then by Lemmas 3.4.3 and 3.4.2 there is no finite $S \subset T$ such that $\bigwedge S \to \phi$ is a tautology and we will never discover the fact.

Predicates $P(x)$ such that if there is an x satisfying P we can effectively find it but we go on searching forever if for all x not $P(x)$ are called *semidecidable* predicates. It can be shown by the methods of recursion theory that the unary predicate $T \vDash_p \phi$ is semidecidable and that the above described method of crude search cannot be improved upon. Later in this text we will show how to reduce the general questions of logical validity of formulas and of logical consequence to the questions of tautological consequence from decidable sets. This will mean that the best we can do in first order logic is to find a proof of a formula from given axioms if there is one. If the formula is unprovable we might never discover it.

3.5 Tableaux with Axioms

3.5.1 Axiom rules. Fix a language $\mathcal{L}$. We now extend propositional tableaux so we can prove that ϕ is a tautological consequence of a decidable set T of formulas $\mathcal{L}$. For every $\psi \in T$ we add a unary *axiom rule*:

$$\frac{}{\psi}\quad (Ax)$$

which means that we can extend a branch of a tableau at an arbitrary position with the assumption ψ. Note that the decidability of T is crucial for this because we can use the axiom rule only if $\psi \in T$. Without decidability we would not be able to recognize whether a given tree of signed formulas is a legal tableau or not.

3.5.2 Proofs with propositional tableaux with axioms. A propositional tableau π for a sequence of signed formulas Δ which possibly uses axiom rules from T is a *propositional tableau for Δ from axioms T*. If π is closed then we assert this by writing $\pi : T \vdash_p [\Delta]$. Note that if $T = \emptyset$ then we have $\pi : \emptyset \vdash_p [\Delta] \Leftrightarrow \pi\!: \vdash_p [\Delta]$. When $\Delta \equiv \phi*$ then we say that π *propositionally proves ϕ from axioms* T and write it as $\pi : T \vdash_p \phi$. We use abbreviations similar to those discussed in Par. 3.2.4 also for the proofs from axioms.

3.5.3 Theorem (Admissible expansion rules in propositional tableaux with axioms). *All rules proved admissible for propositional tableaux in Sect. 3.3 are also admissible in propositional tableaux with axioms.*

Proof. Inspection of the proofs of admissibility of expansion rules in Sect. 3.3 reveals that the proofs remain correct also for tableaux with axiom rules because their presence does not affect the proofs of admissibility. □

3.5.4 Syntactic weakening lemma. *If $S \subseteq T$ then*

$$S \vdash_p \phi \Rightarrow T \vdash_p \phi \; .$$

Proof. Assume $\pi : S \vdash_p \phi$. Every every axiom rule for $\psi \in S$ used in π is also an axiom rule for $\psi \in T$ and so $\pi : T \vdash_p \phi$. □

3.5.5 Theorem on syntactic compactness.

$$T \vdash_p \phi \Rightarrow S \vdash_p \phi \text{ for a finite } S \subseteq T.$$

Proof. Assume $\pi : T \vdash_p \phi$ and construct the finite set S to consist of all conclusions ψ of axiom rules for $\psi \in T$ used in the tableau π. The same rules are axiom rules for $\psi \in S$ and so $\pi : S \vdash_p \phi$. □

3.5.6 Deduction theorem. For a finite set of formulas S:

$$S \vdash_p \phi \Leftrightarrow \; \vdash_p \bigwedge S \to \phi \; .$$

Proof. Let $S = \{\psi_1, \ldots, \psi_n\}$. In the direction $(\Rightarrow)$ assume $\pi : S \vdash_p \phi$, i.e. $\pi : S \vdash_p [\phi*]$. If $n = 0$ then $\bigwedge S \equiv \top$ and we derive $\vdash_p \top \to \phi$ as follows:

$$\begin{array}{c}
\top \rightarrow \phi* \\
\hline
\phi* \quad (\rightarrow_2 *) \\
\cdots\pi\cdots
\end{array}$$

If $n > 0$ then denote by π_1 the tableau formed from π by deleting all expansions by axiom rules. We clearly have $\pi_1 \colon \vdash_p [\phi*, \psi_1, \ldots, \psi_n]$. which is shown in the following on the left:

$$\begin{array}{c}
\phi* \\
\psi_1 \\
\vdots \\
\psi_n \\
\hline
\cdots\pi_1\cdots
\end{array}
\quad \Rightarrow \quad
\begin{array}{cc}
\psi_1 \wedge \cdots \wedge \psi_n \rightarrow \phi* & \\
\hline
\phi* & (\rightarrow_2 *) \\
\psi_1 \wedge \cdots \wedge \psi_n & (\rightarrow_1 *) \\
\psi_1 & (G\wedge_1) \\
\vdots & \\
\psi_n & (G\wedge_n) \\
\cdots\pi_1\cdots &
\end{array}$$

We form the closed tableau on the right which is expanded with the help of the generalized flatten rules (see Thm. 3.3.2) and so $\vdash_p \bigwedge S \rightarrow \phi$.

In the direction ($\Leftarrow$) assume $\pi \colon \vdash_p [\psi_1 \wedge \cdots \wedge \psi_n \rightarrow \phi*]$. We can assume by inversion that the first two expansions in π are by $(\rightarrow_i *)$ flatten rules such that the goal $\bigwedge S \rightarrow \phi*$ is not used in π_1. If $n = 0$ then the situation is shown on the left:

$$\begin{array}{cc}
\top \rightarrow \phi* & \\
\hline
\phi* & (\rightarrow_2 *) \\
\top & (\rightarrow_1 *) \\
\cdots\pi_1\cdots &
\end{array}
\quad \Rightarrow \quad
\begin{array}{c}
\phi* \\
\hline
\cdots\pi_1\cdots
\end{array}$$

and we can form a closed tableau π for $\phi*$ because the assumption $\top$ cannot be used in π_1. If $n > 0$ then we can assume that the inversion of $(\rightarrow_i *)$ flatten rules is followed by by $n-1$ inversions of $(\wedge)$ flatten rules which is shown in the following on the left:

$$\begin{array}{cc}
\psi_1 \wedge \cdots \wedge \psi_n \rightarrow \phi* & \\
\hline
\phi* & (\rightarrow_2 *) \\
\psi_1 \wedge \cdots \wedge \psi_n & (\rightarrow_1 *) \\
\psi_1 & (\wedge_1) \\
\psi_2 \wedge \cdots \wedge \psi_n & (\wedge_2 *) \\
\vdots & \\
\psi_n & (\wedge_2) \\
\cdots\pi_1\cdots &
\end{array}
\quad \Rightarrow \quad
\begin{array}{cc}
\phi* & \\
\hline
\psi_1 & (Ax) \\
\cdots & \\
\psi_n & (Ax) \\
\cdots\pi_1\cdots &
\end{array}$$

We form the closed tableau on the right which is expanded with the help of axiom rules from S and in which we have omitted the assumptions $\psi_i \wedge \cdots \wedge \psi_n$ for $1 \leq i < n$ because they cannot be used in π_1. We thus have $S \vdash_p \phi$. $\square$

3.5.7 Theorem (Introduction/elimination of axioms).

$$T \vdash_p \phi \Leftrightarrow \vdash_p \bigwedge S \to \phi$$

for a finite subset S of T.

Proof. From $T \vdash_p \phi$ we obtain $S \vdash_p \phi$ for a finite subset S of T by Thm. 3.5.5. The opposite direction follows from Lemma 3.5.4 and we have $S \vdash_p \phi$ iff $\vdash_p \bigwedge S \to \phi$ by Thm. 3.5.6. □

3.5.8 Corollary (Soundness and completeness of propositional tableaux). *For any fromula ϕ and set of formulas T there is in each direction a finite subset S of T such that the following holds:*

$$\begin{array}{ccc}
T \models_p \phi & & T \vdash_p \phi \\
\Uparrow 3.4.3 \Downarrow 3.4.4 & & \Uparrow 3.5.4 \Downarrow 3.5.5 \\
S \models_p \phi & & S \vdash_p \phi \\
\Uparrow\!\Downarrow 3.4.2 & & \Uparrow\!\Downarrow 3.5.6 \\
\models_p \bigwedge S \to \phi & \Leftarrow 3.2.5 \Rightarrow 3.2.6 & \vdash_p \bigwedge S \to \phi
\end{array}$$

□

3.5.9 Semidecidability of tautological consequence revisited. One of the consequences of the Corollary 3.5.8 is that we can semidecide the relation $T \models_p \phi$ by tableaux instead of testing for tautologies as outlined in Par. 3.4.7. We do this by constructing possibly infinite branches which are *axiomatically complete*, i.e. which apply the axiom rules for all axioms from T.

In order to decide the relation $T \models_p \phi$ we enumerate the axioms of T into a sequence $\psi_1, \psi_2, \ldots$, and construct a propositional tableau for the goal $\phi*$. We select an open propositionally complete branch of it (if any) and we extend it by an axiom rule by taking ψ_1 into assumptions. We then construct a propositional tableau under the assumption. We select a not closed propositionally complete branch again (if any) and expand it with the axiom rule for ψ_2. We continue in this way in the hope of closing the branch. If this happens we apply the same procedure of systematically applying one axiom after another to the remaining open branches. If all branches close then $T \models_p \phi$ holds.

Otherwise, if T is finite we stop with at least one open branch Δ which is both propositionally and axiomatically complete. The branch is finite. If T is infinite we will go on extending a branch forever because there is at least one infinite branch which is open and propositionally and axiomatically complete.

In both cases there is a propositional interpretation $\mathcal{I}$ constructed by collecting all propositional atoms in the assumptions. We have proved in Par. 3.2.8 that we have $\mathcal{I} \not\models \phi$ and $\mathcal{I} \models \phi_1$ for every assumption ϕ_1 in the branch. Since the branch contains all axioms T as assumptions we have in particular $\mathcal{I} \models T$. But this means that we have $T \not\models_p \phi$. Note that we can effectively determine this fact only when T is finite.

4. Identity Logic

In this chapter we investigate formulas always true on the strength of propositional logic and of properties of identity.

4.1 Some Syntactic Concepts

4.1.1 Free terms. *Free terms* of a set of formulas S of a language $\mathcal{L}$ are terms occurring outside of quantifiers in the formulas of S. This is made precise by a metamathematical function $FT(\alpha)$ defined on terms, formulas, and sets of formulas to yield the set of free terms of α. The function FT satisfies:

$$
\begin{aligned}
FT(x) &= \{x\} \\
FT(f(\tau_1,\ldots,\tau_n)) &= \{f(\tau_1,\ldots,\tau_n)\} \cup FT(\tau_1) \cup \ldots \cup FT(\tau_n) \\
FT(\tau_1 = \tau_2) &= FT(\tau_1) \cup FT(\tau_2) \\
FT(P(\tau_1,\ldots,\tau_n)) &= FT(\tau_1) \cup \ldots \cup FT(\tau_n) \\
FT(\forall x\phi) &= \emptyset \\
FT(\exists x\phi) &= \emptyset \\
FT(\top) &= \emptyset \\
FT(\bot) &= \emptyset \\
FT(\neg\phi) &= FT(\phi) \\
FT(\phi_1 \vee \phi_2) &= FT(\phi_1) \cup FT(\phi_2) \\
FT(\phi_1 \wedge \phi_2) &= FT(\phi_1) \cup FT(\phi_2) \\
FT(\phi_1 \to \phi_2) &= FT(\phi_1) \cup FT(\phi_2) \\
FT(\phi_1 \leftrightarrow \phi_2) &= FT(\phi_1) \cup FT(\phi_2) \\
FT(T) &= \bigcup\{FT(\phi) \mid \phi \in T\} \ .
\end{aligned}
$$

4.2 Quasitautological Consequence

4.2.1 Structures. A structure $\mathcal{M}$ for a language $\mathcal{L}$ is given by

1. a non-empty set D, called the *domain* of the structure,
2. for every n-ary function symbol f of $\mathcal{L}$ an n-ary function $f^{\mathcal{M}}$ over D, i.e. $f^{\mathcal{M}} : D^n \mapsto D$, called the *interpretation of* f,
3. for every n-ary predicate symbol P of $\mathcal{L}$ a subset $P^{\mathcal{M}}$ of D^n called the *interpretation of* P.

Here we define $D^0 = \{\emptyset\}$ and identify nullary functions over D with elements of D. Thus for every constant c of $\mathcal{L}$ we have $c^{\mathcal{M}} \in D$ and for every propositional constant P of $\mathcal{L}$ we have $P^{\mathcal{M}} \subseteq \{\emptyset\}$. We agree to identify the value $P^{\mathcal{M}} = \emptyset$ with falsehood and the value $P^{\mathcal{M}} = \{\emptyset\}$ with truth.

Structures are mathematical objects (triples of sets) whose purpose is to assign meaning to terms and formulas of $\mathcal{L}$. A structure $\mathcal{M}$ is *finite* if its domain D is a finite set and *infinite* otherwise. $\mathcal{M}$ is a *numeric* structure if its domain is a subset of natural numbers.

4.2.2 Assignments. For a structure $\mathcal{M}$ for $\mathcal{L}$ with the domain D we call a function a from $\mathbb{N}$ to D *assignment in* $\mathcal{M}$. The idea is that the assignment a assigns the value $a(i) \in D$ to the variable v_i.

4.2.3 Identity interpretations. An *identity interpretation* $\mathcal{I}$ *for* $\mathcal{L}$ is a triple $\langle Q, \mathcal{M}, a\rangle$ where Q, called the *quantifier set*, is a subset of quantifier formulas of $\mathcal{L}$, $\mathcal{M}$ is a structure for $\mathcal{L}$ and a is an assignment in $\mathcal{M}$. An identity $\mathcal{I}$ is *finite* if its structure is finite and *numeric* if its structure is numeric.

Identity interpretations uniquely determine the meaning of terms and formulas as shown in the following two paragraphs.

4.2.4 Denotation of terms. For a given identity interpretation $\mathcal{I} = \langle Q, \mathcal{M}, a\rangle$ for $\mathcal{L}$ with D the domain of $\mathcal{M}$ we assign to every term τ of $\mathcal{L}$ its *denotation*, designated as $\tau^{\mathcal{I}}$, to be the element of D satisfying the following:

$$\begin{aligned} v_i^{\mathcal{I}} &= a(i) \\ f(\tau_1, \ldots, \tau_n)^{\mathcal{I}} &= f^{\mathcal{M}}(\tau_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}}) \quad f \text{ is } n\text{-ary function symbol of } \mathcal{L}. \end{aligned}$$

If f is a constant symbol, i.e. a nullary function symbol, then we abbreviate $f^{\mathcal{M}}()$ to $f^{\mathcal{M}}$.

The identity interpretation $\mathcal{I}$ is *canonical* if it is a numeric interpretation and for every element d in the domain of its structure we have $d = \tau^{\mathcal{I}}$ for some term τ.

4.2.5 Satisfaction relation for identity interpretations. Let $\mathcal{I} = \langle Q, \mathcal{M}, a\rangle$ be an identity interpretation for $\mathcal{L}$. For every formula ϕ of $\mathcal{L}$ we define the unary relation $\mathcal{I} \vDash \phi$, read as $\mathcal{I}$ *satisfies* ϕ, to be similar to the satisfaction relation for propositional interpretations (see Par. 3.1.2) when ϕ is a propositional formula. If ϕ is a propositional atom then we define

$$
\begin{aligned}
\mathcal{I} \vDash \forall x\phi &\Leftrightarrow \forall x\phi \in Q \\
\mathcal{I} \vDash \exists x\phi &\Leftrightarrow \exists x\phi \in Q \\
\mathcal{I} \vDash \tau_1 = \tau_2 &\Leftrightarrow \tau_1^{\mathcal{I}} = \tau_2^{\mathcal{I}} \\
\mathcal{I} \vDash P(\tau_1, \ldots, \tau_n) &\Leftrightarrow \langle \tau_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}} \rangle \in P^{\mathcal{M}} \ .
\end{aligned}
$$

Here the 'zero-tuple' $\langle\rangle$ is defined as the empty set $\emptyset$. This means that for a propositional constant P we have $\mathcal{I} \vDash P$ iff $P^{\mathcal{M}} = \{\emptyset\}$. This should explain why we have identified the set $\{\emptyset\}$ with the truth.

Assignments in $\mathcal{I}$ are used only in atomic formulas which obtain the meaning from the interpretation of function and predicate symbols specified by the points (2) and (3) in Par. 4.2.1. Specifically, the meaning of identity $\tau_1 = \tau_2$ is determined as the identity of the denotations $\tau_1^{\mathcal{I}} = \tau_2^{\mathcal{I}}$. The reader will note that the symbol of identity in the formula $\tau_1 = \tau_2$ is just a symbol whereas the same symbol in $\tau_1^{\mathcal{I}} = \tau_2^{\mathcal{I}}$ stands for the relation of identity over the domain of $\mathcal{I}$. The meaning of quantifier formulas is determined from the quantifier set Q similarly as the meaning of propositional atoms is determined from propositional interpretations.

4.2.6 Lemma (Reduction to propositional interpretations). *To every identity interpretation $\mathcal{I}$ for $\mathcal{L}$ there is an equivalent propositional interpretation $\mathcal{J}$.*

Proof. Take an identity interpretation $\mathcal{I} = \langle Q, \mathcal{M}, a \rangle$ for $\mathcal{L}$. We construct the propositional interpretation $\mathcal{J}$ as follows:

$$\mathcal{J} = \{\psi \mid \mathcal{I} \vDash \psi \text{ for propositional atoms } \psi\} \ .$$

We prove the equivalence by induction on the construction of ϕ. If ϕ is a propositional atom then $\mathcal{J} \vDash \phi$ iff $\phi \in \mathcal{J}$ iff $\mathcal{I} \vDash \phi$. If $\phi \equiv \phi_1 \vee \phi_2$ then we have $\mathcal{J} \vDash \phi_1 \vee \phi_2$ iff $\mathcal{J} \vDash \phi_1$ or $\mathcal{J} \vDash \phi_2$ iff, by IH, $\mathcal{I} \vDash \phi_1$ or $\mathcal{I} \vDash \phi_2$ iff $\mathcal{I} \vDash \phi_1 \vee \phi_2$. The remaining cases are similar. □

4.2.7 Equality axioms. Let $\mathcal{L}$ be a first-order language. For all terms $\tau_1, \ldots, \tau_n, \rho_1, \ldots, \rho_n$ the following formulas, designated by *Eq*, are called *equality axioms for $\mathcal{L}$*:

$$\tau_1 = \tau_1 \tag{1}$$

$$\tau_1 = \tau_2 \rightarrow \tau_2 = \tau_1 \tag{2}$$

$$\tau_1 = \tau_2 \wedge \tau_2 = \tau_3 \rightarrow \tau_1 = \tau_3 \tag{3}$$

$$\begin{gathered}\tau_1 = \rho_1 \wedge \cdots \wedge \tau_n = \rho_n \rightarrow f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n) \\ f \text{ is } n\text{-ary function symbol, } n > 0\end{gathered} \tag{4}$$

$$\begin{gathered}\tau_1 = \rho_1 \wedge \cdots \wedge \tau_n = \rho_n \wedge P(\tau_1, \ldots, \tau_n) \rightarrow P(\rho_1, \ldots, \rho_n) \\ P \text{ is } n\text{-ary predicate symbol, } n > 0.\end{gathered} \tag{5}$$

Formulas (1) are axioms of *reflexivity*, (2) are axioms of *symmetry*, (3) are axioms of *transitivity*, (4) and (5) are axioms of *function* and *predicate substitution* respectively.

We designate by Eq^T the *restriction* of equality axioms to the free terms of a set of formulas T, i.e.:

$$Eq^T = \{\phi \mid \phi \in Eq \land FT(\phi) \subseteq FT(T)\} \ .$$

4.2.8 Lemma (Expansion of propositional interpretations). *To every set of formulas T of $\mathcal{L}$ and every propositional interpretation $\mathcal{I}$ for $\mathcal{L}$ such that $\mathcal{I} \models Eq^T$ there is a T-equivalent canonical identity interpretation $\mathcal{J}$. $\mathcal{J}$ is finite if the set $FT(T)$ is finite. Every element of the domain of the structure of $\mathcal{J}$ is denoted by a term of $FT(T)$ if the last set is not empty.*

Proof. Take any T and any propositional interpretation $\mathcal{I}$ such that $\mathcal{I} \models Eq^T$. We wish to define the identity interpretation $\mathcal{J} = \langle Q, \mathcal{M}, a\rangle$. We define the quantifier set Q as follows:

$$Q = \{\psi \mid \psi \text{ is a quantifier formula and } \psi \in \mathcal{I} \ .\}$$

We enumerate the set $\mathcal{T} = FT(T)$ by a possibly finite or even empty sequence:

$$\sigma_0, \sigma_1, \sigma_2, \ldots$$

Clearly, the sequence has as many elements as is the cardinality of $\mathcal{T}$. We define the domain D of the structure $\mathcal{M}$ with the help of a *representant* function r mapping the terms of $\mathcal{L}$ to $\mathbb{N}$ by

$$r(\tau) = \min\{i \mid \tau \in \mathcal{T} \Rightarrow \mathcal{I} \models \tau = \sigma_i\} \ .$$

This is a legal definition only if the argument set to min is non-empty for every τ. That this is so can be seen by considering two cases. If $\tau \notin \mathcal{T}$ then the argument to min is $\mathbb{N}$ and so $r(\tau) = 0$. If $\tau \in \mathcal{T}$ then we have $\tau \equiv \sigma_i$ for some i and, since the reflexivity axiom $\tau = \sigma_i$ is in Eq^T, we have $\mathcal{I} \models \tau = \sigma_i$. Hence the argument to min contains i. We now define the domain D of $\mathcal{J}$ as the range of the function r:

$$D = \{r(\tau) \mid \tau \text{ is a term of } \mathcal{L}\} \ .$$

We have $D \subseteq \mathbb{N}$ and if $\mathcal{T} = \emptyset$ then $D = \{0\}$. Otherwise $\sigma_0 \in \mathcal{T}$ and $r(\sigma_0) = 0 \in D$. Note that D has no more elements than $\mathcal{T}$ if $\mathcal{T} \neq \emptyset$ is finite. We prove

$$\tau_1, \tau_2 \in \mathcal{T} \Rightarrow (r(\tau_1) = r(\tau_2) \Leftrightarrow \mathcal{I} \models \tau_1 = \tau_2) \ . \tag{1}$$

Assume $\tau_1, \tau_2 \in \mathcal{T}$. In the direction ($\Rightarrow$) also assume $r(\tau_1) = r(\tau_2)$. From this we get $\mathcal{I} \models \tau_1 = \sigma_i$ and $\mathcal{I} \models \tau_2 = \sigma_i$ for some i. Since $\sigma_i \in \mathcal{T}$, the symmetry axiom $\tau_2 = \sigma_i \to \sigma_i = \tau_2$ and the transitivity axiom $\tau_1 = \sigma_i \to \sigma_i = \tau_2 \to$

$\tau_1 = \tau_2$ are in the set Eq^T. Thus also $\mathcal{I} \models \tau_1 = \tau_2$ holds. In the direction ($\Leftarrow$) assume $\mathcal{I} \models \tau_1 = \tau_2$. We have $r(\tau_1) = i$ for the least i such that $\sigma_i \in \mathcal{T}$ and $\mathcal{I} \models \tau_1 = \sigma_i$ holds. By appropriate symmetry and transitivity axioms in Eq^T we obtain $\mathcal{I} \models \tau_2 = \sigma_i$. We have $r(\tau_2) = j$ for the least $j \leq i$ such that $\sigma_j \in \mathcal{T}$ and $\mathcal{I} \models \tau_2 = \sigma_j$ holds. If $j < i$ then by symmetry and transitivity axioms in Eq^T we would get $\mathcal{I} \models \tau_1 = \sigma_j$ contradicting the definition of i. Hence $i = j$ and so $r(\tau_1) = r(\tau_2)$.

We now take any n-ary function symbol f of $\mathcal{L}$ and define the interpretation $f^{\mathcal{M}} : D^n \mapsto D$ of f as follows:

$$f^{\mathcal{M}}(d_1, \ldots, d_n) = r(f(\tau_1, \ldots, \tau_n)) \quad \text{where } r(\tau_1) = d_1, \ldots, r(\tau_n) = d_n.$$

We must convince ourselves first that this is a legal definition. If $n = 0$ then we have $f^{\mathcal{M}} = r(f)$. If $n > 0$ and $\mathcal{T} = \emptyset$ then, since $D = \{0\}$, we always have $r(f(\tau_1, \ldots, \tau_n)) = 0$. If $n > 0$ and $\mathcal{T} \neq \emptyset$ then, since for every $d \in D$ we have $d = r(\rho)$ for some $\rho \in \mathcal{T}$, the definition determines $f^{\mathcal{M}}(d_1, \ldots, d_n)$ uniquely if the following holds:

$$r(\tau_1) = r(\rho_1) \wedge \cdots \wedge r(\tau_n) = r(\rho_n) \rightarrow r(f(\tau_1, \ldots, \tau_n)) = r(f(\rho_1, \ldots, \rho_n))$$

for every $\tau_1, \ldots, \tau_n, \rho_1, \ldots, \rho_n$ in $\mathcal{T}$. From the assumptions we obtain $\mathcal{I} \models \tau_1 = \rho_1, \ldots, \mathcal{I} \models \tau_n = \rho_n$ by (1). Since the function substitution axiom 4.2.7(4) is in Eq^T and $\mathcal{I} \models Eq^T$, we have $\mathcal{I} \models f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n)$ and so $r(f(\tau_1, \ldots, \tau_n)) = r(f(\rho_1, \ldots, \rho_n))$ by (1).

For every n-ary predicate symbol P of $\mathcal{L}$ we define its interpretation $P^{\mathcal{M}} \subseteq D^n$:

$$P^{\mathcal{M}} = \{\langle r(\tau_1), \ldots, r(\tau_n)\rangle \mid \mathcal{I} \models P(\tau_1, \ldots, \tau_n) \text{ and } \tau_1, \ldots, \tau_n \in \mathcal{T}\} \ .$$

We prove

$$\rho_1, \ldots, \rho_n \in \mathcal{T} \Rightarrow (\mathcal{I} \models P(\rho_1, \ldots, \rho_n) \Leftrightarrow \langle r(\rho_1), \ldots, r(\rho_n)\rangle \in P^{\mathcal{M}}) \tag{2}$$

by taking any $\rho_1, \ldots, \rho_n \in \mathcal{T}$. In the direction ($\Rightarrow$) the property follows from the definition of $P^{\mathcal{M}}$ (even when $n = 0$ because $\rho_1, \ldots, \rho_n \in \mathcal{T}$ holds vacuously and we then have $P^{\mathcal{M}} = \{\langle\rangle\} = \{\emptyset\}$). In the direction ($\Leftarrow$) assume $\langle r(\rho_1), \ldots, r(\rho_n)\rangle \in P^{\mathcal{M}}$. If $n = 0$ then this means $\langle\rangle \in P^{\mathcal{M}}$ and so $\mathcal{I} \models P$. If $n > 0$ we have $r(\tau_1) = r(\rho_1), \ldots, r(\tau_n) = r(\rho_n)$ and $\mathcal{I} \models P(\tau_1, \ldots, \tau_n)$ for some $\tau_1, \ldots, \tau_n \in \mathcal{T}$. We get $\mathcal{I} \models \tau_1 = \rho_1, \ldots, \mathcal{I} \models \tau_n = \rho_n$ from (1). Since the predicate substitution axiom 4.2.7(5) $\in Eq^T$ and $\mathcal{I} \models Eq^T$, we obtain $\mathcal{I} \models P(\rho_1, \ldots, \rho_n)$.

The structure $\mathcal{M}$ is now defined and we define the assignment $a : \mathbb{N} \mapsto D$ by $a(i) = r(v_i)$. Thus also the identity interpretation $\mathcal{J}$ is defined and we prove:

$$\tau \in \mathcal{T} \Rightarrow \tau^{\mathcal{J}} = r(\tau) \tag{3}$$

by induction on the construction of the term τ. So assume $\tau \in \mathcal{T}$ and continue by the case analysis of τ. If $\tau \equiv v_i$ then $v_i^{\mathcal{J}} = a(i) = r(v_i)$. If $\tau \equiv f(\tau_1, \ldots, \tau_n)$ then

$$f(\tau_1, \ldots, \tau_n)^{\mathcal{J}} = f^{\mathcal{M}}(\tau_1^{\mathcal{J}}, \ldots, \tau_n^{\mathcal{J}}) \stackrel{\mathrm{IH}}{=} \\ f^{\mathcal{M}}(r(\tau_1), \ldots, r(\tau_n)) = r(f(\tau_1, \ldots, \tau_n)) \; .$$

Note that $\mathcal{J}$ is a canonical interpretation because if $d \in D$ then $d = r(\tau) = \tau^{\mathcal{J}}$ for some τ which is one of $\sigma_i \in FT(T)$ if the last set is not empty.

The lemma will be proved when we prove for every formula $\phi \in T$ the property:

$$\mathcal{J} \models \phi \Leftrightarrow \mathcal{I} \models \phi \; .$$

So take any $\phi \in T$. Note that $FT(\phi) \subseteq \mathcal{T}$ and proceed by induction on the construction of ϕ. If ϕ is a quantifier formula then we have $\mathcal{J} \models \phi$ iff $\phi \in Q$ iff $\phi \in \mathcal{I}$ iff $\mathcal{I} \models \phi$.

If $\phi \equiv \tau_1 = \tau_2$ then we must have $\mathcal{T} \neq \emptyset$ and so $\mathcal{J} \models \tau_1 = \tau_2$ iff $\tau_1^{\mathcal{J}} = \tau_2^{\mathcal{J}}$ iff, by (3), $r(\tau_1) = r(\tau_2)$ iff, by (1), $\mathcal{I} \models \tau_1 = \tau_2$.

If $\phi \equiv P(\tau_1, \ldots, \tau_n)$ then we must have $\mathcal{T} \neq \emptyset$ and so $\mathcal{J} \models P(\tau_1, \ldots, \tau_n)$ iff $\langle \tau_1^{\mathcal{J}}, \ldots, \tau_n^{\mathcal{J}} \rangle \in P^{\mathcal{N}}$ iff, by (3), $\langle r(\tau_1), \ldots, r(\tau_n) \rangle \in P^{\mathcal{N}}$ iff, by (2), $\mathcal{I} \models P(\tau_1, \ldots, \tau_n)$.

If $\phi \equiv \phi_1 \vee \phi_2$ then $\mathcal{J} \models \phi_1 \vee \phi_2$ iff $\mathcal{J} \models \phi_1$ or $\mathcal{J} \models \phi_2$ iff, by IH, $\mathcal{I} \models \phi_1$ or $\mathcal{I} \models \phi_2$ iff $\mathcal{I} \models \phi_1 \vee \phi_2$. The remaining cases are similar. □

4.2.9 Quasitautological consequence. Fix a language $\mathcal{L}$ and let T be a set of formulas from $\mathcal{L}$. We define the relation ϕ *is a quasitautological consequence of* T, in symbols $T \models_i \phi$, as follows:

$$T \models_i \phi \Leftrightarrow (\mathcal{I} \models T \Rightarrow \mathcal{I} \models \phi) \text{ for all identity interpretations } \mathcal{I}.$$

We write $\models_i \phi$ for $\emptyset \models_i \phi$ and such a ϕ is *quasitautology.* Note that we have

$$\models_i \phi \Leftrightarrow \mathcal{I} \models \phi \text{ for all identity interpretations } \mathcal{I}.$$

4.2.10 Lemma. $\models_i Eq$.

Proof. Take any identity interpretation $\mathcal{I} = \langle Q, \mathcal{M}, a \rangle$ for $\mathcal{L}$. We wish to prove $\mathcal{I} \models \phi$ for an equality axiom ϕ. If ϕ is a predicate substitution axiom 4.2.7(5) then $\mathcal{I} \models \phi$ iff from $\mathcal{I} \models \tau_1 = \rho_1, \ldots, \mathcal{I} \models \tau_n = \rho_n$, and $\mathcal{I} \models P(\tau_1, \ldots, \tau_n)$ follows $\mathcal{I} \models P(\rho_1, \ldots, \rho_n)$. If the assumptions are satisfied we have $\tau_1^{\mathcal{I}} = \rho_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}} = \rho_n^{\mathcal{I}}$, and $\langle \tau_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}} \rangle \in P^{\mathcal{M}}$ and so $\langle \rho_1^{\mathcal{I}}, \ldots, \rho_n^{\mathcal{I}} \rangle \in P^{\mathcal{M}}$, i.e. $\mathcal{J} \models P(\rho_1, \ldots, \rho_n)$.

The remaining cases are similar. □

4.2.11 Theorem (Quasitautological reduction).

$$T \vDash_i \phi \Rightarrow T, Eq^{T\cup\{\phi\}} \vDash_p \phi \tag{1}$$

$$T \vDash_i \phi \Leftrightarrow T, Eq \vDash_p \phi\ . \tag{2}$$

Proof. (1): Assume $T \vDash_i \phi$ and take any propositional interpretation $\mathcal{I}$ such that $\mathcal{I} \vDash T \cup Eq^{T\cup\{\phi\}}$ holds. From Lemma 4.2.8 we obtain a $T \cup \{\phi\}$-equivalent identity interpretation $\mathcal{J}$ and so $\mathcal{J} \vDash T$. We then get $\mathcal{J} \vDash \phi$ from the assumption and $\mathcal{I} \vDash \phi$ from the equivalence.

(2): The direction ($\Rightarrow$) follows from (1) by weakening. In the direction ($\Leftarrow$) assume $T, Eq \vDash_p \phi$ and take any identity interpretation $\mathcal{I}$ for $\mathcal{L}$ such that $\mathcal{I} \vDash T$ holds. We have $\mathcal{I} \vDash Eq$ by Lemma 4.2.10. From Lemma 4.2.6 we obtain an equivalent propositional interpretation $\mathcal{J}$. We thus have $\mathcal{J} \vDash T \cup Eq$, we get $\mathcal{J} \vDash \phi$ from the assumption, and $\mathcal{I} \vDash \phi$ from the equivalence. ◻

4.2.12 Decidability of quasitautologies. One of the consequences of the Reduction theorem is that the predicate $\vDash_i \phi$ of being a quasitautology is decidable. We namely have

$$\vDash_i \phi \Leftrightarrow\ \vDash_p \bigwedge Eq^{\{\phi\}} \to \phi\ . \tag{1}$$

First note that the set $FT(\phi)$ is finite and so there are only finitely many equality axioms with free terms from $FT(\phi)$ which means that the set $Eq^{\{\phi\}}$ is finite. We have $\vDash_i \phi$ iff, by 4.2.11(2), $Eq \vDash_p \phi$ iff, by Semantic deduction lemma 3.4.2, $\vDash_p \bigwedge Eq^{\{\phi\}} \to \phi$.

4.2.13 Theorem. $T \vDash_p \phi \Rightarrow T \vDash_i \phi$.

Proof. If $T \vDash_p \phi$ holds then we have $T, Eq \vDash_p \phi$ by weakening and $T \vDash_i \phi$ by 4.2.11(2). ◻

4.2.14 Theorem. *For every set of formulas T of some $\mathcal{L}$ and for every identity interpretation $\mathcal{I}$ for $\mathcal{L}$ there is a T-equivalent canonical identity interpretation $\mathcal{J}$. Every element of the domain of the structure of $\mathcal{J}$ is denoted by a term of $FT(T)$ if the last set is not empty.*

Proof. For a given identity interpretation $\mathcal{I}$ for $\mathcal{L}$ we obtain an equivalent propositional interpretation $\mathcal{I}_1$ by Lemma 4.2.6. By Lemma 4.2.10 we have $\mathcal{I} \vDash Eq$ and so $\mathcal{I}_1 \vDash Eq^T$ by the equivalence. From Lemma 4.2.8 we obtain a T-equivalent canonical identity interpretation $\mathcal{J}$ such that every element of the domain of the structure of $\mathcal{J}$ is denoted by a term of $FT(T)$ if the last set is not empty. ◻

4.3 Identity Tableaux

4.3.1 Identity tableau expansion rules. Fix a language $\mathcal{L}$. All expansion rules for identity tableaux are unary with premises in assumptions. In the following $\tau, \tau_1, \ldots, \tau_n, \rho_1, \ldots, \rho_n$ are arbitrary terms. *Reflexivity, symmetry,* and *transitivity* rules are in that order:

$$\frac{}{\tau = \tau}\,(\mathit{Refl}) \quad \frac{\tau_1 = \tau_2}{\tau_2 = \tau_1}\,(\mathit{Sym}) \quad \frac{\tau_1 = \tau_2 \;\; \tau_2 = \tau_3}{\tau_1 = \tau_3}\,(\mathit{Trans})$$

Function substitution rules are for every n-ary function symbol f of $\mathcal{L}$ with $n > 0$ as follows:

$$\frac{\tau_1 = \rho_1 \quad \cdots \quad \tau_n = \rho_n}{f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n)}\,(\mathit{Fsub})$$

Predicate substitution rules are for every n-ary predicate symbol P of $\mathcal{L}$ with $n > 0$ as follows:

$$\frac{\tau_1 = \rho_1 \quad \cdots \quad \tau_n = \rho_n \quad P(\tau_1, \ldots, \tau_n)}{P(\rho_1, \ldots, \rho_n)}\,(\mathit{Psub})$$

We can see that every identity rule *corresponds* to exactly one equality axiom.

4.3.2 Proofs with identity tableaux. An identity tableau π for a sequence of signed formulas Δ from axioms in T is called an *identity tableau for Δ from axioms T*. If π is closed then we assert this by writing $\pi : T \vdash_i [\Delta]$. When $\Delta \equiv \phi *$ then we say that π *is an identity tableau proving ϕ from axioms T* and write it as $\pi : T \vdash_i \phi$. We use additional abbreviations similar to those discussed in Par. 3.2.4.

4.3.3 Theorem (Admissible expansion rules in identity tableaux). *All rules proved admissible for propositional tableaux in Sect. 3.3 are also admissible in identity tableaux.*

Proof. Inspection of the proofs of admissibility of expansion rules in Sect. 3.3 reveals that the proofs remain correct also for identity tableaux, the presence of identity rules does not affect the proofs.

The only potential problem could be in the admissibility of cuts on propositional atoms (see Lemma 3.3.8) because we now have identity rules on propositional atoms $\tau_1 = \tau_2$ in assumptions. Fortunately, the elimination of cuts on such formulas removes the goals $\tau_1 = \tau_2 *$ which are not affected by the identity expansion rules. □

4.3.4 Lemma. $\vdash_i Eq$.

Proof. An axiom of reflexivity 4.2.7(1) has the following proof:

$$\frac{\tau = \tau *}{\underset{\circ}{\tau = \tau} \quad (\mathit{Refl})}$$

An axiom of predicate substitution 4.2.7(5) has the following proof:

$$
\begin{array}{c}
\tau_1 = \rho_1 \wedge \cdots \wedge \tau_n = \rho_n \wedge P(\tau_1,\ldots,\tau_n) \rightarrow P(\rho_1,\ldots,\rho_n)* \\
\hline
P(\rho_1,\ldots,\rho_n)* \qquad (\rightarrow_2 *) \\
\tau_1 = \rho_1 \wedge \cdots \wedge \tau_n = \rho_n \wedge P(\tau_1,\ldots,\tau_n) \qquad (\rightarrow_2 *) \\
\tau_1 = \rho_1 \qquad (G\wedge_1) \\
\cdots \\
\tau_n = \rho_n \qquad (G\wedge_n) \\
P(\tau_1,\ldots,\tau_n) \qquad (G\wedge_{n+1}) \\
P(\rho_1,\ldots,\rho_n) \qquad (Psub) \\
\circ
\end{array}
$$

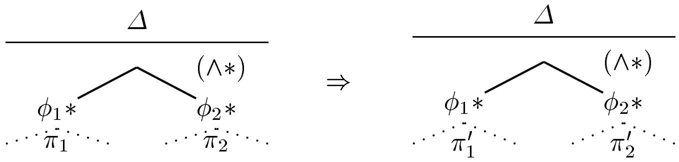
Remaining axioms have similar proofs. □

4.3.5 Lemma (Introduction of identity rules).

$$\pi : T, Eq \vdash_p [\Delta] \Rightarrow T \vdash_i [\Delta]$$

Proof. By induction on the structure of the tableau π. Assume $\pi : T, Eq \vdash_p [\Delta]$ and consider the form of π. If π is empty then we trivially have $T \vdash_i [\Delta]$.

If the first expansion in π is by a propositional rule, say $(\wedge *)$, then $\phi_1 \wedge \phi_2 * \in \Delta$ and π has a form shown in the following on the left:



We obtain identity tableaux π_1' and π_2' such that $\pi_1' : T \vdash_i [\Delta, \phi_1 *]$ and $\pi_2' : T \vdash_i [\Delta, \phi_2 *]$ by two IH's and construct the closed identity tableau for Δ from axioms T shown on the right. The remaining expansions by propositional rules and by axiom rules from T are similar.

If the first expansion in π is by an axiom rule for $\phi \in Eq$ then π has a form shown in the following on the left:

$$
\begin{array}{c}
\Delta \\
\hline
\phi \quad (Ax) \\
\cdots \pi_1 \cdots
\end{array}
\quad \Rightarrow \quad
\begin{array}{c}
\Delta \\
\hline
\phi \quad (L) \\
\cdots \pi_1' \cdots
\end{array}
$$

We obtain an identity tableau π_1' such that $\pi_1' : T \vdash_i [\Delta, \phi]$ by IH, note that $\vdash_i \phi$ by Lemma 4.3.4, and construct by a lemma rule the closed identity tableau for Δ from axioms T shown on the right. □

4.3.6 Lemma (Elimination of identity rules).

$$\pi : T \vdash_i [\Delta] \Rightarrow T, Eq \vdash_p [\Delta] \ .$$

Proof. By induction on the structure of the tableau π. Assume $\pi : T \vdash_i [\Delta]$ and consider the form of π. If π is empty then we trivially have $T \vdash_p [\Delta]$ and we obtain $T, Eq \vdash_p [\Delta]$ by weakening.

If the first expansion in π is by a propositional rule, say $(\rightarrow)$, then $\phi_1 \rightarrow \phi_2 \in \Delta$ and π has a form shown in the following on the left:

$$\begin{array}{c} \Delta \\ \hline \begin{array}{cc} & (\rightarrow) \\ \phi_2 & \phi_1 * \\ \pi_2 & \pi_1 \end{array} \end{array} \quad \Rightarrow \quad \begin{array}{c} \Delta \\ \hline \begin{array}{cc} & (\rightarrow) \\ \phi_2 & \phi_1 * \\ \pi_2' & \pi_1' \end{array} \end{array}$$

We obtain propositional tableaux π_1' and π_2' such that $\pi_1' : T, Eq \vdash_p [\Delta, \phi_1 *]$ and $\pi_2' : T, Eq \vdash_p [\Delta, \phi_2]$ by two IH's and construct the closed propositional tableau for Δ from axioms T, Eq shown on the right. The remaining propositional and axiom expansions are similar.

If the first expansion in π is by a reflexivity rule then π has a form shown in the following on the left:

$$\begin{array}{c} \Delta \\ \hline \tau = \tau \quad (\mathit{Refl}) \\ \pi_1 \end{array} \quad \Rightarrow \quad \begin{array}{c} \Delta \\ \hline \tau = \tau \quad (Ax) \\ \pi_1' \end{array}$$

We obtain a propositional tableau π_1' such that $\pi_1' : T, Eq \vdash_p [\Delta, \tau = \tau]$ by IH and construct the closed propositional tableau for Δ from axioms T, Eq shown on the right.

If the first expansion in π is by a function substitution rule then π has a following form:

$$\begin{array}{c} \Delta \\ \hline f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n) \quad (\mathit{Fsub}) \\ \pi_1 \end{array} \quad \text{where } \tau_1 = \rho_1, \ldots, \tau_n = \rho_n \in \Delta$$

We obtain a propositional tableau π_1' such that

$$\pi_1' : T, Eq \vdash_p [\Delta, f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n)]$$

by IH and construct the following closed propositional tableau for Δ from axioms T, Eq:

$$
\frac{\Delta \quad \text{s.t. } \tau_1 = \rho_1, \ldots, \tau_n = \rho_n \in \Delta}{\tau_1 = \rho_1 \wedge \cdots \wedge \tau_n = \rho_n \to f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n) \quad (Ax)}
$$

$$
\begin{array}{ccc}
 & (\to) & \\
f(\tau_1, \ldots, \tau_n) = f(\rho_1, \ldots, \rho_n) & & \tau_1 = \rho_1 \wedge \cdots \wedge \tau_n = \rho_n * \quad (G\wedge *) \\
\pi_1' & & \begin{array}{ccc} \tau_1 = \rho_1 * & \cdots & \tau_n = \rho_n * \\ \circ & & \circ \end{array}
\end{array}
$$

The remaining identity expansion rules are similar. □

4.3.7 Theorem (Introduction/elimination of identity rules).

$$T \vdash_i \phi \Leftrightarrow T, Eq \vdash_p \phi \ .$$

Proof. In the direction ($\Rightarrow$) assume $\pi : T \vdash_i \phi$, i.e $\pi : T \vdash_i [\phi *]$, and obtain $T, Eq \vdash_p [\phi *]$, i.e. $T, Eq \vdash_p \phi$, by Lemma 4.3.6.

In the direction ($\Leftarrow$) assume $T, Eq \vdash_p \phi$, i.e. $T, Eq \vdash_p [\phi *]$, and obtain $T \vdash_i [\phi *]$, i.e. $T \vdash_i \phi$, by Lemma 4.3.5. □

4.3.8 Corollary (Soundness and completeness of identity tableaux). *For any fromula ϕ and a set of formulas T from $\mathcal{L}$ we have*

$$
\begin{array}{ccc}
T \models_i \phi & & T \vdash_i \phi \\
\Uparrow\!\Downarrow 4.2.11(2) & & \Uparrow\!\Downarrow 4.3.7 \\
T, Eq \models_p \phi & \Leftrightarrow 3.5.8 & T, Eq \vdash_p \phi
\end{array}
$$

□

4.3.9 Decidability of quasitautologies revisited. Property 4.2.12(1) reduces the problem of deciding whether a formula ϕ of some $\mathcal{L}$ is quasitautology to the problem of deciding whether the formula $\bigwedge Eq^{\{\phi\}} \to \phi$ is a tautology. This decision procedure can be called the method of *associates* because the conjunction of equality axioms $\bigwedge Eq^{\{\phi\}}$ is an *identity associate* of ϕ. Quantifier associates were introduced by R. Smullyan [21].

Lemma 4.2.6 and property 4.2.11(1) give us another method of deciding quasitautologies: test $\mathcal{J} \models \phi$ in all finite identity interpretations $\mathcal{J}$ for a finite language consisting of function and predicate symbols in ϕ. Note that the quantifier sets Q of such interpretations can be restricted to subsets of finitely many quantifier formulas among $FPA(\phi)$. Also note that there are only finitely many assignments a to be considered because the only values which matter are the finitely many values $a(i)$ where $v_i \in FT(\phi)$. The formula ϕ is a quasitautology iff $\mathcal{J} \models \phi$ for all such finite identity interpretations $\mathcal{J}$. Such a test for quasitautologies seems to be much less convenient than the method of associates. We mention it here because this is the method used by Boolos and Jeffrey [3] to recognize proofs in their proof calculus for predicate logic.

Identity tableaux offer the most convenient test for quasitautologies. We call a branch Δ of an identity tableau *identically complete* if whenever an identity rule has its premises Δ_1 in Δ then also its conclusion ϕ is an assumption in Δ provided $FT(\phi) \subseteq FT(\Delta_1)$. The reader will note that the last condition can be violated only by function substitution rules whose conclusions can introduce new terms into identity tableaux.

In order to test whether ϕ is a quasitautology we construct a tableau for $\phi*$ and in every open propositionally complete branch we saturate the branch by the conclusions of finitely many identity rules which can be applied on the branch and which do not introduce new terms. If all branches close then ϕ is a quasitautology by Corollary 4.3.8. If there is an open propositionally and identically complete branch then we construct a propositional interpretation $\mathcal{I}$ by collecting all propositional atoms in the assumptions of the branch. We have proved in Par. 3.2.8 that we have $\mathcal{I} \nvDash \phi$ and $\mathcal{I} \vDash \psi$ for all assumptions ψ in the branch. Now, the branch is identically complete, and so we must have $\mathcal{I} \vDash Eq^{\{\phi\}}$. But this means that $Eq^{\{\phi\}} \nvDash_p \phi$ holds and so we have $\nvDash_i \phi$ by 4.2.11(1).

Identity tableaux facilitate also a semidecidable test for quasitautological consequence from decidable axioms T: $T \vDash_i \phi$. This is an extension of the procedure described in Par. 3.5.9 where we identically complete every open branch which is propositionally complete just before we add the next axiom to the assumptions of the branch. By the same reasoning as above we can show that if there is an open branch which is propositionally, identically, and axiomatically complete then we have a propositional interpretation $\mathcal{I}$ such that $\mathcal{I} \vDash T \cup Eq^{T \cup \{\phi\}}$ and $\mathcal{I} \nvDash \phi$. Hence $\mathcal{I}$ witnesses $T, Eq^{T \cup \{\phi\}} \nvDash_p \phi$ and we get $T \nvDash_i \phi$ by 4.2.11(1).

5. Quantification Logic

In this section we investigate the notion of *logical consequence* where a formula ϕ follows from a set of axioms T by the laws of logic alone. This means that ϕ follows from T because of the properties of propositional connectives, identitity relation, and quantifiers and without taking into considerations the extralogical properties of its function and predicate symbols beyond those which are captured by the axioms T.

5.1 Some Syntactic Concepts

In contrast to the preceding chapters where the variables played no special role we will need in this chapter to pay the attention to the variables occurring in formulas of first order languages.

5.1.1 Free variables. *Free variables* of a set of formulas S of a language $\mathcal{L}$ are variables x occurring in the formulas of S outside of quantifiers $\exists x$ and $\forall x$. This is made precise by a metamathematical function $FV(\alpha)$ defined on terms, formulas, and sets of formulas to yield the set of free variables of α. The function FV satisfies the set identities given in Fig. 5.1.

5.1.2 Sentences. A term τ (formula ϕ) of some $\mathcal{L}$ such that $FV(\tau) = \emptyset$ ($FV(\phi) = \emptyset$) is *closed* and *open* otherwise. Closed formulas are called *sentences.* Sets T of closed formulas are *closed. Universal instantiation* of a formula ϕ is any sentence $\forall x_1 \ldots \forall x_n \phi$ such that $x_1, \ldots, x_n \in FV(\phi)$. We usually denote by $\forall \phi$ any universal instantiation of ϕ.

A variable x is *bound* in a formula ϕ if $\exists x \psi$ or $\forall x \psi$ occurs as a subformula in ϕ.

5.1.3 Substitution. If α is a term, formula, or a set of formulas of a language $\mathcal{L}$ then we will denote by $\alpha_x[\tau]$ the application of the ternary metamathematical *substitution* function which yields term, formula, or set similar to α but with every free occurrence of the variable x replaced by the term τ. The substitution function is defined to satisfy the term identities given in Fig. 5.2.

$$
\begin{aligned}
FV(x) &= \{x\} \\
FV(f(\tau_1, \ldots, \tau_n)) &= FV(\tau_1) \cup \ldots \cup FV(\tau_n) \\
FV(\tau_1 = \tau_2) &= FT(\tau_1) \cup FT(\tau_2) \\
FV(P(\tau_1, \ldots, \tau_n)) &= FV(\tau_1) \cup \ldots \cup FV(\tau_n) \\
FV(\forall x \phi) &= FV(\phi) \setminus \{x\} \\
FV(\exists x \phi) &= FV(\phi) \setminus \{x\} \\
FV(\top) &= \emptyset \\
FV(\bot) &= \emptyset \\
FV(\neg \phi) &= FV(\phi) \\
FV(\phi_1 \vee \phi_2) &= FV(\phi_1) \cup FV(\phi_2) \\
FV(\phi_1 \wedge \phi_2) &= FV(\phi_1) \cup FV(\phi_2) \\
FV(\phi_1 \rightarrow \phi_2) &= FV(\phi_1) \cup FV(\phi_2) \\
FV(\phi_1 \leftrightarrow \phi_2) &= FV(\phi_1) \cup FV(\phi_2) \\
FV(T) &= \bigcup \{FV(\phi) \mid \phi \in T\} .
\end{aligned}
$$

Fig. 5.1. Function yielding sets of free variables

$$
\begin{aligned}
y_x[\tau] &\equiv \begin{cases} \tau & \text{if } y \equiv x \\ y & \text{otherwise} \end{cases} \\
f(\tau_1, \ldots, \tau_n)_x[\tau] &\equiv f(\tau_{1x}[\tau], \ldots, \tau_{nx}[\tau]) \\
(\tau_1 = \tau_2)_x[\tau] &\equiv \tau_{1x}[\tau] = \tau_{2x}[\tau] \\
P(\tau_1, \ldots, \tau_n)_x[\tau] &\equiv P(\tau_{1x}[\tau], \ldots, \tau_{nx}[\tau]) \\
(\forall y \phi)_x[\tau] &\equiv \begin{cases} \forall y \phi & \text{if } y \equiv x \\ \forall y \phi_x[\tau] & \text{otherwise} \end{cases} \\
(\exists y \phi)_x[\tau] &\equiv \begin{cases} \exists y \phi & \text{if } y \equiv x \\ \exists y \phi_x[\tau] & \text{otherwise} \end{cases} \\
\top_x[\tau] &\equiv \top \\
\bot_x[\tau] &\equiv \bot \\
\neg \phi_x[\tau] &\equiv \phi_x[\tau] \\
(\phi_1 \vee \phi_2)_x[\tau] &\equiv \phi_{1x}[\tau] \vee \phi_{2x}[\tau] \\
(\phi_1 \wedge \phi_2)_x[\tau] &\equiv \phi_{1x}[\tau] \wedge \phi_{2x}[\tau] \\
(\phi_1 \rightarrow \phi_2)_x[\tau] &\equiv \phi_{1x}[\tau] \rightarrow \phi_{2x}[\tau] \\
(\phi_1 \leftrightarrow \phi_2)_x[\tau] &\equiv \phi_{1x}[\tau] \leftrightarrow \phi_{2x}[\tau] \\
T_x[\tau] &\equiv \{\phi_x[\tau] \mid \phi \in T\} .
\end{aligned}
$$

Fig. 5.2. Substitution function

For reasons discussed in Par. 5.2.11 we will use the the substitution function $\alpha_x[\tau]$ only with terms τ which are *free for x in α* meaning that no variable occurring in τ becomes bound in the result of the substitution. In other words, whenever the recursion reaches a quantified formula, say, $(\forall y\phi)_x[\tau]$ with $y \not\equiv x$ we have $y \notin FV(\tau)$. Note that a closed term τ is free for x in any ϕ.

We now agree on a convention that whenever we will write $\alpha_x[\tau]$ without explicitly mentioning that τ is free for x in α this restriction will be tacitly assumed.

5.1.4 Indication of variables. We will often *indicate* by writing $\phi[x]$ that the variable x is possibly free in ϕ. When we later write $\phi[\tau]$ we are designating the same formula as $\phi_x[\tau]$.

The method of indication is useful when we indicate more variables at once: $\phi[\vec{x}]$. In such situations we always tacitly assume that the n-tuple of variables $\vec{x}$ consists of pairwise distinct variables. By writing $\phi[\vec{\tau}]$ we designate the same formula as $\phi_{x_1}[\tau_1]\cdots_{x_n}[\tau_n]$.

5.1.5 Cantor's diagonal pairing function. We will need the well-known Cantor's 'diagonal' pairing function J defined as

$$J(x,y) = \frac{(x+y+1)\cdot(x+y)}{2} + x \ .$$

It is not hard to see that every natural number z can be uniquely written as $z = J(x,y)$. Moreover, for any numbers x and y the value $J(x,y)$ can be efectively computed and also for a given number z the unique numbers x and y such that $z = J(x,y)$ can be effectively computed.

5.1.6 Witnessing extensions of first-order languages. Let $\mathcal{L}$ be a first-order language. We denote by $\mathcal{L}_c$ its *witnessing extension* by the addition of *Henkin* (witnessing) constants c_k where $k = J(i+1,j)$ for some i, j. This c_k is said to be of *rank* $(i+1)$. Henkin constants are always chosen as new constants not occurring in $\mathcal{L}$.

A formula ϕ of $\mathcal{L}_c$ is of *rank* i if ϕ is of $\mathcal{L}$ and $i = 0$ or if for some Henkin constant c_k with rank i we have $c_k \in FT(\phi)$ and no Henkin constant of higher rank is in $FT(\phi)$.

We now assign the Henkin constants to the existentially quantified sentences of $\mathcal{L}_c$ as follows. We can clearly enumerate the formulas of any language into a sequence. Moreover, by ommiting certain formulas, we can also enumerate for every number i all existentially quantified sentences of $\mathcal{L}_c$ of rank i:

$$\psi_0^i \ \psi_1^i \ \psi_2^i \ \ldots \ , \tag{1}$$

i.e. sentences where $\psi_j^i \equiv \exists x\phi$ for some ϕ of rank i from $\mathcal{L}_c$. We fix one such enumeration relatively to every $\mathcal{L}$ (and thus also relatively to $\mathcal{L}_c$) and i.

The Henkin constant $c_{J(i+1,j)}$ is said to *belong* to the sentence ψ_j^i.

5.1.7 Quantifier axioms. Fix a language $\mathcal{L}$ and consider its witnessing extension $\mathcal{L}_c$. We call the sentences

$$\phi_x[\tau] \to \exists x\phi \tag{1}$$
$$\forall x\phi \to \phi_x[\tau] \tag{2}$$

where $\exists x\phi$ and $\forall x\phi$ are sentences of $\mathcal{L}_c$ and τ a closed term of $\mathcal{L}_c$ *instantiation* axioms.

We call the sentence

$$\exists x\phi \to \phi_x[c_k] \tag{3}$$

where $\exists x\phi$ is a sentence of $\mathcal{L}_c$ and c_k the Henkin constant belonging to it the (Henkin) *witnessing axiom for* $\exists x\phi$.

We call the sentence

$$\phi_x[c_k] \to \forall x\phi \tag{4}$$

where $\forall x\phi$ is a sentence of $\mathcal{L}_c$ and c_k the Henkin constant belonging to the sentence $\exists x\neg\phi$ the (Henkin) *counterexample axiom for* $\forall x\phi$. Witnessing and counterexample axioms are together called *Henkin* axioms. We designate the witnessing axioms by Ha.

Note that the Henkin axioms for sentences $\exists x\phi$ and $\forall x\phi$ of rank i do not need to have ranks $i+1$ because it can happen that $x \notin FV(\phi)$.

The set Qa of *quantifier* axioms is the set of sentences of $\mathcal{L}_c$ consisting of the instantiation and Henkin axioms.

5.2 Logical Consequence

5.2.1 Interpretations. An *interpretation* $\mathcal{I}$ *for* $\mathcal{L}$ is a pair $\langle \mathcal{M}, a\rangle$ where $\mathcal{M}$ is a structure for $\mathcal{L}$ with domain D and a is an assignment in $\mathcal{M}$.

Denotations $\tau^{\mathcal{I}}$ of terms τ of $\mathcal{L}$ are defined exactly as in Par. 4.2.4.

For the definition of the satisfaction relation we will need an operator taking the assignment a, variable x, and $d \in D$ to the assigment designated by $a(\,{}^{d}_{x}\,)$ and such that

$$a(\,{}^{d}_{x}\,)(i) = \begin{cases} d & \text{if } x \equiv v_i \\ a(i) & \text{if } x \not\equiv v_i. \end{cases}$$

For the above interpretation $\mathcal{I}$ we designate by $\mathcal{I}(\,{}^{d}_{x}\,)$ the interpretation $\langle \mathcal{M}, a(\,{}^{d}_{x}\,)\rangle$.

The satisfaction relation $\mathcal{I}$ *satisfies* ϕ, written as $\mathcal{I} \vDash \phi$, is similar to the satisfaction relation for identity interpretations (see Par. 4.2.5) when ϕ is an atomic or propositional formula. For quantifier formulas we define the relation as follows:

$$\mathcal{I} \models \forall x\phi \Leftrightarrow \mathcal{I}(\tfrac{d}{x}) \models \phi \text{ for all } d \in D$$
$$\mathcal{I} \models \exists x\phi \Leftrightarrow \mathcal{I}(\tfrac{d}{x}) \models \phi \text{ for some } d \in D.$$

Interpretations $\mathcal{I}$ for $\mathcal{L}_c$ such that $\mathcal{I} \models Ha$ are called *Henkin interpretations.*

5.2.2 Agreement of interpretations. If S is a set of terms then two interpretations $\mathcal{I} = \langle \mathcal{M}, a\rangle$ and $\mathcal{J} = \langle \mathcal{M}, b\rangle$ sharing the same structure *agree on* S if the assignments a and b *agree on* S, i.e. if for every variable $v_i \in S$ we have $a(i) = b(i)$.

5.2.3 Equivalence lemma. *If the interpetations $\mathcal{I}$ and $\mathcal{J}$ for $\mathcal{L}$ agree on*

1. *$FV(\tau)$ then $\tau^{\mathcal{I}} = \tau^{\mathcal{J}}$,*
2. *$FV(T)$ then $\mathcal{I} \equiv_T \mathcal{J}$.*

Proof. 1) Assume $\mathcal{I} = \langle \mathcal{M}, a\rangle$ and $\mathcal{J} = \langle \mathcal{M}, b\rangle$ and prove the property by induction on the construction of τ. If $\tau \equiv v_i$ then $v_i^{\mathcal{I}} = a(i) = b(i) = v_i^{\mathcal{J}}$. If $\tau \equiv f(\tau_1, \dots, \tau_n)$ then

$$f(\tau_1, \dots, \tau_n)^{\mathcal{I}} = f^{\mathcal{M}}(\tau_1^{\mathcal{I}}, \dots, \tau_n^{\mathcal{I}}) \stackrel{\text{IH}}{=} f^{\mathcal{M}}(\tau_1^{\mathcal{J}}, \dots, \tau_n^{\mathcal{J}}) = f(\tau_1, \dots, \tau_n)^{\mathcal{J}} .$$

2) Take any $\phi \in T$ and prove

$$\mathcal{I} \models \phi \Leftrightarrow \mathcal{J} \models \phi \text{ for } \mathcal{I} \text{ and } \mathcal{J} \text{ agreeing on } FV(T)$$

by induction on the construction of ϕ. If $\phi \equiv \tau_1 = \tau_2$ then we have $\mathcal{I} \models \tau_1 = \tau_2$ iff $\tau_1^{\mathcal{I}} = \tau_2^{\mathcal{I}}$ iff, by 1), $\tau_1^{\mathcal{J}} = \tau_2^{\mathcal{J}}$ iff $\mathcal{J} \models \tau_1 = \tau_2$. The case when $\phi \equiv P(\tau_1, \dots, \tau_n)$ is similar.

If $\phi \equiv \exists x\phi_1$ then $\mathcal{I} \models \exists x\phi_1$ iff $\mathcal{I}(\tfrac{d}{x}) \models \phi_1$ for some $d \in D$ where D is the domain of the structure shared by $\mathcal{I}$ and $\mathcal{J}$ iff, by IH, $\mathcal{J}(\tfrac{d}{x}) \models \phi_1$ for some $d \in D$ iff $\mathcal{J} \models \exists x\phi_1$. The case when $\phi \equiv \forall x\phi_1$ is similar.

If $\phi \equiv \neg\phi_1$ then $\mathcal{I} \models \neg\phi_1$ iff $\mathcal{I} \not\models \phi_1$ iff, by IH, $\mathcal{J} \not\models \phi_1$, iff $\mathcal{J} \models \neg\phi_1$. The remaining propositional cases for ϕ are similar.

5.2.4 Substitution lemma. For every interpretation $\mathcal{I}$ for $\mathcal{L}$, any terms ρ_1, ρ_2, any formula ϕ, and any term τ free for x in ϕ we have:

$$(\rho_{1\,x}[\rho_2])^{\mathcal{I}} = \rho_1^{\mathcal{I}(\frac{\rho_2^{\mathcal{I}}}{x})} \tag{1}$$
$$\mathcal{I} \models \phi_x[\tau] \Leftrightarrow \mathcal{I}(\tfrac{\tau^{\mathcal{I}}}{x}) \models \phi \ . \tag{2}$$

Proof. Take any interpretation $\mathcal{I} = \langle \mathcal{M}, a\rangle$ and let D be the domain of $\mathcal{M}$. (1): By induction on the construction of ρ_1. If $\rho_1 \equiv v_i$ then if $v_i \equiv x$ we have

$$(x_x[\rho_2])^{\mathcal{I}} = \rho_2^{\mathcal{I}} = a(\tfrac{\rho_2^{\mathcal{I}}}{x})(i) = x^{\mathcal{I}(\frac{\rho_2^{\mathcal{I}}}{x})}$$

and if $v_i \not\equiv x$ we have

$$(v_{i\,x}[\rho_2])^{\mathcal{I}} = v_i^{\mathcal{I}} = a(\genfrac{}{}{0pt}{}{\rho_2^{\mathcal{I}}}{x})(i) = v_i^{\mathcal{I}(\genfrac{}{}{0pt}{}{\rho_2^{\mathcal{I}}}{x})} \ .$$

If $\rho_1 \equiv f(\tau_1, \ldots, \tau_n)$ then

$$\begin{aligned}(f(\tau_1, \ldots, \tau_n)_x[\rho_2])^{\mathcal{I}} &= (f(\tau_{1\,x}[\rho_2], \ldots, \tau_{n\,x}[\rho_2]))^{\mathcal{I}} = \\ &\quad f^{\mathcal{M}}((\tau_{1\,x}[\rho_2])^{\mathcal{I}}, \ldots, (\tau_{1\,x}[\rho_2])^{\mathcal{I}}) \overset{\text{IH}}{=} \\ &\quad f^{\mathcal{M}}(\tau_1^{\mathcal{I}(\genfrac{}{}{0pt}{}{\rho_2^{\mathcal{I}}}{x})}, \ldots, \tau_n^{\mathcal{I}(\genfrac{}{}{0pt}{}{\rho_2^{\mathcal{I}}}{x})}) = (f(\tau_1, \ldots, \tau_n))^{\mathcal{I}(\genfrac{}{}{0pt}{}{\rho_2^{\mathcal{I}}}{x})} \ .\end{aligned}$$

(2): By induction on the construction of ϕ. If $\phi \equiv \tau_1 = \tau_2$ then we have $\mathcal{I} \vDash (\tau_1 = \tau_2)_x[\tau]$ iff $\mathcal{I} \vDash \tau_{1\,x}[\tau] = \tau_{2\,x}[\tau]$ iff $(\tau_{1\,x}[\tau])^{\mathcal{I}} = (\tau_{2\,x}[\tau])^{\mathcal{I}}$ iff, by (1), $\tau_1^{\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x})} = \tau_2^{\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x})}$ iff $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \tau_1 = \tau_2$.

If $\phi \equiv P(\tau_1, \ldots, \tau_n)$ then $\mathcal{I} \vDash P(\tau_1, \ldots, \tau_n)_x[\tau]$ iff $\mathcal{I} \vDash P(\tau_{1\,x}[\tau], \ldots, \tau_{n\,x}[\tau])$ iff $\langle(\tau_{1\,x}[\tau])^{\mathcal{I}}, \ldots, (\tau_{n\,x}[\tau])^{\mathcal{I}}\rangle \in P^{\mathcal{M}}$ iff, by (1), $\langle \tau_1^{\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x})}, \ldots, \tau_n^{\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x})}\rangle \in P^{\mathcal{M}}$ iff $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash P(\tau_1, \ldots, \tau_n)$.

If $\phi \equiv \exists y \phi_1$ then if $x \equiv y$ then we have $\mathcal{I} \vDash (\exists y \phi_1)_x[\tau]$ iff $\mathcal{I} \vDash \exists y \phi_1$ iff by Lemma 5.2.3, since $\mathcal{I}$ and $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x})$ agree on $FV(\exists y \phi_1)$, $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \exists y \phi_1$.

If $x \not\equiv y$ then we have $\mathcal{I} \vDash (\exists y \phi_1)_x[\tau]$ iff $\mathcal{I} \vDash \exists y \phi_{1\,x}[\tau]$ iff $\mathcal{I}(\genfrac{}{}{0pt}{}{d}{y}) \vDash \phi_{1\,x}[\tau]$ for some $d \in D$ iff by IH, since τ is free for x in ϕ_1, $\mathcal{I}(\genfrac{}{}{0pt}{}{d}{y})(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}(\genfrac{}{}{0pt}{}{d}{y})}}{x}) \vDash \phi_1$ for some $d \in D$ iff, by Lemma 5.2.3, since $y \notin FV(\tau)$, $\mathcal{I}(\genfrac{}{}{0pt}{}{d}{y})(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \phi_1$ for some $d \in D$ iff $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x})(\genfrac{}{}{0pt}{}{d}{y}) \vDash \phi_1$ for some $d \in D$ iff $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \exists y \phi_1$. If $\phi \equiv \forall y \phi_1$ then the proof is similar.

If $\phi \equiv \phi_1 \vee \phi_2$ then we have $\mathcal{I} \vDash (\phi_1 \vee \phi_2)_x[\tau]$ iff $\mathcal{I} \vDash \phi_{1\,x}[\tau] \vee \phi_{2\,x}[\tau]$ iff $\mathcal{I} \vDash \phi_{1\,x}[\tau]$ or $\mathcal{I} \vDash \phi_{2\,x}[\tau]$ iff by IH, since τ is free for x in ϕ_1, ϕ_2, $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \phi_1$ or $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \phi_2$ iff $\mathcal{I}(\genfrac{}{}{0pt}{}{\tau^{\mathcal{I}}}{x}) \vDash \phi_1 \vee \phi_2$. The remaining propositional cases are similar. $\square$

5.2.5 Models. Let $\mathcal{M}$ be a structure for $\mathcal{L}$ with a domain D and $\phi[\vec{x}]$ a formula of $\mathcal{L}$ with all of its free variables among the indicated ones. By Lemma 5.2.3 any two assignments in $\mathcal{M}$ a and b which coincide on $\vec{x}$ are such that

$$\langle \mathcal{M}, a\rangle \vDash \phi \Leftrightarrow \langle \mathcal{M}, b\rangle \vDash \phi$$

and so for $\vec{d} \in D$ we can write $\mathcal{M} \vDash \phi[\vec{d}]$ as an abbreviation for $\langle \mathcal{M}, a\rangle \vDash \phi$ where a is any assignment such that $a(x_1) = d_1, \ldots, a(x_n) = d_n$.

We define $\mathcal{M} \vDash \phi$ as

$$\mathcal{M} \vDash \phi[\vec{d}] \quad \text{for all } \vec{d} \in D \ .$$

If ϕ is a sentence then we have $\mathcal{M} \vDash \phi$ iff $\langle \mathcal{M}, a\rangle \vDash \phi$ for some assignment a (and equivalently for all assignments a) and in that case we say that $\mathcal{M}$ is a *model* of ϕ, or that ϕ is *true* in $\mathcal{M}$.

For a set T of formulas of $\mathcal{L}$ we write $\mathcal{M} \models T$ for $\mathcal{M} \models \phi$ for all $\phi \in T$. $\mathcal{M}$ is a *model* of a set T of sentences of $\mathcal{L}$ if $\mathcal{M} \models T$. T is *satisfiable* if it is true in some structure, i.e. if T has a model.

5.2.6 Expansions of structures. Let $\mathcal{L}_1$ be an extension of a language $\mathcal{L}$ and let $\mathcal{M}$ be a structure for $\mathcal{L}$ with a domain D. The structure $\mathcal{N}$ for $\mathcal{L}_1$ is an *expansion* of $\mathcal{M}$ if the domain of $\mathcal{N}$ is D and the interpretation in $\mathcal{N}$ of every function and predicate symbol from $\mathcal{L}$ is the same as in $\mathcal{M}$.

The interpretation $\mathcal{J}$ for $\mathcal{L}_1$ is an *expansion* of the interpretation $\mathcal{I}$ for $\mathcal{L}$ if the structure of $\mathcal{J}$ is an expansion of the structure for $\mathcal{I}$ and both interpretations have the same assignments.

Two interpretations $\mathcal{I}$ for $\mathcal{L}$ and $\mathcal{J}$ for $\mathcal{L}_1$ where $\mathcal{L}_1$ is an extension of $\mathcal{L}$ are *equivalent on T*, which we write as $\mathcal{I} \equiv_T \mathcal{J}$, if T is a subset of formulas of $\mathcal{L}$ and $\mathcal{I} \models \phi \Leftrightarrow \mathcal{J} \models \phi$ for all $\phi \in T$. We write $\mathcal{I} \equiv_{\mathcal{L}} \mathcal{J}$ if $\mathcal{I}$ and $\mathcal{J}$ are equivalent on the formulas of $\mathcal{L}$.

5.2.7 Expansion theorem. *If $\mathcal{J}$ for $\mathcal{L}_1$ is an expansion of $\mathcal{I}$ for $\mathcal{L}$ then*

$$\tau^{\mathcal{J}} = \tau^{\mathcal{I}} \qquad \textit{for all terms } \tau \textit{ of } \mathcal{L} \tag{1}$$

$$\mathcal{J} \equiv_{\mathcal{L}} \mathcal{I}\ . \tag{2}$$

Proof. Assume that $\mathcal{J} = \langle \mathcal{N}, a \rangle$ with the domain D and $\mathcal{I} = \langle \mathcal{M}, a \rangle$.

(1): By induction on the construction of τ. If $\tau \equiv v_i$ then $v_i^{\mathcal{J}} = a(i) = v_i^{\mathcal{I}}$. If $\tau \equiv f(\tau_1, \ldots, \tau_n)$ for f in $\mathcal{L}$ then

$$f(\tau_1, \ldots, \tau_n)^{\mathcal{J}} = f^{\mathcal{N}}(\tau_1^{\mathcal{J}}, \ldots, \tau_n^{\mathcal{J}}) \overset{\mathrm{IH}}{=} f^{\mathcal{N}}(\tau_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}}) = \\ f^{\mathcal{M}}(\tau_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}}) = f(\tau_1, \ldots, \tau_n)^{\mathcal{I}}\ .$$

(2): The property follows from

$$\phi \text{ in } \mathcal{L}; \text{ for all } \mathcal{J} \text{ for } \mathcal{L} \text{ and } \mathcal{I} \text{ for } \mathcal{L}_1 \text{ s.t. } \mathcal{J} \text{ expands } \mathcal{I} \Rightarrow (\mathcal{J} \models \phi \Leftrightarrow \mathcal{I} \models \phi)$$

proved by induction on the construction of ϕ. If $\phi \equiv \tau_1 = \tau_2$ then we have $\mathcal{J} \models \tau_1 = \tau_2$ iff $\tau_1^{\mathcal{J}} = \tau_2^{\mathcal{J}}$ iff, by (1), $\tau_1^{\mathcal{I}} = \tau_2^{\mathcal{I}}$ iff $\mathcal{I} \models \tau_1 = \tau_2$. The case when $\phi \equiv P(\tau_1, \ldots, \tau_n)$ is similar.

If $\phi \equiv \exists x \phi_1$ then $\mathcal{J} \models \exists x \phi_1$ iff $\mathcal{J}(\frac{d}{x}) \models \phi_1$ for some $d \in D$ where D is the shared domain iff, by IH, $\mathcal{I}(\frac{d}{x}) \models \phi_1$ for some $d \in D$ iff $\mathcal{I} \models \exists x \phi_1$. The case when $\phi \equiv \forall x \phi_1$ is similar.

If $\phi \equiv \neg \phi_1$ then $\mathcal{J} \models \neg \phi_1$ iff $\mathcal{J} \not\models \phi_1$ iff, by IH, $\mathcal{I} \not\models \phi_1$, iff $\mathcal{I} \models \neg \phi_1$. The remaining propositional cases for ϕ are similar. □

5.2.8 Lemma (Reduction to identity interpretations). *To every interpretation $\mathcal{I}$ for $\mathcal{L}$ there is an equivalent identity interpretation $\mathcal{J}$ for $\mathcal{L}$.*

Proof. Take any interpretation $\mathcal{I} = \langle \mathcal{M}, a \rangle$ for $\mathcal{L}$. We construct the identity interpretation $\mathcal{J} = \langle Q, \mathcal{M}, a \rangle$ by defining

$$Q = \{\psi \mid \mathcal{I} \models \psi \text{ for quantifier formulas } \psi\} .$$

Note that the assignment a in $\mathcal{I}$ is also an assignment in $\mathcal{J}$ because both interpretations share the structure $\mathcal{M}$. For the same reason we have

$$\tau^{\mathcal{J}} = \tau^{\mathcal{I}} \tag{1}$$

for every term τ of $\mathcal{L}$.

We prove the equivalence of $\mathcal{J}$ and $\mathcal{I}$ by proving $\mathcal{J} \models \phi \Leftrightarrow \mathcal{I} \models \phi$ by induction on construction of formulas ϕ of $\mathcal{L}$. If ϕ is a quantifier formula then $\mathcal{J} \models \phi$ iff $\phi \in Q$ iff $\mathcal{I} \models \phi$. If $\phi \equiv \tau_1 = \tau_2$ then $\mathcal{J} \models \tau_1 = \tau_2$ iff $\tau_1^{\mathcal{J}} = \tau_2^{\mathcal{J}}$ iff, by (1), $\tau_1^{\mathcal{I}} = \tau_2^{\mathcal{I}}$ iff $\mathcal{I} \models \tau_1 = \tau_2$. If $\phi \equiv P(\tau_1, \ldots, \tau_n)$ then $\mathcal{J} \models P(\tau_1, \ldots, \tau_n)$ iff $\langle \tau_1^{\mathcal{J}}, \ldots, \tau_n^{\mathcal{J}} \rangle \in P^{\mathcal{M}}$ iff, by (1), $\langle \tau_1^{\mathcal{I}}, \ldots, \tau_n^{\mathcal{I}} \rangle \in P^{\mathcal{M}}$ iff $\mathcal{I} \models P(\tau_1, \ldots, \tau_n)$. If $\phi \equiv \phi_1 \vee \phi_2$ then we have $\mathcal{J} \models \phi_1 \vee \phi_2$ iff $\mathcal{J} \models \phi_1$ or $\mathcal{J} \models \phi_2$ iff, by IH, $\mathcal{I} \models \phi_1$ or $\mathcal{I} \models \phi_2$ iff $\mathcal{I} \models \phi_1 \vee \phi_2$. The remaining cases are similar. □

5.2.9 Logical consequence. Fix a language $\mathcal{L}$ and let T be a set of formulas from $\mathcal{L}$. We define the relation ϕ *is a logical consequence of* T, in symbols $T \models \phi$, as follows:

$$T \models \phi \Leftrightarrow (\mathcal{I} \models T \Rightarrow \mathcal{I} \models \phi) \text{ for all interpretations } \mathcal{I}.$$

We write $\models \phi$ for $\emptyset \models \phi$ and such a ϕ is a *valid* formula. Note that we have

$$\models \phi \Leftrightarrow \mathcal{I} \models \phi \text{ for all interpretations } \mathcal{I}.$$

If T is closed then we have $T \models \phi$ iff $\mathcal{M} \models \phi$ for all models of T.

The following lemma asserts that the instantiation axioms are valid and that Henkin counterexample axioms are logical consequences of Ha. Hence, Qa is staisfied in every Henkin interpretation.

5.2.10 Lemma.

$$\models \phi_x[\tau] \rightarrow \exists x\phi \qquad \tau,\ \phi \textit{ of any } \mathcal{L},\ \tau \textit{ free for } x \textit{ in } \phi \tag{1}$$

$$\models \forall x\phi \rightarrow \phi_x[\tau] \qquad \tau,\ \phi \textit{ of any } \mathcal{L},\ \tau \textit{ free for } x \textit{ in } \phi \tag{2}$$

$$Ha \models Qa\ . \tag{3}$$

Proof. (1): Take any interpretation $\mathcal{I}$ for $\mathcal{L}$ with the domain D and any formula $\phi_x[\tau] \rightarrow \exists x\phi$ satisfying the assumptions. Assume $\mathcal{I} \models \phi_x[\tau]$ and obtain $\mathcal{I}(\,{}^{\tau^{\mathcal{I}}}_{x}\,) \models \phi$ by Lemma 5.2.4. Since $\tau^{\mathcal{I}} \in D$ we get $\mathcal{I} \models \exists x\phi$.

(2): the proof is similar to that of (1).

(3): Take any Henkin interpretation $\mathcal{I}$ for $\mathcal{L}_c$ with the domain D and any $\psi \in Qa$. If $\psi \in Ha$ we have $\mathcal{I} \models \psi$ trivially and if ψ is an instantiation axiom we get the same by (1) or (2) because the term τ is closed and so it is free for x in ϕ. If ψ is a counterexample axiom of a form $\phi_x[c] \to \forall x\phi$ then $\exists x\neg\phi \to \neg\phi_x[c] \in Ha$ and so $\mathcal{I} \models \exists x\neg\phi \to \neg\phi_x[c]$. We now assume $\mathcal{I} \models \phi_x[c]$ and obtain $\mathcal{I} \not\models \neg\phi_x[c]$ and then $\mathcal{I} \not\models \exists x\neg\phi$. But then $\mathcal{I}(\,{}^{d}_{x}\,) \not\models \neg\phi$, i.e. $\mathcal{I}(\,{}^{d}_{x}\,) \models \phi$, for all $d \in D$ and so $\mathcal{I} \models \forall x\phi$. $\square$

5.2.11 Remark. Why did we impose the freeness restriction on substitutions into quantified formulas. We did this because we wish the instantiation formulas 5.2.10(1) and 5.2.10(2) to be valid.

For instance, consider the formula $\exists y\, y \neq x$. We have $(\exists y\, y \neq x)_x[y] \equiv \exists y\, y \neq y$. The formula $\forall x \exists y\, y \neq x \to (\exists y\, y \neq x)_x[y]$, i.e. the formula

$$\forall x \exists y\, y \neq x \to \exists y\, y \neq y$$

has the form of 5.2.10(2) but the term y is not free for x in $\exists y\, y \neq x$. This violation of the substitution condition prevents the formula from being valid. This can be seen by noting that $\mathcal{I} \models \forall x \exists y\, y \neq x$ holds for any interpretation $\mathcal{I}$ with at least two elements in its domain whereas $\mathcal{I} \models \exists y\, y \neq y$ is satisfied for no interpretation $\mathcal{I}$.

5.2.12 Lemma (Henkin expansion). *For every interpretation $\mathcal{I}$ for $\mathcal{L}$ there is a Henkin expansion $\mathcal{J}$ for $\mathcal{L}_c$.*

Proof. Take any interpretation $\mathcal{I} = \langle \mathcal{M}, a \rangle$ for $\mathcal{L}$ and let D be the domain of $\mathcal{M}$. We wish to construct the interpretation $\mathcal{J} = \langle \mathcal{N}, a \rangle$ as an expansion of $\mathcal{I}$ satisfying Ha. To that end we define for $i \geq 0$ a sequence of interpretations $\mathcal{J}_i = \langle \mathcal{N}_i, a \rangle$ with the structures $\mathcal{N}_i$ for languages $\mathcal{L}_i$. We define $\mathcal{L}_0 = \mathcal{L}$ and $\mathcal{L}_{i+1}$ as the extension of $\mathcal{L}_i$ with the Henkin constants of rank $i+1$. Thus $\mathcal{L}_i$ contains all Henkin constants with ranks $\leq i$. We define the structures $\mathcal{N}_i$ and thus also the interpretations $\mathcal{J}_i$ by induction on i in such a way that $\mathcal{J}_{i+1}$ will be an expansion of $\mathcal{J}_i$ and for all Henkin constants c of rank $i+1$ belonging to sentences $\exists x\phi$ of $\mathcal{L}_i$ of rank i we will have

$$\mathcal{J}_{i+1} \models \exists x\phi \to \phi_x[c]\ . \tag{1}$$

In the base case we set $\mathcal{N}_0 = \mathcal{M}$ and so $\mathcal{J}_0 = \mathcal{I}$. In the inductive case we take any Henkin constant c of rank $i+1$. The constant belongs to a sentence $\exists x\phi$ of $\mathcal{L}_i$ which is of rank i and we consider two cases. If $\mathcal{J}_i \models \exists x\phi$ holds then $\mathcal{J}_i(\,{}^{d}_{x}\,) \models \phi$ for some $d \in D$ and we interpret $c^{\mathcal{N}_{i+1}} = d$. If $\mathcal{J}_i \not\models \exists x\phi$ then we interpret $c^{\mathcal{N}_{i+1}} = d$ where d is arbitrary element of D. This ends the definition of $\mathcal{N}_{i+1}$. The interpreation $\mathcal{J}_{i+1}$ is an expansion of $\mathcal{J}_i$ and they are equivalent on the formulas of $\mathcal{L}_i$ by Lemma 5.2.7. For every Henkin constant c if rank $i+1$ we prove (1) by considering the same two cases again. If $\mathcal{J}_i \models \exists x\phi$ holds then we have $\mathcal{J}_{i+1} \models \exists x\phi$ and $\mathcal{J}_{i+1}(\,{}^{c^{\mathcal{N}_i}}_{x}\,) \models \phi$ by the interpretation of c.

We obtain $\mathcal{J}_{i+1} \vDash \phi_x[c]$ by Lemma 5.2.4. This satisfies (1). If $\mathcal{J}_i \nvDash \exists x\phi$ then we have $\mathcal{J}_{i+1} \nvDash \exists x\phi$ and so (1) holds again.

With the construction of interpretations $\mathcal{J}_i$ done we note that whenever $0 \leq i < j$ the language $\mathcal{L}_j$ is an extension of $\mathcal{L}_i$, $\mathcal{J}_j$ is an expansion of $\mathcal{J}_i$, and the interpretations are equivalent on $\mathcal{L}_i$ by Lemma 5.2.7. Thus $\mathcal{J}_j$ satisfies the axioms of *Ha* whose Henkin constants have ranks $\leq j$. We also have $\mathcal{J}_i \equiv_{\mathcal{L}} \mathcal{I}$. We now construct the interpretation $\mathcal{J} = \langle \mathcal{N}, a \rangle$ for $\mathcal{L}_c$ as an expansion of $\mathcal{I}$ where the structure $\mathcal{N}$ is an expansion of $\mathcal{M}$ interpreting Henkin constants of rank i in the same way as $\mathcal{J}_i$. Thus $\mathcal{J} \equiv_{\mathcal{L}} \mathcal{I}$ and, since $\mathcal{J}$ is also an expansion of every $\mathcal{J}_i$ and thus $\mathcal{J} \equiv_{\mathcal{L}_i} \mathcal{J}_i$ by Lemma 5.2.7, we have $\mathcal{J} \vDash Ha$. □

5.2.13 Lemma (Expansion of identity interpretations). *For every $\mathcal{L}$ and every identity interpretation $\mathcal{I}$ for $\mathcal{L}_c$ such that $\mathcal{I} \vDash Qa$ there is a canonical Henkin interpretation $\mathcal{J}$ for $\mathcal{L}_c$ equivalent to $\mathcal{I}$ on the sentences of $\mathcal{L}_c$.*

Proof. Take any identity interpretation $\mathcal{I}$ for $\mathcal{L}_c$ such that $\mathcal{I} \vDash Qa$. Let T be the set of sentences of $\mathcal{L}_c$. We obtain a T-equivalent canonical identity interpretation $\mathcal{I}_1 = \langle Q, \mathcal{M}, a \rangle$ for a structure $\mathcal{M}$ with the domain D and an assignment a by Lemma 4.2.14. The set $FT(T)$ is not empty because it contains at least the Henkin constants and its elements are closed terms. Thus for every $d \in D$ there is a closed term $\tau \in FT(T)$ such that $\tau^{\mathcal{I}_1} = d$. Since $Qa \subseteq T$ we have $\mathcal{I}_1 \vDash Qa$. We construct the interpretation $\mathcal{J} = \langle \mathcal{M}, a \rangle$ which is canonical because

$$\tau^{\mathcal{J}} = \tau^{\mathcal{I}_1} \tag{1}$$

holds. By induction on the structure of formulas ϕ we prove

$$\phi \in T \Rightarrow (\mathcal{J} \vDash \phi \Leftrightarrow \mathcal{I}_1 \vDash \phi)\ . \tag{2}$$

Thus assume $\phi \in T$ and if $\phi \equiv \tau_1 = \tau_2$ then we have $\mathcal{J} \vDash \tau_1 = \tau_2$ iff $\tau_1^{\mathcal{J}} = \tau_2^{\mathcal{J}}$ iff, by (1), $\tau_1^{\mathcal{I}_1} = \tau_2^{\mathcal{I}_1}$ iff $\mathcal{I}_1 \vDash \tau_1 = \tau_2$.

If $\phi \equiv P(\tau_1, \ldots, \tau_n)$ then we have $\mathcal{J} \vDash P(\tau_1, \ldots, \tau_n)$ iff $\langle \tau_1^{\mathcal{J}}, \ldots, \tau_n^{\mathcal{J}} \rangle \in P^{\mathcal{M}}$ iff, by (1), $\langle \tau_1^{\mathcal{I}_1}, \ldots, \tau_n^{\mathcal{I}_1} \rangle \in P^{\mathcal{M}}$ iff $\mathcal{I}_1 \vDash P(\tau_1, \ldots, \tau_n)$.

If $\phi \equiv \exists x\phi_1$ then if $\mathcal{J} \vDash \exists x\phi_1$ holds we have $\mathcal{J}(\tfrac{d}{x}) \vDash \phi_1$ for some $d \in D$. There is a closed term τ of $\mathcal{L}_c$ such that $\tau^{\mathcal{J}} \overset{(1)}{=} \tau^{\mathcal{I}_1} = d$ and so $\mathcal{J}(\tfrac{\tau^{\mathcal{J}}}{x}) \vDash \phi_1$ and we obtain $\mathcal{J} \vDash {\phi_1}_x[\tau]$ by Lemma 5.2.4. Because ${\phi_1}_x[\tau] \in T$ we obtain $\mathcal{I}_1 \vDash {\phi_1}_x[\tau]$ by IH and, since ${\phi_1}_x[\tau] \rightarrow \exists x\phi \in Qa$, we get $\mathcal{I}_1 \vDash \exists x\phi_1$.

Vice versa, if $\mathcal{I}_1 \vDash \exists x\phi_1$ holds then we have $\exists x\phi \rightarrow {\phi_1}_x[c] \in Qa$ for the Henkin constant c belonging to $\exists x\phi$. From $\mathcal{I}_1 \vDash \exists x\phi \rightarrow {\phi_1}_x[c]$ we get $\mathcal{I}_1 \vDash {\phi_1}_x[c]$ and then $\mathcal{J} \vDash {\phi_1}_x[c]$ by IH. Hence $\mathcal{J}(\tfrac{c^{\mathcal{J}}}{x}) \vDash \phi_1$ by Lemma 5.2.4 and so $\mathcal{J} \vDash \exists x\phi_1$ holds. The case when $\phi \equiv \forall x\phi_1$ is similar.

If $\phi \equiv \phi_1 \vee \phi_2$ then $\mathcal{J} \vDash \phi_1 \vee \phi_2$ iff $\mathcal{J} \vDash \phi_1$ or $\mathcal{J} \vDash \phi_2$ iff, since $\phi_1, \phi_2 \in T$, we have by IH $\mathcal{I}_1 \vDash \phi_1$ or $\mathcal{I}_1 \vDash \phi_2$ iff $\mathcal{I}_1 \vDash \phi_1 \vee \phi_2$. The remaining cases for ϕ are similar.

We have $\mathcal{I} \equiv_T \mathcal{I}_1$ from the construction of $\mathcal{I}_1$. From (2) we get $\mathcal{I}_1 \equiv_T \mathcal{J}$ and so $\mathcal{I} \equiv_T \mathcal{J}$ holds.

The reader will note that the use of Henkin axioms in the inductive proof of (2) works only when T consists of sentences and so the lemma cannot be extended to the formulas of $\mathcal{L}$. $\square$

5.2.14 Theorem. *If $\mathcal{I}$ is an interpretation for $\mathcal{L}$ then there is a canonical interpretation $\mathcal{J}$ for $\mathcal{L}$ equivalent to $\mathcal{I}$ on the sentences of $\mathcal{L}$.*

Proof. For a given interpretation $\mathcal{I}$ for $\mathcal{L}$ we obtain a Henkin expansion $\mathcal{I}_1$ for $\mathcal{L}_c$ by Lemma 5.2.12 and we have $\mathcal{I}_1 \equiv_{\mathcal{L}} \mathcal{I}$ by Lemma 5.2.7. We then get $\mathcal{I}_1 \models Qa$ by 5.2.10(3) and obtain an identity interpretation $\mathcal{I}_2$ for $\mathcal{L}_c$ equivalent to $\mathcal{I}_1$ by Lemma 5.2.8. Since then $\mathcal{I}_2 \models Qa$ holds, we get a canonical interpretation $\mathcal{J}$ for $\mathcal{L}_c$ equivalent to $\mathcal{I}_2$ on the sentences of $\mathcal{L}_c$ by Lemma 5.2.13. Since the sentences of $\mathcal{L}$ are sentences of $\mathcal{L}_c$, the interpretation $\mathcal{I}$ is equivalent to $\mathcal{J}$ on the sentences of $\mathcal{L}$. $\square$

5.2.15 Theorem (Henkin reduction). *If ϕ and T consist of sentences of $\mathcal{L}$ then*

$$T \models \phi \Leftrightarrow T, Qa \models_i \phi \ . \tag{1}$$

Proof. In the direction ($\Rightarrow$) assume $T \models \phi$ and take any identity interpretation $\mathcal{I}$ for $\mathcal{L}_c$ such that $\mathcal{I} \models T \cup Qa$. There is an interpretation $\mathcal{J}$ for $\mathcal{L}_c$ equivalent to $\mathcal{I}$ on the sentences of $\mathcal{L}_c$ by Lemma 5.2.13. Since the sentences of $\mathcal{L}$ are sentences of $\mathcal{L}_c$, we have $\mathcal{J} \models T$ and hence $\mathcal{J} \models \phi$ from the assumption. But then $\mathcal{I} \models \phi$ by the equivalence.

In the direction ($\Leftarrow$) assume $T, Qa \models_i \phi$ and take any interpretation $\mathcal{I}$ for $\mathcal{L}$ such that $\mathcal{I} \models T$ holds. There is a Henkin expansion $\mathcal{I}_1$ for $\mathcal{L}_c$ by Lemma 5.2.12 which is equivalent to $\mathcal{I}$ on the formulas of $\mathcal{L}$ by Lemma 5.2.7. Thus $\mathcal{I}_1 \models T$ and we also have $\mathcal{I}_1 \models Qa$ by 5.2.10(3). There is an identity interpretation $\mathcal{J}$ for $\mathcal{L}_c$ equivalent to $\mathcal{I}_1$ by Lemma 5.2.8. Hence $\mathcal{J} \models T \cup Qa$ and we get $\mathcal{J} \models \phi$ from the assumption and $\mathcal{I} \models \phi$ by the equivalence. $\square$

5.2.16 Theorem. *If ϕ and T consist of sentences of $\mathcal{L}$ then*

$$T \models_i \phi \Rightarrow T \models \phi \ .$$

Proof. If $T \models_i \phi$ holds then we have $T, Qa \models_i \phi$ by weakening and $T \models \phi$ by Thm. 5.2.15. $\square$

5.2.17 Theorem (Generalization). *If T is closed and ϕ a formula of some $\mathcal{L}$ then*

$$T \models \phi \Leftrightarrow T \models \forall\phi \ .$$

Proof. The theorem is proved by a repeated application of an auxiliary assertion

$$T \models \phi \Leftrightarrow T \models \forall x\phi$$

which is proved in the direction $(\rightarrow)$ by assuming $T \models \phi$ and taking any interpretation for $\mathcal{L}$ with a domain D such that $\mathcal{I} \models T$. For any $d \in D$ interpretations $\mathcal{I}(\frac{d}{x})$ and $\mathcal{I}$ agree on $FV(T)$ because T is closed and so $\mathcal{I}(\frac{d}{x}) \models T$ by Lemma 5.2.3. Thus $\mathcal{I}(\frac{d}{x}) \models \phi$ from the assumption and so $\mathcal{I} \models \forall x\phi$.

In the direction $(\leftarrow)$ we assume $T \models \forall x\phi$ and take any interpretation for $\mathcal{L}$ such that $\mathcal{I} \models T$. Thus $\mathcal{I} \models \forall x\phi$ and, since $\phi_x[x] \equiv \phi$, we obtain $\mathcal{I} \models \phi$ by 5.2.10(2). ☐

5.2.18 Theorem (Skolem-Löwenheim). *If T is a set of sentences of some $\mathcal{L}$ and ϕ a formula of $\mathcal{L}$ then*

1. *if T is satisfiable then T has a numerical model,*
2. *$T \models \phi$ iff ϕ is true in all numerical models of T.*

Proof. 1) If T is is satisfiable then it has a model $\mathcal{M}$, i.e. $\mathcal{M} \models T$. Since T is a set of sentences we have $\langle \mathcal{M}, a\rangle \models T$ for any assignment a in $\mathcal{M}$. There is a canonical interpretation $\mathcal{J}$ such that $\mathcal{J} \models T$ by Thm. 5.2.14. Thus $\mathcal{J} = \langle \mathcal{N}, b\rangle$ for a numerical structure $\mathcal{N}$ and an assignment b in $\mathcal{N}$. But then $\mathcal{N} \models T$.

2) The direction $(\rightarrow)$ is trivial. In the direction $(\leftarrow)$ assume $T \not\models \phi$. Thus T has a model $\mathcal{M}$ in which $\mathcal{M} \not\models \phi$, i.e. $\mathcal{M} \models \neg\forall\phi$ by Thm. 5.2.17 and so there is a numerical model $\mathcal{N}$ of $T, \neg\forall\phi$ by 1). Thus $\mathcal{N}$ is a model of T s.t. $\mathcal{N} \not\models \forall\phi$, i.e. $\mathcal{N} \not\models \phi$. ☐

5.2.19 Import of Skolem-Löwenheim's theorem. This paragraph is not yet finished. Numeric structures are the most important ones. The next two parts of this text are devoted to the study of theorems true in the most important numeric structure: the standard model of Peano Arithmetic.

5.3 Quantification Tableaux

5.3.1 Tableau expansion rules. Fix a language $\mathcal{L}$. All expansion rules for (quantifier) tableaux are unary. *Quantifier instantiation* rules are

$$\frac{\forall x\phi}{\phi_x[\tau]}\,(\forall) \qquad \frac{\exists x\phi*}{\phi_x[\tau]*}\,(\exists*)$$

for all formulas ϕ, variables x, and terms τ free for x in ϕ. *Eigen-variable* rules are

$$\frac{\exists x\phi}{\phi_x[y]}\,(\exists) \qquad\qquad \frac{\forall x\phi *}{\phi_x[y]*}\,(\forall *)$$

for all formulas ϕ, variables x, and *eigen-variables* y free for x in ϕ.

The reader will note that the instantiation rules corrrespond to the valid formulas 5.2.10(2)(2) and the eigen-variable rules to Henkin axioms.

5.3.2 Proofs with tableaux. A tableau π for a sequence of signed formulas Δ from axioms in T is called a *tableau for Δ from axioms T* if every eigen-variable y in π satisfies the *eigen-variable condition* that it is not free in any signed formula in the branch above the conclusion of the corresponding eigen-variable rule and neither it is free in T. If π is closed then we assert this by writing $\pi : T \vdash [\Delta]$. The requirement that the eigen-variables be not free in axioms are not that severe as they might look because our axioms will be mostly closed.

When $\Delta \equiv \phi*$ then we say that π *is a tableau proving ϕ from axioms T* and write it as $\pi : T \vdash \phi$. We use additional abbreviations similar to those discussed in Par. 3.2.4.

We first adapt to quantifier tableaux some of the theorems formulated for propositional tableaux.

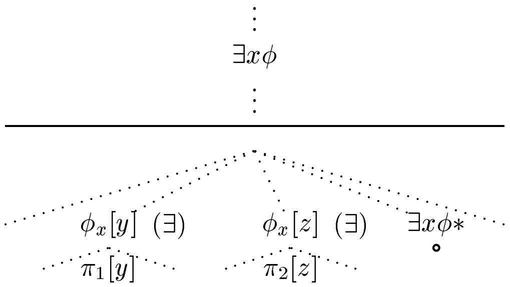
5.3.3 Theorem (Admissible rules in tableaux). *Generalized flatten (see Thm. 3.3.2), generalized split (see Thm. 3.3.3), and propositional inversion (see Thm. 3.3.5) are admissible in any tableaux. Inversion rules for* $(\exists)$ *and* $(\forall *)$*:*

$$T \vdash [\Delta, \exists x\phi] \Rightarrow \pi : T \vdash [\Delta, \phi_x[y]] \quad \text{for a } y \text{ and } \pi \text{ with no } (\exists) \text{ on } \exists x\phi$$
$$T \vdash [\Delta, \forall x\phi *] \Rightarrow \pi : T \vdash [\Delta, \phi_x[y]*] \quad \text{for a } y \text{ and } \pi \text{ with no } (\forall *) \text{ on } \forall x\phi * .$$

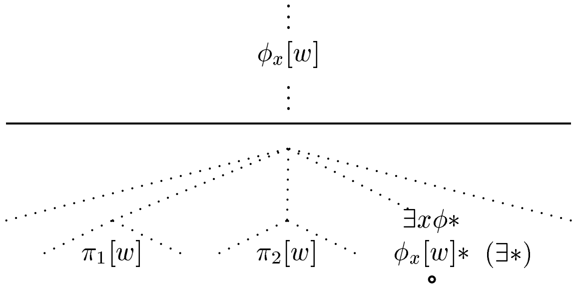
are admissible in tableaux with closed axioms T.

Proof. Inspection of proofs of admissibility of expansion generalized flatten and split rules as well as of propositional inversion rules reveals that the proofs remain correct also for (quantifier) tableaux; the presence of quantifier and identity rules does not affect the proofs.

We prove just that the inversion of $(\exists)$ rule is admissible, the proof of the inversion of $(\forall *)$ is similar. Consider the following closed tableau



where we have indicated three out of possibly many uses of the assumption $\exists x\phi$. The first two uses are by $(\exists)$ rules with the eigen-variables y and z and the third use closes the branch. The following closed tableau shows the inverted rule:



where we have chosen a new variable w, removed the two conclusions of $(\exists)$ rules (since they occur above), systematically renamed the variables y and z to w in the tableaux $\phi_1[y]$ and $\phi_2[z]$, and closed the branch containing the goal $\exists x\phi*$ with a $(\exists *)$ rule. Note that we can always find a new variable w because there are only finitely many of them free or bound in the tableau. This makes w free for x in ϕ and free for y and z in the quantified formulas of π_1 and π_2. Also note that the renaming of variables does not affect any axiom expansions because they are sentences. $\square$

5.3.4 Syntactic compactness and deduction theorems.

$$T \vdash \phi \Rightarrow S \vdash \phi \qquad \text{finite } S \subseteq T \tag{1}$$

$$S \vdash \phi \Leftrightarrow \ \vdash \bigwedge S \to \phi \qquad S \text{ finite.} \tag{2}$$

Proof. (1): This is the theorem on syntactic compactness 3.5.5 whose proof directly lifts up to the general tableaux.

(2): This is the Deduction theorem 3.5.6 whose proof directly lifts up to the general tableaux. $\square$

5.3.5 Renaming lemma. *If T in $\mathcal{L}$ is closed, $\Delta[\vec{x}]$ is a sequence of formulas of $\mathcal{L}$ with all free variables among the indicated ones, and the variables in $\vec{y}$ are free for the corresponding variables in Δ then*

$$\pi : T \vdash \Delta[\vec{x}] \Rightarrow T \vdash \Delta[\vec{y}] \ .$$

Proof. By induction on the number of expansions in π. If π is empty then whatever closes $\Delta[\vec{x}]$ must close $\Delta[\vec{y}]$. If the last expansion in π is by a rule which does not introduce new variables, say $(\neg *)$, then, for a premise $\neg\phi[\vec{x}]* \in \Delta[\vec{x}]$, we show the tableau π on the left:

$$\begin{array}{c}\Delta[\vec{x}]\\ \hline \phi[\vec{x}] \quad (\neg *)\\ \cdots\pi_1\cdots\end{array} \quad \Rightarrow \quad \begin{array}{c}\Delta[\vec{y}]\\ \hline \phi[\vec{y}] \quad (\neg *)\\ \cdots\pi_1'\cdots\end{array}$$

We have $\pi_1 : T \vdash [\Delta[\vec{x}], \phi[\vec{x}]]$ and we obtain $\pi_1' : T \vdash [\Delta[\vec{y}], \phi[\vec{y}]]$ for some π_1' by IH. We construct the tableu π' shown on the right. Note that $\neg\phi[\vec{y}]* \in \Delta[\vec{y}]$ and thus $\pi' : T \vdash \Delta[\vec{y}]$.

$(\neg *)$ rules, remaining propositional rules, as well as all identity rules except reflexivity, are rules which do not introduce new variables and they are invariant to systematic renaming of free variables in their premises and conclusions.

If the first expansion in π is by a rule which may introduce new variables, say $(\exists)$, then, for a premise $\exists v\phi[v, \vec{x}]* \in \Delta[\vec{x}]$ we show the tableau π on the left:

$$\begin{array}{c}\Delta[\vec{x}]\\ \hline \phi[\tau[\vec{z}, \vec{x}], \vec{x}] \quad (\exists)\\ \cdots\pi_1\cdots\end{array} \quad \Rightarrow \quad \begin{array}{c}\Delta[\vec{y}]\\ \hline \phi[\tau[\vec{z}, \vec{y}], \vec{y}] \quad (\exists)\\ \cdots\pi_1'\cdots\end{array}$$

We have $\pi_1 : T \vdash [\Delta[\vec{x}], \phi[\tau[\vec{z}, \vec{x}], \vec{x}]]$ an we obtain $\pi_1' : T \vdash [\Delta[\vec{y}], \phi[\tau[\vec{z}, \vec{y}], \vec{y}]]$ for some π_1' by IH. We construct the tableau π' shown on the right. Note that $\exists v\phi[v, \vec{y}]* \in \Delta[\vec{y}]$ and thus $\pi' : T \vdash [\Delta[\vec{y}]]$.

$(\exists)$ rules, remaining quantifier rules, axiom rules, as well as reflexivity rules, may introduce new variables into tableaux. All but the axiom rules are invariant to systematic renaming of free variables in their premises and conclusions. We have assumed that the axioms in T are closed which makes the axiom rules invariant to renaming too. □

5.3.6 Lemma (Admissibility of cuts on propositional formulas). *If the cut rules on all propositional atoms in a formula ϕ are admissible in (quantifier) tableaux then also the cut rule on ϕ is admissible.*

Proof. Inspection of the proof of the similar Lemma 3.3.7 for propositional tableaux reveals that the lemma holds also for tableaux (with identity and quantifier rules). □

5.3.7 Theorem (Admissibility of cuts). *Cut rules on arbitrary formulas are admissible in tableaux with closed axioms.*

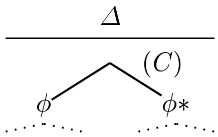
Proof. For the duration of this proof we call a tableau $\pi : T \vdash [\Delta]$ *normal* if

1. the axioms T are sentences,
2. free variables in the formulas of Δ and π are disjoint with all bound variables used in Δ and π,
3. all new variables introduced into π by the reflexivity, instantiation, and eigen-variable rules are pairwise distinct.

We prove

> if π is a normal closed tableau from T for Δ with a cut on the formula ϕ as the first and only expansion by a cut in π then there is a tableau π' such that $\pi' : T \vdash [\Delta]$

by induction on the number of propositional connectives and quantifiers in the cut formula ϕ. The tableau π can be visualized as follows

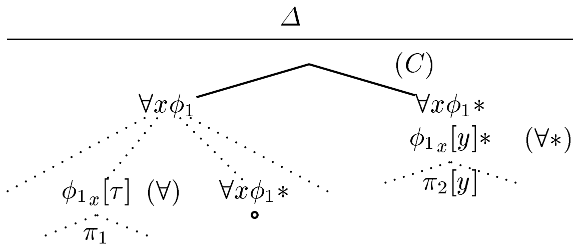


(1)

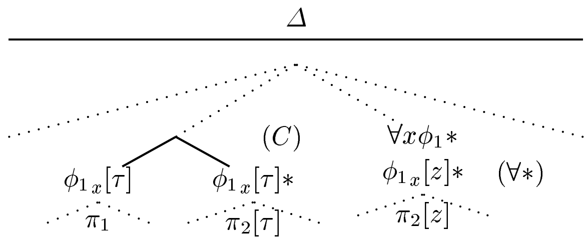
If ϕ is an atomic formula then the cut on ϕ is admissible by the same argument as in Lemma 3.3.8 (taking into account the comment on cuts on identity formulas in Thm. 4.3.3).

If ϕ is a propositional formula then cuts on all propositional atoms in ϕ are admissible by IH and so the cut on ϕ is admissible by Lemma 5.3.6.

If $\phi \equiv \forall x \phi_1$ then (1) looks as follows:



where we may assume without loss of generality that the $(\forall *)$ rule on the right has been inverted. Thus the goal $\forall x \phi_1 *$ is not used for anything in the tableau $\pi_2[y]$. We have also indicated on the left one of possibly many uses of the assumption $\forall x \phi_1$ in an $(\forall)$ rule and in the closing of a branch. We transform π into π' by modifying the tableau under the assumption $\forall x \phi_1$:



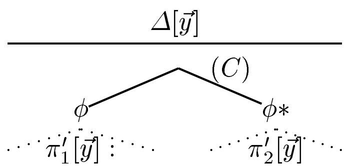
where we replace every use of a $(\forall)$ rule with the conclusion ${\phi_1}_x[\tau]$ by a cut on this formula. The branch leading to the goal ${\phi_1}_x[\tau]*$ is closed by the tableau

$\pi_2[\tau]$ obtained from $\pi_2[y]$ by substituting for the eigen-variable y the term τ. The substitution cannot affect axiom expansions in $\pi_2[y]$ because they are closed by 1). Furthermore, no variable free in τ is bound anywhere in $\pi_2[y]$ by 2) and so all substitutions are free. Finally, no eigen-variable condition on any eigen-variable w in $pi_2[\tau]$ is violated because w cannot be introduced into the branch leading to ${\phi_1}_x[\tau]*$ by 3).

We also apply a $(\forall *)$ rule with new eigen-variables z everywhere where the assumption $\forall x \phi_1$ was used for closing. We restore the normality of π' if needed by renaming with new variables all variables introduced in the possibly many copies of $\pi_2[y]$. The tableau π' clearly does not use the assumption $\forall x \phi_1$ and the cuts on all formulas ${\phi_1}_x[\tau]$ are admissible by IH. Hence $\pi' : T \vdash [\Delta]$ holds.

The case when $\phi \equiv \exists x \phi_1$ is proved similarly.

In order to finish the proof we must show how to convert the tableau (1) into a normal tableau. The tableau consists of two branches such that $\pi_1[\vec{x}] : T \vdash [\Delta[\vec{x}], \phi[\vec{x}]]$ and $\pi_2[\vec{x}] : T \vdash [\Delta[\vec{x}], \phi[\vec{x}]*]$. We have indicated all free variables in Δ and ϕ. The condition 1) is satisfied by the assumption of the theorem that T is closed. We satisfy the conditions 2) and 3) by choosing new variables $\vec{y}$ and systematically renaming to new variables the free variables introduced into π_1 and π_2. In this way we obtain $\pi'_1[\vec{y}] : T \vdash [\Delta[\vec{y}], \phi[\vec{y}]]$, $\pi'_2[\vec{y}] : T \vdash [\Delta[\vec{y}], \phi[\vec{y}]*]$ for some π'_1 and π'_2 by Lemma 5.3.5. The tableau



is normal, its cut is admissible, and we obtain $\pi' : T \vdash \Delta[\vec{y}]$ for a cut-free π'. We now apply Lemma 5.3.5 again to get $T \vdash \Delta[\vec{x}]$. □

5.3.8 Theorem (Admissibility of the generalization rule). *If T is closed and ϕ a formula of some $\mathcal{L}$ then*

$$T \vdash \phi \Leftrightarrow T \vdash \forall \phi \ .$$

Proof. The theorem is proved by a repeated application of an auxiliary assertion

$$T \vdash \phi \Leftrightarrow T \vdash \forall x \phi$$

which is proved in the direction $(\rightarrow)$ by assuming $\pi_1 : T \vdash \phi$ for some π_1 and constructing the tableau π':

$$\begin{array}{c} \forall x \phi * \\ \hline \phi \qquad (\forall *) \\ \cdots \pi_1 \cdots \end{array}$$

for the eigen-variable x where we note that $\phi_x[x] \equiv \phi$. Thus $\pi' : T \vdash \forall x\phi$.

In the direction ($\leftarrow$) we assume $\pi : T \vdash \forall \phi$. The tableau can be presented by $(\forall)*$ inversion for some w as follows:

$$
\begin{array}{cc}
\forall x\phi \, * & \\
\hline
\phi_x[w] & (\forall *) \\
\vdots \, \pi_1 &
\end{array}
$$

We have $\pi_1 : T \vdash \phi_x[w]$ from which we obtain $T \vdash \phi$ by Lemma 5.3.5 because $\phi_x[x] \equiv \phi$. □

5.3.9 Lemma. $Ha \vdash Qa$.

Proof. Take any $\psi \in Q$ and consider four cases. If ψ is an existential instantiation axiom $\phi_x[\tau] \to \exists x\phi$ then we can prove it even without Henkin axioms:

$$
\begin{array}{cc}
\phi_x[\tau] \to \exists x\phi \, * & \\
\hline
\phi_x[\tau] & (\to_1 *) \\
\exists x\phi * & (\to_2 *) \\
\phi_x[\tau] * & (\exists *) \\
\circ &
\end{array}
$$

If ψ is an universal instantiation axiom $\forall x\phi \to \phi_x[\tau]$ then the proof is similar.

If ψ is a witnessing axiom $\exists x\phi \to \phi_x[c]$ then we construct the following one expansion tableau:

$$
\begin{array}{cc}
\exists x\phi \to \phi_x[c] \, * & \\
\hline
\exists x\phi \to \phi_x[c] & (Ax) \\
\circ &
\end{array}
$$

If ψ is a counterexample axiom $\phi_x[c] \to \forall x\phi$ then the Henkin constant is shared with the witnessing axiom: $\exists x\neg\phi \to \neg\phi_x[c]$. We prove ψ with a new eigen-variable z as follows:

$$
\begin{array}{c}
\phi_x[c] \to \forall x\phi * \\
\hline
\exists x\neg\phi \to \neg\phi_x[c] \quad (Ax) \\
(\to) \\
\begin{array}{cc|cc}
\neg\phi_x[c] & & \exists x\neg\phi * & \\
\phi_x[c]* & (\neg) & \forall x\phi * & (\to_2 *) \\
\phi_x[c] & (\to_1 *) & \phi_x[z]* & (\forall *) \\
\circ & & \neg\phi_x[z]* & (\exists *) \\
 & & \phi_x[z] & (\neg *) \\
 & & \circ &
\end{array}
\end{array}
$$

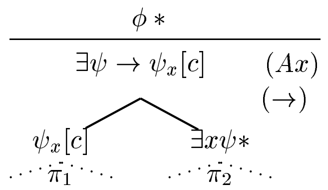
5.3.10 Theorem (Elimination of Henkin witnessing axioms). *If T and ϕ consist of sentences of a language $\mathcal{L}$ and $\mathcal{L}_c$ is its witnessing extension then*

$$T, Ha \vdash \phi \Rightarrow T \vdash \phi\ .$$

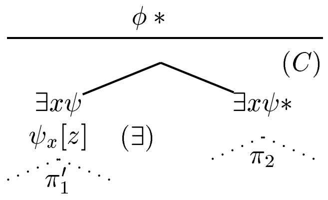
Proof. Assume $\pi : T, Ha \vdash \phi$ for closed T and ϕ. We have $\pi : T, Ha_1 \vdash \phi$ for a finite subset Ha_1 of Ha by 5.3.4(1). The theorem follows from the following assertion:

if $\pi : T, Ha_1 \vdash \phi$ for a finite subset Ha_1 of Ha then $T \vdash \phi$.

which is proved by induction on the size of Ha_1. If $Ha_1 = \emptyset$ there is nothing to prove. Otherwise select from Ha_1 a witnessing axiom $\psi_0 \equiv \exists\psi \rightarrow \psi_x[c]$ with the Henkin variable of maximal rank and denote by Ha_2 the set of remaining axioms. We may assume without loss of generality that π has the following form



where neither π_1 nor π_2 contain expansions by the axiom ψ_0. This is because we can delete all expansions by the axiom ψ_0 from π and put it as the first expansion in π. The inversion of ψ_0 can only affect eigen-variable rules but the condition that no eigen-variable occurs free in ψ_0, which is a sentence anyway, assures that the inversion is always possible. We can also invert the $(\rightarrow)$ expansion for ψ_0. We construct a tableau π' for ϕ as follows:



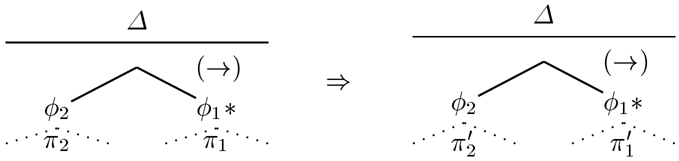
where we have replaced the expansion by ψ_0 by an admissible cut on the formula $\exists x\psi$. Its right branch is closed by π_2 and the left branch is expanded by the eigen-variable rule with a new variable z after which the branch is closed with the tableau π_1' obtained from π_1 by replacing everywhere the constant c by z. The crucial fact is that the Henkin constant c occurs neither in T nor in ϕ because these are in the language $\mathcal{L}$. Thus the axioms from T and the subformulas of ϕ occurring in π_1 are not affected by the replacement. Since c is of maximal rank in Ha_1, it occurs neither in Ha_2 nor in $\exists x\psi$. Thus neither the axioms from Ha_2 used in π_1 are affected by the replacement. We have $\pi' : T, Ha_2 \vdash \phi$ from which we obtain $T \vdash \phi$ by IH. $\square$

5.3.11 Lemma (Elimination of quantifier rules). *If T and Δ consist of sentences of a language $\mathcal{L}$ and $\mathcal{L}_c$ is its witnessing extension then*

$$\pi : T \vdash [\Delta] \Rightarrow T, Qa \vdash_i [\Delta] \ .$$

Proof. By induction on the number of expansions in the tableau π. Assume $\pi : T \vdash [\Delta]$ with closed T, Δ and consider the form of π. If π is empty then we trivially have $T \vdash_i [\Delta]$ and we obtain $T, Qa \vdash_i [\Delta]$ by weakening.

If the first expansion in π is by a propositional rule, say $(\to)$, then we have a closed $\phi_1 \to \phi_2 \in \Delta$ and π has the form shown in the following on the left:



Since ϕ_1, ϕ_2 are closed, we obtain identity tableaux π_1' and π_2' such that $\pi_1' : T, Qa \vdash_i [\Delta, \phi_1 *]$ and $\pi_2' : T, Qa \vdash_i [\Delta, \phi_2]$ by two IH's and construct the closed identity tableau for Δ from axioms T, Qa shown on the right. The remaining propositional, axiom, and all identity expansions except reflexivity are similar. This is because neither of the mentioned expansions introduces new free variables (recall axioms in T are closed). The exception is the reflexivity rule shown on the left:

$$\begin{array}{c}\Delta\\ \hline \tau = \tau \quad (\mathit{Refl})\\ \cdots\pi_1\cdots\end{array} \quad\Rightarrow\quad \begin{array}{c}\Delta\\ \hline \tau_1 = \tau_1 \quad (\mathit{Refl})\\ \cdots\pi_2\cdots\end{array} \quad\Rightarrow\quad \begin{array}{c}\Delta\\ \hline \tau_1 = \tau_1 \quad (\mathit{Refl})\\ \cdots\pi_2'\cdots\end{array}$$

If the term τ is not closed then we substitute for its free variables some Henkin constant whereby we obtain a closed term τ_1. We perform the same substitutions in the formulas of π_1 whereby we obtain a tableau π_2. Note that the substitutions do not affect the structure of π_1 because T and Δ are closed. The new tableau π' for Δ with the same number of expansions as π is shown above in the middle. We have $\pi' : T \vdash [\Delta]$ and also $\pi_2 : T \vdash [\Delta, \tau_1 = \tau_2]$. We apply IH to the last tableau and obtain an identity tableau π_2' s.t. $\pi_2' : T, Qa \vdash_i [\Delta, \tau_1 = \tau_2]$, We then construct the closed identity tableau π'' for Δ from axioms T, Qa shown on the right.

If the first expansion in π is by quantifier instantiation rule, say $(\exists *)$, then we have a closed $\exists x \phi * \in \Delta$ and π has the following form:

$$\begin{array}{c}\Delta\\ \hline \phi_x[\tau] * \quad (\exists *)\\ \cdots\pi_1\cdots\end{array}$$

If the term τ contains free variables then we substitute for them, similarly as in the preceding case, some Henkin constant and we perform the same substitutions in the tableau π_1 whereby we obtain a closed term τ_1 and a tableau π_2 s.t. $\pi_2 : T \vdash [\Delta, \phi_x[\tau_1]*]$. We then obtain an identity tableau π_2' such that $\pi_2' : T, Qa \vdash_i [\Delta, \phi_x[\tau_1]*]$ by IH and construct the following closed identity tableau for Δ from axioms T, Qa as follws:

$$
\begin{array}{c}
\Delta \\
\hline
\phi_x[\tau_1] \to \exists x\phi \quad (Ax) \\
(\to) \\
\begin{array}{cc}
\exists x\phi & \phi_x[\tau_1]* \\
\circ & \pi_2'
\end{array}
\end{array}
$$

If the first expansion in π is by an eigen-variable rule, say $(\exists)$, then we have a closed $\exists x\phi \in \Delta$ and π has the following form:

$$
\begin{array}{c}
\Delta \\
\hline
\phi_x[y] \quad (\exists) \\
\pi_1[y]
\end{array}
$$

Note that the eigen-variable y cannot freely occur in T or in Δ because both are closed. Let c be the Henkin constant belonging to $\exists x\phi$. We substitute c for y in $\phi_x[y]$ and $\pi_1[y]$ whereby we obtain a tableau $\pi_1[c]$ such that $\pi_1[c] : T \vdash [\Delta, \phi_x[c]]$. Since $\phi_x[c]$ is closed, we obtain an identity tableau π_1' such that $\pi_1' : T, Qa \vdash [\Delta, \phi_x[c]]$ by IH and we construct the closed identity tableau π' for Δ from axioms T, Qa as follows:

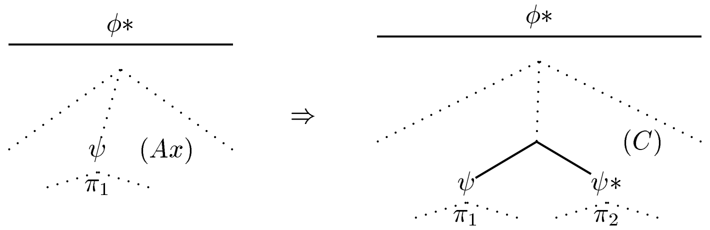
$$
\begin{array}{c}
\Delta \\
\hline
\exists x\phi \to \phi_x[c] \quad (Ax) \\
(\to) \\
\begin{array}{cc}
\phi_x[c] & \exists x\phi* \\
\pi_1' & \circ
\end{array}
\end{array}
$$

The remaining quantifier expansion rules are similar. $\square$

5.3.12 Theorem (Introduction/elimination of quantifier rules). *If T and ϕ consist of sentences of a language $\mathcal{L}$ and $\mathcal{L}_c$ is its witnessing extension then*

$$T \vdash \phi \Leftrightarrow T, Qa \vdash_i \phi \ .$$

Proof. In the direction $(\Rightarrow)$ assume $\pi : T \vdash \phi$, i.e. $\pi : T \vdash [\phi*]$, and apply Lemma 5.3.11 to get $T, Qa \vdash_i [\phi*]$, i.e. $T, Qa \vdash_i \phi$. In the direction $(\Leftarrow)$ assume $\pi : T, Qa \vdash_i \phi$ which is shown in the following on the left



where we have indicated just one out of possibly many (or none) expansions by the axiom rule with $\psi \in Qa$. We construct a new tableau π' shown on the right where we replace every such expansion by a cut on ψ whose right branch is closed by the tableau π_2 obtained by Lemma 5.3.9 to satisfy $\pi_2 : Ha \vdash \psi$. Cuts are admissible by Lemma 5.3.7 and so $\pi' : T, Ha \vdash \phi$ from which we obtain $T \vdash \phi$ by Thm. 5.3.10. $\square$

5.3.13 Theorem (Soundness and completeness of tableaux). *If T of some $\mathcal{L}$ is closed and ϕ is a formula of $\mathcal{L}$ then*

$$T \models \phi \Leftrightarrow T \vdash \phi \; . \tag{1}$$

If also ϕ is a sentence then Fig. 5.3 shows the complete semantic and syntactic reductions.

$$\begin{array}{lcl}
T \models \phi & \overset{\textbf{(a)}}{\Longleftrightarrow} & T \vdash \phi \\
\Updownarrow \text{ (Henkin reduction: 5.2.15)} & & \Updownarrow \text{ (Intro/elim of q-rules: 5.3.12)} \\
T, Qa \models_i \psi & \overset{\textbf{(b)}}{\Longleftrightarrow} & T, Qa \vdash_i \phi \\
\Updownarrow \text{ (Quasitautological reduction: 4.2.11)} & & \Updownarrow \text{ (Intro/elim of i-rules: 4.3.7)} \\
T, Qa, Eq \models_p \phi & \overset{\textbf{(c)}}{\Longleftrightarrow} & T, Qa, Eq \vdash_p \phi \\
\Updownarrow \text{ (Tautological reduction: 3.4.5)} & & \Updownarrow \text{ (Intro/elim of axioms: 3.5.7)} \\
\models_p \psi_1 \wedge \cdots \wedge \psi_n \to \phi & \overset{\textbf{(d)}}{\Longleftrightarrow} & \vdash_p \psi_1 \wedge \cdots \wedge \psi_n \to \phi \\
\text{for some } \psi_1, \ldots, \psi_n \in T \cup Qa \cup Eq & & \text{for some } \psi_1, \ldots, \psi_n \in T \cup Qa \cup Eq
\end{array}$$

(a): Soundness and completeness of tableaux: 5.3.13

(b): Soundness and completeness of identity tableaux: 4.3.8

(c): Soundness and completeness of propositional tableaux: 3.5.8

(d): Soundness and completeness of propositional tableaux without axioms: 3.2.7

Fig. 5.3. Soundness and completeness of tableaux for closed T and ϕ.

Proof. When ϕ is a sentence then we have $T \vDash \phi$ iff, by Thm. 5.2.15, $T, Qa \vDash_i \phi$ iff, by Corollary 4.3.8, $T, Qa \vdash_i \phi$ iff, by Thm. 5.3.12, $T \vdash \phi$. This is shown in Fig. 5.3.

If ϕ is a formula then we have $T \vDash \phi$ iff, by Thm. 5.2.17, $T \vDash \forall\phi$ for a universal closure $\forall\phi$ of ϕ iff, by the just proved special case, $T \vdash \forall\phi$ iff, by Thm. 5.3.8, $T \vdash \phi$. $\square$

5.3.14 Semidecidability of validity. This paragraph is not yet finished. We can find a proof if valid. If not we may search forever for an counterexample. This is the best, but the proof of it requires a knowledge of the theory of computability.

6. First-order Theories

A *first-order theory in* $\mathcal{L}$, or simply theory in $\mathcal{L}$, is a set T of sentences of the first-order language $\mathcal{L}$. *Theorems* of T are formulas ϕ provable from T: $T \vdash \phi$.

6.1 Theorems of Predicate Calculus

For every language $\mathcal{L}$ the theorems of the *empty* theory $\emptyset$ in $\mathcal{L}$ are called theorems of *predicate calculus*.

6.1.1 Tableau vs. informal proofs. This paragraph is not finished. It will deal with proofs proofs of basic theorems of predicate calculus formally and informally. The theorems deal with quantifiers, prenex operations, instantiations (substitution), etc.

We now prove two *rules of Leibnitz* which are a generalization of function *Fsub* and predicate *Psub* substitution rules to arbitrary terms and formulas.

6.1.2 Theorem (Rules of Leibnitz). *For a term $\sigma[x_1, \ldots, x_n]$ and a formula $\phi[x_1, \ldots, x_n]$ with of a language $\mathcal{L}$ and with the free variables among the indicated ones the following are admissible rules of inference:*

$$\frac{\tau_1 = \rho_1 \;\ldots\; \tau_n = \rho_n}{\sigma[\tau_1, \ldots, \tau_n] = \sigma[\rho_1, \ldots, \rho_n]}\,(L_1) \qquad \frac{\tau_1 = \rho_1 \;\ldots\; \tau_n = \rho_n \;\; \phi[\tau_1, \ldots, \tau_n]}{\phi[\rho_1, \ldots, \rho_n]}\,(L_2)$$

Proof. (L_1): An application of the rule is shown on the left:

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \hline \sigma[\tau_1, \ldots, \tau_n] = \sigma[\rho_1, \ldots, \rho_n] \qquad (L_1) \\ \pi \end{array} \quad \Rightarrow \quad \begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \hline \\ \pi' \end{array}$$

where we have indicated by $[\vec{\tau} = \vec{\rho}]$ the premises $\tau_1 = \rho_1, \ldots, \tau_n = \rho_n$. We wish to find a closed tableau π' shown on the right by induction on the structure of the term σ.

If $\sigma \equiv y$ where y is not among the indicated variables then the conclusion of (L_1) is $y = y$ and we start π' with a reflexivity rule:

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \hline y = y \qquad (\mathit{Refl}) \\ \cdots \pi \cdots \end{array}$$

If $\sigma \equiv x_i$ where $1 \leq i \leq n$ then the conclusion of (L_1) is $\tau_i = \rho_i$ and we can omit it altogether because it is already among the premises. Thus $\pi' \equiv \pi$:

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \hline \\ \cdots \pi \cdots \end{array}$$

If $\sigma \equiv f(\sigma_1, \ldots, \sigma_m)$ then we construct π' by applying (L_1) m-times to the terms σ_i because this is admissible by IH and then by using a function substitution rule for f:

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \hline \sigma_1[\vec{\tau}] = \sigma_1[\vec{\rho}] \qquad (L_1) \\ \vdots \\ \sigma_m[\vec{\tau}] = \sigma_m[\vec{\rho}] \qquad (L_1) \\ f(\sigma_1[\vec{\tau}], \ldots, \sigma_m[\vec{\tau}]) = f(\sigma_1[\vec{\rho}], \ldots, \sigma_m[\vec{\rho}]) \qquad (Fsub) \\ \cdots \pi \cdots \end{array}$$

(L_2): An application of the rule is shown on the left:

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \phi[\tau_1, \ldots, \tau_n] \\ \hline \phi[\rho_1, \ldots, \rho_n] \qquad (L_2) \\ \cdots \pi \cdots \end{array} \quad \Rightarrow \quad \begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \phi[\tau_1, \ldots, \tau_n] \\ \hline \\ \cdots \pi' \cdots \end{array}$$

We wish to find a closed tableau π' shown on the right by induction on the number of propositional connectives and quantifiers in the formula ϕ.

If $\phi \equiv \top$ or $\phi \equiv \bot$ then both $\phi[\vec{\tau}]$ and $\phi[\vec{\rho}]$ are identical and we can omit the conclusion altogether by setting $\pi' \equiv \pi$ as in the case $\sigma \equiv x_i$ of (L_1).

If $\phi \equiv P(\sigma_1, \ldots, \sigma_m)$ then we construct π' similarly as in the case $\sigma \equiv R(\sigma_1, \ldots, \sigma_m)$ of (L_1) and use a predicate substitution rule for P.

If $\phi \equiv \sigma_1 = \sigma_2$ then we construct π' by applying (L_1) to terms σ_1 and σ_2 and then by using the rules of identity as shown:

$$
\begin{array}{ll}
\multicolumn{2}{c}{[\vec{\tau} = \vec{\rho}]} \\
\multicolumn{2}{c}{\vdots} \\
\multicolumn{2}{c}{\sigma_1[\vec{\tau}] = \sigma_2[\vec{\tau}]} \\
\hline
\sigma_2[\vec{\tau}] = \sigma_2[\vec{\rho}] & (L_1) \\
\sigma_1[\vec{\tau}] = \sigma_2[\vec{\rho}] & (\mathit{Trans}) \\
\sigma_1[\vec{\tau}] = \sigma_1[\vec{\rho}] & (L_1) \\
\sigma_1[\vec{\rho}] = \sigma_1[\vec{\tau}] & (\mathit{Sym}) \\
\sigma_1[\vec{\rho}] = \sigma_2[\vec{\rho}] & (\mathit{Trans}) \\
\multicolumn{2}{l}{\quad \cdots\pi\cdots}
\end{array}
$$

If $\phi \equiv \neg\phi_1$ then we may assume that π starts with an inversion of $(\neg)$-rule applied to $\neg\phi_1[\vec{\rho}]$ as shown in the following on the left:

$$
\begin{array}{ll}
\multicolumn{2}{c}{[\vec{\tau} = \vec{\rho}]} \\
\multicolumn{2}{c}{\vdots} \\
\multicolumn{2}{c}{\neg\phi_1[\vec{\tau}]} \\
\hline
\neg\phi_1[\vec{\rho}] & (L_2) \\
\phi_1[\vec{\rho}]* & (\neg) \\
\multicolumn{2}{c}{\cdots\pi_1\cdots}
\end{array}
\quad \Rightarrow \quad
\begin{array}{llll}
\multicolumn{4}{c}{[\vec{\tau} = \vec{\rho}]} \\
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\neg\phi_1[\vec{\tau}]} \\
\hline
 & & (C) & \\
\phi_1[\vec{\rho}] & & \phi_1[\vec{\rho}]* & \\
\rho_1 = \tau_1 & (\mathit{Sym}) & \cdots\pi_1\cdots & \\
\vdots & & & \\
\rho_n = \tau_n & (\mathit{Sym}) & & \\
\phi_1[\vec{\tau}] & (L_2) & & \\
\phi_1[\vec{\tau}]* & (\neg) & & \\
\circ & & &
\end{array}
$$

We construct π' as shown on the right by introducing a cut on $\phi_1[\vec{\rho}]$ and on the assumption side by applying IH to $\phi[\vec{\rho}]$ to obtain $\phi[\vec{\tau}]$ after inserting n symmetry rules. The branch is then closed by applying $(\neg)$ to $\neg\phi_1[\vec{\tau}]$ in the premises.

If $\phi \equiv \phi_1 \vee \phi_2$ then we may assume that π starts with an inversion of $(\vee)$-rule applied to $\phi_1[\vec{\rho}] \vee \phi_2[\vec{\rho}]$ as shown in the following on the left:

$$
\begin{array}{ll}
\multicolumn{2}{c}{[\vec{\tau} = \vec{\rho}]} \\
\multicolumn{2}{c}{\vdots} \\
\multicolumn{2}{c}{\phi_1[\vec{\tau}] \vee \phi_2[\vec{\tau}]} \\
\hline
\multicolumn{2}{c}{\phi_1[\vec{\rho}] \vee \phi_2[\vec{\rho}] \quad (L_2)} \\
\multicolumn{2}{r}{(\vee)} \\
\phi_1[\vec{\rho}] & \phi_2[\vec{\rho}] \\
\cdots\pi_1\cdots & \cdots\pi_2\cdots
\end{array}
\quad \Rightarrow \quad
\begin{array}{llll}
\multicolumn{4}{c}{[\vec{\tau} = \vec{\rho}]} \\
\multicolumn{4}{c}{\vdots} \\
\multicolumn{4}{c}{\phi_1[\vec{\tau}] \vee \phi_2[\vec{\tau}]} \\
\hline
\multicolumn{4}{c}{(\vee)} \\
\phi_1[\vec{\tau}] & & \phi_2[\vec{\tau}] & \\
\phi_1[\vec{\rho}] & (L_2) & \phi_2[\vec{\rho}] & (L_2) \\
\cdots\pi_1\cdots & & \cdots\pi_2\cdots &
\end{array}
$$

We construct π' as shown on the right by applying $(\vee)$-rule to the assumption $\phi_1[\vec{\tau}] \vee \phi_2[\vec{\tau}]$ and then by applying (L_2) on both sides by IH.

If $\phi \equiv \exists y \phi_1[y, \vec{x}]$ then we may assume that π starts with an inversion of $(\exists)$-rule with an eigen-variable z applied to $\exists y \phi_1[y, \vec{\rho}]$ as shown in the following on the left:

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \exists y \phi_1[y, \vec{\tau}] \\ \hline \exists y \phi_1[y, \vec{\rho}] \quad (L_2) \\ \phi_1[z, \vec{\rho}] \quad (\exists) \\ \cdots \pi_1 \cdots \end{array} \quad \Rightarrow \quad \begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \exists y \phi_1[y, \vec{\tau}] \\ \hline \phi_1[z, \vec{\tau}] \quad (\exists) \\ \phi_1[z, \vec{\rho}] \quad (L_2) \\ \cdots \pi_1 \cdots \end{array}$$

We construct π' as shown on the right by applying the $(\exists)$-rule with an eigen-variable z to the premise $\exists y \phi_1[y, \vec{\tau}]$ and then by using (L_2) by IH.

If $\phi \equiv \forall y \phi_1[y, \vec{x}]$ then in the tableau π shown in the following on the left we show just one of possibly many expansions of a $(\forall)$-rule applied to the assumption $\forall y \phi_1[y, \vec{\rho}]$. We also show a possible closure of a branch in π by this assumption.

$$\begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \forall y \phi_1[y, \vec{\tau}] \\ \hline \forall y \phi_1[y, \vec{\rho}] \qquad (L_2) \\ \begin{array}{ccc} \phi_1[\sigma, \vec{\rho}] \ (\forall) & & \forall y \phi_1[y, \vec{\rho}]* \\ \cdots \pi_1 \cdots & & \circ \end{array} \end{array} \quad \Rightarrow \quad \begin{array}{c} [\vec{\tau} = \vec{\rho}] \\ \vdots \\ \forall y \phi_1[y, \vec{\tau}] \\ \hline \begin{array}{ccc} \phi_1[\sigma, \vec{\tau}] \ (\forall) & & \forall y \phi_1[y, \vec{\rho}]* \\ \phi_1[\sigma, \vec{\rho}] \ (L_2) & & \phi_1[z, \vec{\rho}]* \ (\forall *) \\ & & \phi_1[z, \vec{\tau}] \ (\forall) \\ \pi_1 & & \phi_1[z, \vec{\rho}] \ (L_2) \\ & & \circ \end{array} \end{array}$$

We construct π' as shown on the right by reconstructing all branches similar to the shown ones as follows. In the branch on the left we instantiate the premise $\forall y \phi_1[y, \vec{\tau}]$ with $y := \sigma$ and then apply (L_2) by IH. In the branch on the right we apply the eigen-variable to $\forall y \phi_1[y, \vec{\rho}]*$ with a new eigen-variable z. We then instantiate the premise $\forall y \phi_1[y, \vec{\tau}]$ with $y := z$ and then close the branch by applying (L_2) by IH.

The remaining propositional cases for ϕ are dealt with similarly. $\square$

6.1.3 Theorems of Leibnitz. For any terms $\sigma[x_1, \ldots, x_n]$ and formulas $\phi[x_1, \ldots, x_n]$ we obtain as an immediate consequence of rules of Leibnitz:

$$\vdash \tau_1 = \rho_1 \wedge \ldots \wedge \tau_n = \rho_n \to \sigma[\tau_1, \ldots, \tau_n] = \sigma[\rho_1, \ldots, \rho_n] \tag{1}$$

$$\vdash \tau_1 = \rho_1 \wedge \ldots \wedge \tau_n = \rho_n \wedge \phi[\tau_1, \ldots, \tau_n] \to \phi[\rho_1, \ldots, \rho_n] \ . \tag{2}$$

6.1.4 Identity theorem. If the variable x is possibly free in a formula $\phi[x]$ and does not occur in a term τ then

$$\vdash \exists x(x = \tau \land \phi[x]) \leftrightarrow \phi[\tau] \tag{1}$$
$$\vdash \forall x(x = \tau \to \phi[x]) \leftrightarrow \phi[\tau] \ . \tag{2}$$

(1): In the direction ($\to$) assume $x = \tau$ and $\phi[x]$ for some x. We obtain $\phi[\tau]$ by the theorem of Leibnitz 6.1.3(2). In the direction ($\leftarrow$) assume $\phi[\tau]$. Since $\tau = \tau$, we get $\exists x(x = \tau \land \phi[x])$ by setting $x := \tau$.

(2): This is similar.

6.1.5 Equivalence theorem. This paragraph is not yet finished. If a formula ϕ contains an occurrence of a formula $\psi[\vec{x}]$:

$$\psi \equiv \ldots \psi[\vec{x}] \ldots$$

where we have indicated that all bound variables of ϕ in whose scope lies the occurrence of ψ are among $\vec{x}$. If the formula ϕ_1 is obtained from ϕ by replacing this occurrence of ψ by a formula ψ_1. then

$$\vdash \forall \vec{x}(\psi \leftrightarrow \psi_1) \land \phi \to \phi_1 \ . \tag{1}$$

Note that we have as an immediate consequence by the Generalization rule 5.3.8:

$$\vdash \psi \leftrightarrow \psi_1 \Rightarrow \ \vdash \phi \leftrightarrow \phi_1 \tag{2}$$

6.1.6 Variant theorem. We say that a formula ϕ_1 is a *variant* of ϕ if ϕ_1 differs from ϕ only in the names of its bound variables. More precisely, if ϕ_1 is obtained from ϕ by a sequence of replacements of its subformulas $\exists x\psi[x]$ or $\forall x\psi[x]$ by the corresponding subformulas $\exists y\psi[y]$ or $\forall x\psi[y]$ for a variable y not free in ψ.

If ϕ_1 is a variant of ϕ we have

$$\vdash \phi \leftrightarrow \phi_1 \ . \tag{1}$$

Thus follows from the following properties by 6.1.5(2):

$$\vdash \exists x\psi[x] \leftrightarrow \exists y\psi[y] \tag{2}$$
$$\vdash \forall x\psi[x] \leftrightarrow \forall y\psi[y] \ . \tag{3}$$

(2): In the direction ($\to$) assume $\psi[x]$ for some x and obtain $\exists y\phi[x]$ by setting $y := x$. The direction ($\leftarrow$) is similar.

(3): In the direction ($\to$) assume $\forall x\psi[x]$ and take any y. We get $\phi[y]$ by instantiating the assumption with $x := y$. The direction ($\leftarrow$) is similar.

6.2 Extensions of Theories

6.2.1 Theories. A *theory* T *in* $\mathcal{L}$ is a set of sentences of some first-order language $\mathcal{L}$. We call $\mathcal{L}$ *the language of* T and designate it by $\mathcal{L}_T$.

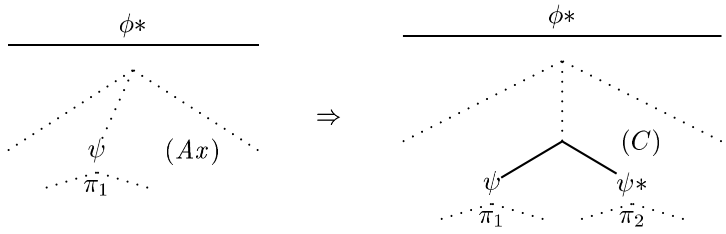
Sentences of T are called *axioms* of the theory T. A theory is *open* if its axioms are universal closures of quantifier-free formulas, i.e. if every axiom has a form $\forall\vec{x}\phi$ with ϕ a formula without quantifiers.

A formula ϕ of $\mathcal{L}_T$ is a *theorem* of T if $T \vdash \phi$. Axioms $\phi \in T$ are trivially theorems of T.

6.2.2 Lemma. *If T, T_1, S are theories in $\mathcal{L}$ and ϕ a formula of $\mathcal{L}$ then*

$$S \vdash T \text{ and } T, T_1 \vdash \phi \Rightarrow S, T_1 \vdash \phi \ .$$

Proof. Assume $S \vdash T$ and $\pi : T, T_1 \vdash \phi$ where π is shown in the following on the left:



with one of possibly many expansions by an axiom $\psi \in T$. We construct the tableau π' shown on the right by replacing every such expansion by a cut on ψ whose right branch is closed by a tableau π_2 such that $\pi_2 : S \vdash \psi$. We assume that the eigen-variables of π_2 were systematically renamed so they do not occur freely in the branch above $\psi*$. We clearly have $\pi' : S, T_1 \vdash \phi$. $\square$

6.2.3 Consistency of theories. A theory T is *consistent* if $T \nvdash \bot$. Because $\bot \to \phi$ is a tautology, every formula ϕ is a theorem of an inconsistent theory. An inconsistent theory is thus worthless and so the consistency is the minimal requirement on theories. Because the consistence is defined by provability it is a syntactic concept. The consistency of open theories is syntactically characterized by the theorem of Hilbert-Ackermann Thm. 6.2.4 and the consistency of all theories is semantically characterized in Thm. 6.2.5.

If the reader finds the proof of the first characterization theorem trivial he should bear in mind that our tableau system has a subformula property where the proofs proceed without any detours such as the formulas introduced by the cut rules. Hilbert and Ackermann [13] (see also Shoenfield [20]) used a formal system based on modus ponens which is a form of cut. The theorem becomes non-trivial in cut-based proof systems. The difficulty of its proof is comparable to that of the proof of our non-trivial theorem on the admissibility of cuts.

6.2.4 Theorem (Hilbert-Ackermann). *An open theory is inconsistent iff* $\vdash_i \bigwedge S \to \bot$ *for a finite set* S *of instances of its axioms.*

Proof. Let T be an open theory. If T is inconsistent then we have $\pi : T \vdash \bot$ for some basic tableau π. The only quantifier rules in π are $(\forall)$-rules instantiating the axioms of T. We remove from π all formulas of a form $\forall\phi$, which can be only axioms from T and its instantiations, whereby we obtain a tableau π_1 s.t. $\pi_1 : S \vdash_i \bot$ where S is a finite sets of all quantifier-free instances of axioms in T. We then get $\vdash_i \bigwedge S \to \bot$ by the Deduction theorem 5.3.4.

Vice versa, if $\vdash_i \bigwedge S \to \bot$ then $\pi : S \vdash_i \bot$ by Thm. 5.3.4 and we can insert into π in front of every application of an axiom $\phi \in S$ the appropriate axiom $\forall\phi \in T$ followed by instantiations by $(\forall)$-rules leading to S whereby we obtain $T \vdash \bot$. □

6.2.5 Theorem. *A theory is consistent iff it has a model.*

Proof. We have $T \vdash \bot$ iff $T \models \bot$, i.e. a theory T is consistent iff $T \not\models \bot$ by the Completeness theorem 5.3.13. If T has no model, i.e. if $\mathcal{M} \not\models T$ for all structures $\mathcal{M}$ for $\mathcal{L}_T$, then $T \models \bot$ and so T is inconsistent. Vice versa, if T is inconsistent, i.e. if $T \models \bot$, then take any structure $\mathcal{M}$ for $\mathcal{L}_T$. We have $\mathcal{M} \not\models \bot$ and so $\mathcal{M} \not\models T$. Hence T has no model. □

6.2.6 Extensions of theories. A theory S is an *extension* of a theory T if $\mathcal{L}_S$ is an extension of $\mathcal{L}_T$ and every theorem of T is a theorem of S, i.e.

$$T \vdash \phi \Rightarrow S \vdash \phi \quad \text{for all formulas } \phi \text{ of } \mathcal{L}_T \ .$$

Note that T is an extension of itself. Also S is an extension of T iff $\mathcal{L}_S$ extends $\mathcal{L}_T$ and $S \vdash T$ by Lemma 6.2.2 but this does not imply that the axioms of T are among those of S, i.e. $S \subseteq T$.

Let S be an extension of T and K a set of formulas of $\mathcal{L}_T$. We say that T and S are *equivalent on* K if $S \vdash K \Rightarrow T \vdash K$. We designate this by writing $T \equiv_K S$. If K consists of all formulas of $\mathcal{L}_T$ we write $T \equiv_{\mathcal{L}_T} S$.

Note that if T and S are equivalent on K as above then, since $T \vdash K \Rightarrow S \vdash K$ because S extends T, a formula of K is a theorem of S iff it is a theorem of T.

The theories T and S are *equivalent* if S extends T and T extends S. Note that we then have $\mathcal{L}_T = \mathcal{L}_S$ and $T \equiv_{\mathcal{L}_T} S$ which we write simply as $T \equiv S$.

The following theorem characterizes the situation when we can consistently extend a theory T by adding a single axiom without extending the language. We can, namely, add the axiom iff its negation is unprovable in T.

6.2.7 Theorem. *Let* T *be a theory and* ϕ *a sentence of* $\mathcal{L}_T$*. The extended theory* T, ϕ *is consistent iff* $T \nvdash \neg\phi$.

Proof. If $T \vdash \neg\phi$ then, since $T, \phi \vdash \phi$, we have $T \vdash \bot$. Vice versa, if $T, \phi \vdash \bot$ then $T \vdash \phi \to \bot$ by the Deduction theorem and so $T \vdash \neg\phi$. □

6.2.8 Conservative extensions. Not all extensions are interesting. Uninteresting extensions are extensions turning consistent theories into inconsistent ones.

For instance, take a formalized theory of natural numbers which we will study in a form of so called Peano arithmetic, shortly PA, in the second part of this text. The square root of 2 is not a natural number (not even a rational one as was already known to Greeks). An attempt to extend PA with a new constant symbol $\sqrt{2}$ and a new axiom $2 = \sqrt{2}\cdot\sqrt{2}$ yields an extension PA_1 of PA because we trivially have $\mathrm{PA}_1 \vdash \mathrm{PA}$. Unfortunately PA_1 is inconsistent whereas PA is consistent. This is because we trivially have $\mathrm{PA}_1 \vdash 2 = \sqrt{2}\cdot\sqrt{2}$ but $\mathrm{PA} \vdash \forall x\, 2 \neq x\cdot x$, hence $\mathrm{PA}_1 \vdash \forall x\, 2 \neq x\cdot x$, and so $\mathrm{PA}_1 \vdash 2 \neq \sqrt{2}\cdot\sqrt{2}$. Because $\phi \land \neg\phi \to \perp$ is a tautology we then get $\mathrm{PA}_1 \vdash \perp$.

This leads us to extensions S of T which are equivalent with T on $\mathcal{L}_T$, i.e. such that $T \equiv_{\mathcal{L}_T} S$. Such extensions are called *conservative* extensions because they do not add any new theorems in the language of T. Specifically if T is consistent then $\perp$, which is in $\mathcal{L}_T$, is not a theorem of T and we cannot have $S \vdash \perp$. Hence also S is consistent.

In order to prove that the extension S of T is conservative, which is more simply put as *S is conservative over T*, it suffices to prove that whenever $S \vdash \phi$ where ϕ is a formula of $\mathcal{L}_T$ then also $T \vdash \phi$. Note that the converse holds because S extends T and so every theorem of T is a theorem of S. By the Generalization rule 5.3.8 it suffices to prove the above for the sentences ϕ of $\mathcal{L}$.

Note that the extension of T to T, ϕ when $T \nvdash \neg\phi$ is not in general conservative because the extended theory proves ϕ which can be *undecidable* in T, i.e. neither ϕ nor $\neg\phi$ are provable in T.

6.3 Extensions by Explicitly Defined Predicates

Mathematicians often introduce new predicates as abbreviations for larger formulas. They do it in order to increase the readability of their theorems and to shorten their proofs. A typical example is the introduction of the predicate $x < y$ into a theory T which contains the binary function of addition and the constant 1. Formulas of a form $\tau_1 < \tau_2$ can be viewed as abbreviations for formulas

$$\exists z(\tau_1 + (z+1) = \tau_2)$$

where the variable z is new. One can then proceed to prove properties of $<$, say the transitivity:

$$T \vdash x < y \land y < z \to x < z \ ,$$

always keeping on mind that this is just an abbreviation for a larger and less readable theorem

$$T \vdash \exists a(x + 1 + (a + 1) = y) \wedge \exists b(y + (b + 1) = z) \rightarrow \exists c(x + (c + 1) = z) \ .$$

The problem with this approach is that when one wants to prove a metatheoretical, theorem on provability in T, which often happens in logic but rarely in mathematics, one has to eliminate all abbreviations. A cleaner approach from a logical point of view is the extension of $\mathcal{L}_T$ with a new binary predicate symbol $<$ and the addition to T of a new axiom for $<$ which is any universal closure of:

$$x < y \leftrightarrow \exists z(x + (z + 1) = y) \ .$$

We then wish to know that the extended theory S is conservative over T, i.e. that it does not add any power to T beyond notational convenience. One can actually prove more than this by defining a translation $\phi^\star$ into $\mathcal{L}_T$ of every formula ϕ of $\mathcal{L}_S$ such that we have

$$S \vdash \phi \Leftrightarrow T \vdash \phi^\star \ .$$

6.3.1 Extensions by explicitly defined predicates. Let T be a theory, $\phi[\vec{x}]$ a formula of $\mathcal{L}_T$ with the free variables among the indicated ones, and P a new n-ary predicate symbol ($n \geq 0$). Consider the formula

$$P(\vec{x}) \leftrightarrow \phi[\vec{x}] \tag{1}$$

which is in the extension $\mathcal{L}_T + P$ of $\mathcal{L}_T$. Designate by S the theory $T, \forall(1)$ whose language is the extension of $\mathcal{L}_T$ with the symbol P and whose axioms are T plus any universal closure of (1) which is called the *defining axiom* for P.

We trivially have $S \vdash T$ and so S is an extension of T which we call *extension by explicitly defined predicate.* The term 'explicit' refers to the fact that the defining axiom is not 'recursive', i.e. that P is not applied in ϕ. This is obviously so because ϕ is in a language which does not contain the predicate symbol P. We then have

$$S \vdash P(\vec{x}) \leftrightarrow \phi[\vec{x}] \tag{2}$$

by Thm. 5.3.8 because S trivially proves its axiom $\forall(1)$.

6.3.2 Translation function. Let S be the extended theory $T, \forall 6.3.1(1)$. For every formula ψ of $\mathcal{L}_S$ we designate by $\psi^\star$ any formula of $\mathcal{L}_T$ obtained from ψ by replacing in it every application $P(\vec{\tau})$ by a formula $\phi'[\vec{\tau}]$ where ϕ' is a variant of ϕ such that the substitution of $\vec{\tau}$ in ϕ' is free for $\vec{x}$. We call any such formula $\psi^\star$ a *translation* of ψ.

6.3.3 Translation lemma. *If S is the extended theory $T, \forall 6.3.1(1)$ and ψ a formula of $\mathcal{L}_S$ then we have*

$$S \vdash \psi \leftrightarrow \psi^* \ . \tag{1}$$

Proof. It is clearly sufficient to show

$$S \vdash P(\vec{\tau}) \leftrightarrow \phi'[\vec{\tau}] \tag{2}$$

where $\vec{\tau}$ are terms of $\mathcal{L}_T$ (and thus of $\mathcal{L}_S$) and ϕ' a variant of ϕ because we can then repeatedly apply the Equivalence theorem (6.1.5) to the theorem of S: $\psi \leftrightarrow \psi$ until we eliminate all applications of P on the right.

We prove (2) by working in S where we have $P(\vec{x}) \leftrightarrow \phi'[\vec{x}]$ from the defining axiom of P by the Variant theorem (6.1.6). From this we get the property by instantiating $\vec{x} := \vec{\tau}$. □

6.3.4 Theorem. *The extension $S = T, \forall(P(\vec{x}) \leftrightarrow \phi[\vec{x}])$ of T by the explicitly defined predicate P is conservative and for any formula ψ of $\mathcal{L}_T$ we have*

$$S \vdash \psi \Leftrightarrow T \vdash \psi^\star \ . \tag{1}$$

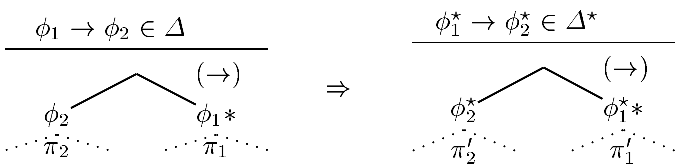
Proof. Assume $S \vdash \psi$ for a formula ψ of $\mathcal{L}_T$. Then $T \vdash \psi^\star$ by 6.3.3(2) and, since $\psi^\star \equiv \psi$, we have $T \vdash \psi$. This proves the conservation. Property (1) is proved in the direction ($\leftarrow$) by assuming $T \vdash \psi^\star$. We have $S \vdash \psi^\star$, since S extends T, and so $S \vdash \psi$ by Lemma 6.3.3.

In the direction ($\rightarrow$) Property (1) follows from an auxiliary property

$$\pi : S \vdash [\Delta] \Rightarrow T \vdash [\Delta^\star]$$

where Δ is a sequence of formulas of $\mathcal{L}_S$ and $\Delta^\star$ is the sequence of formulas of $\mathcal{L}_T$ obtained by translating the corresponding formulas of Δ. The auxiliary property is proved by induction on the structure of π. If π is empty then Δ is closed. This happens if $\top * \in \Delta$ but then $\top * \equiv \top^\star * \in \Delta^\star$, or $\bot \in \Delta$ but then $\bot \equiv \bot^\star \in \Delta^\star$, or $\phi, \phi * \in \Delta$ but then $\phi^\star, \phi^\star * \in \Delta^\star$. In any case $\Delta^\star$ is closed and we even have $\vdash [\Delta^\star]$.

If the first expansion in π is by a propositional rule, say ($\rightarrow$), then π has the form shown in the following on the left:



Since $(\phi_1 \rightarrow \phi_2)^\star \equiv \phi_1^\star \rightarrow \phi_2^\star$, we obtain identity tableaux π_1' and π_2' such that $\pi_1' : T \vdash [\Delta^\star, \phi_1^\star *]$ and $\pi_2' : T \vdash [\Delta^\star, \phi_2^\star]$ by two IH's from $\pi_1 : S \vdash [\Delta, \phi_1 *]$ and $\pi_2' : S \vdash [\Delta, \phi_2]$. We then construct the closed tableau for $\Delta^\star$ from axioms T shown on the right. The remaining propositional, quantifier, identity expansions except by predicate substitution rule applied to P are similar. This is because the translation is recursively applied, for instance, $(\psi_x[\tau] \rightarrow \exists x\psi)^\star \equiv {\psi^\star}_x[\tau] \rightarrow \exists x\psi^\star$.

If the first expansion in π is by a predicate substitution rule applied to P then π looks as follows:

$$\begin{array}{c}
\Delta \qquad \tau_1 = \rho_1, \dots, \tau_n = \rho_n, P(\tau_1, \dots, \tau_n) \in \Delta \\
\hline
P(\rho_1, \dots, \rho_n) \qquad (Psub) \\
\pi_1
\end{array}$$

We have $(\tau_i = \rho_i)^\star \equiv \tau_i = \rho_i, P(\tau_1, \dots, \tau_n)^\star \equiv \phi'[\tau_1, \dots, \tau_n]$, and $P(\rho_1, \dots, \rho_n)^\star \equiv \phi'[\rho_1, \dots, \rho_n]$ for a variant $\phi'[\vec{x}]$ of $\phi[\vec{x}]$ where we may assume that the bound variables of ϕ' are such that both substitutions are free for $\vec{x}$. For $\pi_1 : S \vdash [\Delta, P(\rho_1, \dots, \rho_n)]$ we obtain $\pi_1' : T \vdash [\Delta^\star, \phi'[\rho_1, \dots, \rho_n]]$ by IH. We have

$$\pi_2 : \vdash [\tau_1 = \rho_1, \dots, \tau_n = \rho_n, \phi'[\tau_1, \dots, \tau_n], \phi'[\rho_1, \dots, \rho_n]*]$$

for some π_2 by a rule of Leibnitz. We then construct the following closed tableau for $\Delta^\star$ from axioms T:

$$\begin{array}{c}
\Delta^\star \qquad \tau_1 = \rho_1, \dots, \tau_n = \rho_n, \phi'[\tau_1, \dots, \tau_n] \in \Delta^\star \\
\hline
(C) \\
\begin{array}{cc}
\phi'[\rho_1, \dots, \rho_n] & \phi'[\rho_1, \dots, \rho_n]* \\
\pi_1' & \pi_2
\end{array}
\end{array}$$

If the first expansion in π is by an axiom rule for $\psi \in T$ then, since $\psi^\star \equiv \psi$, we construct $\pi' : T \vdash [\Delta^\star]$ similarly as for the propositional cases above. If the axiom is the defining axiom for P then π looks as follows:

$$\begin{array}{c}
\Delta \\
\hline
\forall\vec{x}(P(\vec{x}) \leftrightarrow \phi[\vec{x}]) \qquad (Ax) \\
\pi_1
\end{array}$$

We have

$$(\forall\vec{x}(P(\vec{x}) \leftrightarrow \phi[\vec{x}]))^\star \equiv \forall\vec{x}(\phi[\vec{x}] \leftrightarrow \phi[\vec{x}])$$

and for $\pi_1 : S \vdash [\Delta, \forall\vec{x}(P(\vec{x}) \leftrightarrow \phi[\vec{x}])]$ we obtain $\pi_1' : T \vdash [\Delta^\star, \forall\vec{x}(\phi[\vec{x}] \leftrightarrow \phi[\vec{x}])]$ by IH. We clearly have $\pi_2 : \vdash \forall\vec{x}(\phi[\vec{x}] \leftrightarrow \phi[\vec{x}])$ for some π_2. We then construct the following closed tableau for $\Delta^\star$ from axioms T:

$$\begin{array}{c}
\Delta^\star \\
\hline
(C) \\
\begin{array}{cc}
\forall\vec{x}(\phi[\vec{x}] \leftrightarrow \phi[\vec{x}]) & \forall\vec{x}(\phi[\vec{x}] \leftrightarrow \phi[\vec{x}])* \\
\pi_1' & \pi_2
\end{array}
\end{array} \qquad \square$$

6.4 Skolem Extensions

6.4.1 Skolem axioms. Suppose that T is a theory whose language does not contain the n-ary function symbol f $(n \geq 0)$. Further suppose that $\phi[\vec{x}, y]$ is a formula of $\mathcal{L}_T$ with the free variables among the $n+1$ indicated ones. The sentence

$$\forall \vec{x}(\exists y \phi[\vec{x}, y] \rightarrow \phi[\vec{x}, f(\vec{x})]) \tag{1}$$

is called the *Skolem axiom for ϕ and f*. The reader will note that in view of prenex theorems of predicate calculus we could have equivalently written the sentence (1) also as a universal closure of

$$\phi[\vec{x}, y] \rightarrow \phi[\vec{x}, f(\vec{x})] \; . \tag{2}$$

Extension of T to S by the addition of the function symbol f to its language and of the Skolem axiom (1) to its axioms is a *Skolem extension* of T. We will prove in this section that S is conservative over T both by semantic and finitary proofs. For that we use until the end of this section the abbreviation

$$\phi_1[\vec{x}, y] \equiv \exists y \phi[\vec{x}, y] \rightarrow \phi[\vec{x}, y])$$

and call the formulas

$$\forall x_i \ldots \forall x_n \phi_1[\tau_1, \ldots, \tau_{i-1}, x_i, \ldots, x_n, \tau_1, \ldots, f(\tau_{i-1}, x_i, \ldots, x_n)] \tag{3}$$

where $1 \leq i \leq n$ *partial* instances of the Skolem axiom and formulas $\phi_1[\vec{\tau}, f(\vec{\tau})]$ *full* instances.

Terms of the form $f(\vec{\tau})$ are called *f-terms* and function substitution expansion rules for f are called *f-substitution rules*. If the conclusion of an f-substitution rule is $f(\vec{\tau}) = f(\vec{\tau})$ then the rule is called *trivial*. Trivial f-substitution rules are not needed because their conclusions $f(\vec{\tau}) = f(\vec{\tau})$ can be obtained also by reflexivity rules.

We will need below the following notation. We designate by $\mathcal{L}_t$ the witnessing extension of $\mathcal{L}_T$, by $\mathcal{L}_s$ the witnessing extension of $\mathcal{L}_S$. A formula of $\mathcal{L}_S$ is *free for f* if it does not contain any f-terms whose arguments contain a bound occurrence of a variable. We denote by H_s all Henkin witnessing and counterexample axioms for $\mathcal{L}_S$ which are free for f, and by H_t all Henkin witnessing and counterexample axioms for $\mathcal{L}_T$. We designate by Sk_s the set of of full instances of the Skolem axiom: $\phi_1[\vec{\tau}, f(\vec{\tau})]$ where $\vec{\tau}$ are closed terms of $\mathcal{L}_s$.

6.4.2 Semantic proof of conservativity of Skolem extensions. Skolem axioms 6.4.1(1) are a generalization of Henkin witnessing axioms where the term $f(\vec{\tau})$ acts as a witness for the formula $\exists y \phi[\vec{\tau}, y]$. If f is a constant, i.e. if $n = 0$, then the Skolem axiom is

$$\exists y\phi[y] \to \phi[f] \tag{1}$$

and it looks like the Henkin witnessing axiom for $\exists y\phi[y]$ except that the constant symbol f is not fixed as it is for Henkin constants. The reader will note that the theorem on the elimination of Henkin witnessing axioms (5.3.10) asserts that the extension of any theory T in $\mathcal{L}$ to the theory T, Ha in $\mathcal{L}_c$ is conservative.

We will now prove that Skolem extensions are conservative. When the new function symbol f is a constant then this follows Thm. 5.3.10. Indeed, if $\pi : T, (1) \vdash \psi$ for a sentence ψ of $\mathcal{L}_T$ then $\pi' : T, Ha \vdash \psi$ where π' is formed by systematically replacing in π the constant symbol f by the Henkin constant c belonging to $\exists y\phi[y]$. We then obtain $T \vdash \psi$ by Thm. 5.3.10.

The above proof is called *finitary* in mathematical logic. For our purposes it suffices to say that finitary proofs are such when one manipulates by constructive means tableaux which are syntactic objects. Finitary proofs are considered more convincing than the semantic arguments by means of models. As it happens, the extension Thm. 6.4.5 of the above finitary proof to the case when $n > 0$, which is the main result of this section, is extremely non-trivial. On the other hand, the semantic proof is almost trivial.

The semantic proof that the theory S from Par. 6.4.1 is conservative over T is by assuming $S \vdash_1 \psi$ for a sentence ψ of $\mathcal{L}_T$. We have $S \models \psi$ by Thm. 5.3.13 and it suffices to prove $T \models \psi$. So let $\mathcal{M}$ for $\mathcal{L}_T$ be a model of T with a domain D such that $d_0 \in D$. We expand $\mathcal{M}$ to a structure $\mathcal{N}$ for $\mathcal{L}_S$ by defining

$$f^{\mathcal{N}}(d_1, \ldots, d_n) = \begin{cases} d & \text{if for some } d \in D \text{ we have } \mathcal{M} \models \phi[d_1, \ldots, d_n, d] \\ d_0 & \text{otherwise.} \end{cases}$$

We have $\mathcal{M} \models \psi_1$ iff $\mathcal{N} \models \psi_1$ for all sentences ψ_1 of $\mathcal{L}_T$ by Thm. 5.2.7. Hence $\mathcal{N} \models T$ and we can easily prove $\mathcal{N} \models \forall 6.4.1(1)$. Thus $\mathcal{N} \models \psi$ from the assumption and then $\mathcal{M} \models \phi$, since ψ is a sentence of $\mathcal{L}_T$.

6.4.3 Invariance of tableau rules under replacement of f-terms. Let the theories T and S be as in Par. 6.4.1. For the finitary proof of conservativity of S over T we need to investigate the effect of systematic replacements of f-terms by another terms in tableaux $\pi : T, Sk_s, H_s \vdash \psi$ where ψ is a sentence of $\mathcal{L}_T$. We assume that the tableau π, which is in the language $\mathcal{L}_s$, consists of sentences only. This means that there are no eigen-variable rules in π. We will see from the proof of Lemma 6.4.4 that π might contain, in addition to the basic expansion rules, also cut rules applied to identities $\tau_1 = \tau_2$ and applications of Leibnitz rules in the following form:

$$\frac{\tau_1 = \rho_1 \ \ldots \ \tau_n = \rho_n \ \ \phi_1[\vec{\tau}, \vec{\sigma}]}{\phi_1[\vec{\tau}, \vec{\sigma}]} \, (L_2) \ .$$

The f-terms can be introduced into π by axioms H_s and Sk_s, by quantifier instantiation, cut, reflexivity, and by f-substitution rules.

Quantifier instantiation rules are invariant under the replacement of f-terms by other terms unless arguments of f-terms contain bound variables, i.e. they are not free fro f. For instance, take the partial instance

$$\forall x_n \phi_1[\tau_1, \dots, \tau_{n-1}, x_n, f(\tau_1, \dots, \tau_{n-1}, x_n)]$$

of the Skolem axiom 6.4.1(1). If it used as a premise to a ($\forall$)-instantiation rule with the conclusion $\phi_1[\tau_1, \dots, \tau_{n-1}, x_n, f(\tau_1, \dots, \tau_{n-1}, \tau_n)]$ then the replacement of the closed term $f(\tau_1, \dots, \tau_{n-1}, \tau_n)$ by a different term invalidates the rule. Note that an replacement of an f-term occurring, say, in τ_{n-1} does not destroy the character of the rule because the same change is done in both the premise and in the conclusion. The reader will note that the tableau π can apply only invariant quantifier instantiation rules.

An f-substitution rule with the conclusion $f(\vec{\tau}) = f(\vec{\rho})$ is not invariant under the replacement of the f-terms $f(\vec{\tau})$ and $f(\vec{\rho})$. It is, however, invariant under the replacement of an f-term anywhere in the arguments $\vec{\tau}$ and $\vec{\rho}$.

An axiom $\phi_1[\vec{\tau}, f(\vec{\tau})]$ from Sk_s is not invariant under the replacement of $f(\vec{\tau})$ but it is invariant under the replacement of any other f-terms applied in $\vec{\tau}$.

An axiom $\exists x \psi_1[x] \to \psi_1[c_1]$ or $\psi_2[c_2] \to \forall x \psi_2[x]$ from H_s is not invariant under the replacement of an f term even though it is free for f. If, however, the replacement is *deep* in the sense that it also systematically modifies the Henking constants c_1 and c_2 the invariance can be restored. In order to explain this we recall that the Henkin constant c_j of rank $i+1$ from $\mathcal{L}_s$ belongs to the sentence $\exists x \psi_3[x]$ which is at the j-th in the enumeration of existential sentences 5.1.6(1) of $\mathcal{L}_s$ of rank i. We can thus visualize the Henkin constant c_j written with *symbolic index*: $c_{\exists x \psi_3[x]}$. The deep replacement of an f-term in a Henkin witnessing $\exists x \psi_1[x] \to \psi_1[c_{\exists x \psi_1[x]}]$ or counterexample $\psi_2[c_{\exists x \neg \psi_2[x]}] \to \forall x \psi_2[x]$ axiom means that we replace the f-term also in the symbolic indices of Henkin constants. Note that the symbolic indices $\exists x \psi_1[x]$ and $\exists x \neg \psi_2[x]$ may again contain Henkin constants (of lower rank) and we must perform the deep replacement also in them. After the deep replacement we look up the symbolic indices in the corresponding enumerations 5.1.6(1) and replace them by ordinary indices. It should be clear that the deep replacement changes an axiom from H_s into an axiom from H_s and so its use in the tableau π can be visualized to be invariant under the deep replacement of f-terms.

All other expansion rules, including the cut and Leibnitz rules in the above form, are invariant under systematic replacements of f-terms by different terms. Since a Henkin constant can be replaced by another Henkin constant without invalidating any rules except possibly those in H_s, the deep replacement of f-terms in π may invalidate at most the f-substitution rules and the axioms from Sk_s.

6.4.4 Lemma (Elimination of f-substitution rules). *If for a sentence ψ of $\mathcal{L}_T$ as described in Par. 6.4.1 we have $\pi : T, Sk_s, H_s \vdash \psi$ where π*

consists of sentences only and its expansion rules, except the axioms Sk_s and f-substitution rules, are invariant under the deep replacement of f-terms then there is a similar tableau π_0 such that $\pi_0 : T, Sk_s, H_s \vdash \psi$ but π_0 does not apply non-trivial f-substitution rules.

Proof. Take any π satisfying the assumption os the lemma. We determine the *weight* of tableaux with f-terms those occurring in π as follows. We order all distinct f-terms occurring in the tableau π into a finite sequence

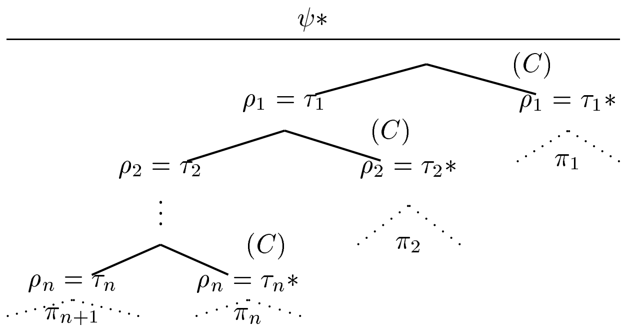
$$\sigma_1 \; \sigma_2 \; \ldots \; \sigma_k$$

ordered by the non-decreasing number of applications of the symbol f. The *weight* of the f-term τ_i is i. Note that the f-terms with higher weight cannot occur as subterms of f-terms with lesser weight.

A conclusion $\sigma_i = \sigma_j$ of a non-trivial f-substitution rule is assigned the *weight* $k \cdot \max(i, j) + \min(i, j)$. The *weight* of a tableau with all f-terms some σ_i is the maximum of weights of its non-trivial conclusions of f-substitution rules.

The lemma is proved by induction on the weight of π. If there are at most trivial f-substitution rules in π then we set $\pi_0 \equiv \pi$ and we are done. Note that this includes the case when $n = 0$ because then there are no f-rules.

If the weight of π is $m > 0$ then we select all non-trivial conclusions $f(\vec{\tau}) = f(\vec{\rho})$ and $f(\vec{\rho}) = f(\vec{\tau})$ of f-substitution rules with the weight m. We may assume without loss of generality that the weight of $f(\vec{\tau})$ is higher than the weight of $f(\vec{\rho})$. We intend to eliminate such rules, and thereby decrease the weight of π, by turning the f-substitution rules into trivial ones by deep replacing all occurrences of terms $f(\vec{\tau})$ by the term $f(\vec{\rho})$. As such a replacement may invalidate some f-substitution rules and axioms Sk_s we have to proceed with caution. We construct the tableau $\pi' : T, Sk_s, H_s \vdash \psi$ with weight $< m$ as:



where we will now determine the subtableaux $\pi_1, \ldots, \pi_n$, and π_{n+1}.

The tableau π can be visualized as follows:

$$
\begin{array}{ccc}
[\vec{\tau} = \vec{\rho}] & \qquad & [\vec{\rho} = \vec{\tau}] \\
\vdots & & \vdots \\
f(\vec{\tau}) = f(\vec{\rho}) \ \ (Fsub) & & f(\vec{\rho}) = f(\vec{\tau}) \ \ (Fsub) \\
\pi_a & & \pi_b
\end{array}
\tag{1}
$$

where we have indicated two typical conclusions of the f-substitution rules with the weight m. The notation $[\vec{\tau} = \vec{\rho}]$ is just an indication that the n-assumptions $\tau_1 = \rho_1, \ldots, \tau_n = \rho_n$ occur somewhere along the branch. For any i s.t. $1 \leq i \leq n$ we form the tableau π_i from π by the following replacements:

$$
\frac{\begin{array}{c} \psi* \\ \vdots \\ \rho_i = \tau_i* \\ \vdots \end{array}}{\begin{array}{ccc}
[\vec{\tau} = \vec{\rho}] & \qquad & [\vec{\rho} = \vec{\tau}] \\
\vdots & & \vdots \\
\rho_i = \tau_i \ \ (Sym) & & \circ \\
\circ & &
\end{array}}
$$

The reader will note that the tableau π_i is in the tableau π' at the end of the branch with the goal $\rho_i = \tau_i*$. In the transformation on the right the branch thus closes against the assumption $\rho_i = \tau_i$ which is among the ones indicated by $[\vec{\rho} = \vec{\tau}]$. In the transformation on the left we apply the symmetry rule to the assumption $\tau_i = \rho_i$ which is among the ones indicated by $[\vec{\tau} = \vec{\rho}]$. The conclusion $\rho_i = \tau_i$ of the symmetry rule thus closes the branch against the goal $\rho_i = \tau_i*$. We apply the shown transformation to all topmost conclusions in π of the f-substitution rule with the weight m. This means that the tableau π_i is without such rules and it has a weight $< m$.

For the construction of the tableau π_{n+1} we can visualize the tableau π as follows:

$$
\begin{array}{ccc}
 & \vdots & \\
[\vec{\tau} = \vec{\rho'}] & [\vec{\rho''} = \vec{\tau}] & \phi_1[\vec{\tau}, f(\vec{\tau})] \;\; (Ax) \\
\vdots & \vdots & \pi_c \\
f(\vec{\tau}) = f(\vec{\rho'}) \;\; (Fsub) & f(\vec{\rho''}) = f(\vec{\tau}) \;\; (Fsub) & \\
\pi_a & \pi_b &
\end{array}
\tag{2}
$$

where we have not shown the conclusions of f-substitution rules with the weight m as visualized in 6.4.4(1). We have instead shown two typical conclusions of non-trivial f-substitution rules containing $f(\vec{\tau})$ and which are with lesser weights. We have also application $\phi_1[\vec{\tau}, f(\vec{\tau})]$ of an axiom from Sk_s.

We now perform the deep replacement in the above copy of π of all f-terms $f(\vec{\tau})$ by the f-terms $f(\vec{\rho})$. The replacement turns all conclusions of f-substitution rules with weights m into conclusions of rules of reflexivity but it invalidates the conclusions of f-substitution rules similar to the two shown. It also invalidates the axiom rule from Sk_s The tableau-like tree after the replacement looks as shown in Fig. 6.1 where we have shown that the tree after a correction will be located in the tableau π' at the position of π_{n+1}.

$$
\begin{array}{ccc}
 & \psi * & \\
 & \rho_1 = \tau_1 & \\
 & \vdots & \\
 & \rho_n = \tau_n & \\
\hline
 & \vdots & \\
[\vec{\tau} = \vec{\rho'}] & [\vec{\rho''} = \vec{\tau}] & \phi_1[\vec{\tau}, f(\vec{\rho})] \;\; (?) \\
\vdots & \vdots & \pi_c \\
f(\vec{\rho}) = f(\vec{\rho'}) \;\; (?) & f(\vec{\rho''}) = f(\vec{\rho}) \;\; (?) & \\
\pi_a & \pi_b &
\end{array}
$$

Fig. 6.1. Tableau-like figure after the deep replacement $f(\vec{\tau}) := f(\vec{\rho})$

Note that the additional terms shown in the figure are not affected by the replacement because the f-term $f(\vec{\tau})$ cannot occur in them. Hovewever, there can be f-terms in the tableau π with higher weights than $f(\vec{\tau})$ and which can contain the last term as subterms. Since there are no non-trivial f-substitution rules for those higher weight f-terms in π, the replacement does not invalidate any of the rules containing the higher weight f-terms although the terms themselves change.

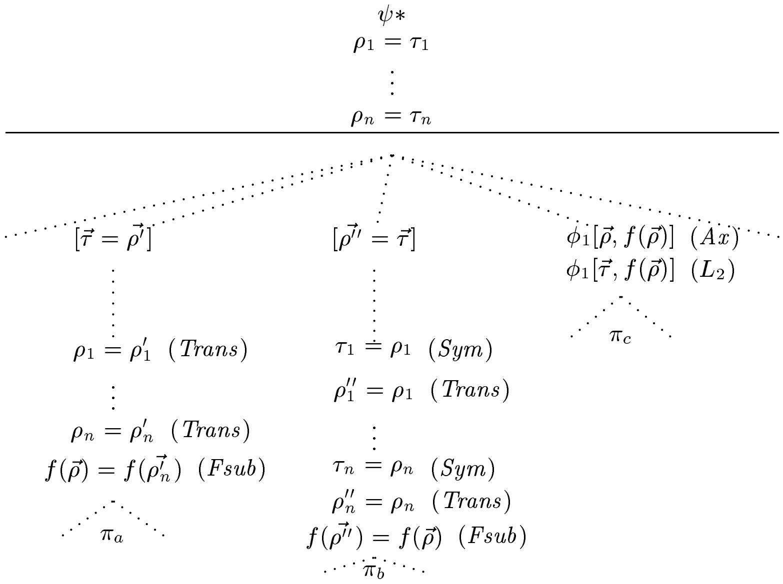


Fig. 6.2. Corrected tableau π_{n+1}

We now correct the tableau-like tree in Fig. 6.1 whereby we obtain the tableau π_{n+1} shown in Fig. 6.2. The branch above the tableau π_a is corrected by the insertion of n conclusions $\rho_i = \rho_i'$ of transitivity rules after which the formula $f(\vec{\rho}) = f(\vec{\rho'})$ is a conclusion of an f-substitution rule with weight $< m$. The branch above the tableau π_b is corrected by the insertion of conclusions of symmetry rules $\tau_i = \rho_i$ followed by conclusions of transitivity rules $\rho_i'' = \rho_i$. This is repeated n-times after which the formula $f(\vec{\rho''}) = f(\vec{\rho})$ is a conclusion of an f-substitution rule with a weight $< m$. The branch above the tableau π_c is corrected by an axiom $\phi_1[\vec{\rho}, f(\vec{\rho})]$ from Sk_s. We then use an admissible Leibnitz rule (L_2) to introduce the conclusion $\phi_1[\vec{\tau}, f(\vec{\rho})]$.

We perform the just described corrections for all conclusions similar to typical conclusions visualized in (2). The tableau π_{n+1} has a weight $< m$ and so does the tableau π'. We now apply the induction hypothesis to π' whereby we obtain a tableau π_0 s.t. $\pi_0 : T, Sk_s, H_s \vdash \psi$ without any non-trivial f-substitution rules. $\square$

6.4.5 Theorem. *Skolem extensions are conservative.*

Proof. Let S be a Skolem extension of T as in Par. 6.4.1 and assume $\pi : S \vdash \psi$ for a basic tableau π and a formula ψ of $\mathcal{L}_T$. Because of the Generalization rule 5.3.8 we may assume without loss of generality that ψ is a sentence. We now replace in π all free variables other than eigen-variables by arbitrary

Henkin constants from $\mathcal{L}_S$ whereby we obtain a closed tableau π_1 for ψ which is in the language $\mathcal{L}_s$. Note that variables other than eigen-variables can be introduced into π only by quantifier instantiation and reflexivity rules.

The next transformation is the elimination of all eigen-variable rules from π_1. The elimination is similar as in the proof of the Lemma 5.3.11 on the elimination of quantifier rules except that we do not eliminate the quantifier instantiation rules. Since the premises of all eigen-variable rules in π_1 are free for f, the introduced Henkin witnessing and counterexample axioms are from H_s and so we obtain a tableau π_2 consisting of sentences and such that $\pi_2 : S, H_s \vdash \psi$.

We now delete from π_2 all partial instances of the Skolem axiom 6.4.1(1) whereby we obtain a tableau π_3 such that $\pi_3 : T, Sk_s, H_s \vdash \psi$. The tableau satisfies the assumptions of Lemma 6.4.4 and we obtain from it a similar tableau $\pi_4 : T, Sk_s, H_s \vdash \psi$ which is without non-trivial f-substitution rules.

We intend to eliminate from π_4 the applications of axioms from Sk_s:

$$\phi_1[\vec{\tau}, f(\vec{\tau})] \equiv \exists y \phi[\vec{\tau}, y] \to \phi[\vec{\tau}, f(\vec{\tau})] \ .$$

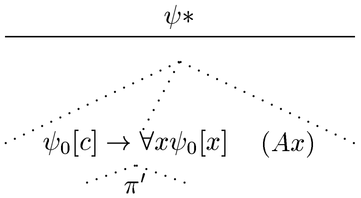
by deeply replacing the closed term $f(\vec{\tau})$ by the Henkin constant c belonging to the sentence $\exists y \phi[\vec{\tau}, y]$. This constant can be written with symbolic index as $c_{\exists y \phi[\vec{\tau}, y]}$ and the deep replacement turns the above axiom to a Henkin witnessing axiom from H_s:

$$\exists y \phi[\vec{\tau}, y] \to \phi[\vec{\tau}, c_{\exists x \phi[\vec{\tau}, x]}] \ .$$

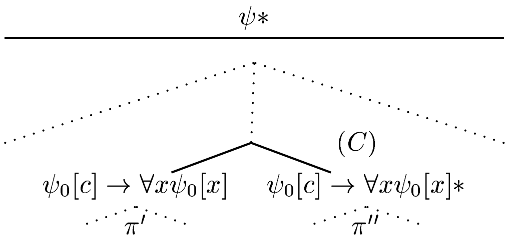
Toward that end we deeply replace all f-terms $f(\vec{\rho})$ in π_4 by the Henkin constants $c_{\exists y \phi[\vec{\rho}, y]}$ whereby we obtain a tableau π_5. The order of elimination of f-terms is immaterial because it leads to identical results but it is crucial that we perform the replacements not only in the formulas of π_4 but also in the indices of all Henking constants occurring in π_4. It should be clear that the elimination of f-terms turns the full instances of Skolem axioms into Henkin witnessing axioms from Ha_s and does not change the character of any other rules in π_4. Specifically, Henkin witnessing axioms are turned into Henkin witnessing axioms without f-terms.

There are no f-terms in the sentences of π_5, nor in the indices of its Henkin constants and we have $\pi_5 : T, H_s \vdash \psi$. We now take every Henkin constant occurring in π_5 and write in the symbolic form $c_{\exists x \psi_0[x]}$ where also the Henkin constants in ψ_0 are with symbolic indices and also the Henkin constants in these symbolic indices are such .... We change the symbolic indices back to the numerical form by looking up the existential sentences in the appropriate enumerations 5.1.6(1) but this time for the language $\mathcal{L}_t$. The look up is done first for the formulas of the lowest rank and then for the formulas with the next higher ranks, ... We thus obtain a tableau π_6 such that $\pi_6 : T, H_t \vdash \psi$.

We eliminate next the Henkin counterexample axioms from π_6 just as it was done in the proof of the theorem on the Introduction/elimination of quantifier rules 5.3.12. We, namely, take any counterexample axiom in π_6:



and replace it by a cut:



whose right branch is closed by the tableau π'' obtained by Lemma 5.3.9 to satisfy $\pi'' : Ha \vdash \psi_0[c] \to \forall x \psi_0[x]$. We denote by Ha the Henkin witnessing axioms for $\mathcal{L}_T$. We thus obtain a tableau π_7 such that $\pi_7 : T, Ha \vdash \psi$ to which we apply the Theorem on the conservativity of Henkin witnessing axioms 5.3.10 and obtain $T \vdash \psi$. $\square$

6.4.6 Skolemization and Herbrand's theorem. One of the uses of Skolem axioms is to eliminate, by a process called *Skolemization*, quantifiers from formulas at the price of introducing *Skolem* functions. Since we will not need this in the further development, we just illustrate the process with an example.

In order to eliminate the quantifiers from a sentence we bring it to a prenex form, say, $\exists x \forall y \exists z \forall w \phi[x, y, z, w]$ where the formula ϕ is quantifier free. We consider the following Skolem axioms:

$$\forall x(\exists y \forall z \exists w \neg\phi[x, y, z, w] \to \forall z \exists w \neg\phi[x, f(x), z, w])$$
$$\forall x \forall z(\exists w \neg\phi[x, f(x), z, w] \to \neg\phi[x, f(x), z, g(x, z)])$$

for new function symbols f and g. It is not hard to see that we have

$$\vdash \forall x \forall z \neg\phi[x, f(x), z, g(x, z)] \to \forall x \exists y \forall z \exists w \neg\phi[x, y, z, w] \tag{1}$$

in the predicate calculus. For the proof of converse we need the two Skolem axioms and we have

$$T \vdash \forall x \exists y \forall z \exists w \neg\phi[x, y, z, w] \to \forall x \forall z \neg\phi[x, f(x), z, g(x, z)] \tag{2}$$

in the theory T consisting of the two Skolem axioms.

The celebrated theorem of Herbrand asserts

$$\begin{aligned}&\models \exists x\forall y\exists z\forall w\phi[x,y,z,w] \Leftrightarrow \\ &\qquad \models_i \phi[\tau_1, f(\tau_1), \rho_1, g(\tau_1,\rho_1)] \vee \ldots \vee \phi[\tau_n, f(\tau_n), \rho_n, g(\tau_n,\rho_n)] \\ &\qquad \text{for some } n \geq 1 \text{ and terms } \tau_1,\, \rho_1,\, \ldots,\, \tau_n,\, \rho_n.\end{aligned}$$

We first show

$$\vdash \exists x\forall y\exists z\forall w\phi[x,y,z,w] \Leftrightarrow\; \vdash \exists x\exists z\phi[x,f(x),z,g(x,z)] \tag{3}$$

where the sentence $\exists x\exists z\phi[x,f(x),z,g(x,z)]$ is called a *Herbrand normal form* of the sentence $\exists x\forall y\exists z\forall w\phi[x,y,z,w]$.

(3): In the direction $\Rightarrow$ we assume $\vdash \exists x\forall y\exists z\forall w\phi[x,y,z,w]$. Thus $\vdash \neg\forall x\exists y\forall z\exists w\neg\phi[x,y,z,w]$ and we get $\vdash \neg\forall x\forall z\neg\phi[x,f(x),z,g(x,z)]$ by (1), i.e. $\vdash \exists x\exists z\phi[x,f(x),z,g(x,z)]$.

In the direction $\Leftarrow$ we assume $\vdash \exists x\exists z\phi[x,f(x),z,g(x,z)]$ and get $T \vdash \neg\forall x\forall z\neg\phi[x,f(x),z,g(x,z)]$. We then have $T \vdash \neg\forall x\exists y\forall z\exists w\neg\phi[x,y,z,w]$ by (2). We then get $\vdash \neg\forall x\exists y\forall z\exists w\neg\phi[x,y,z,w]$ by the conservativity of T and hence $\vdash \exists x\forall y\exists z\forall w\phi[x,y,z,w]$.

We show next

$$\begin{aligned}&\vdash \exists x\exists z\phi[x,f(x),z,g(x,z)] \Leftrightarrow \\ &\qquad \vdash_i \phi[\tau_1, f(\tau_1), \rho_1, g(\tau_1,\rho_1)] \vee \ldots \vee \phi[\tau_n, f(\tau_n), \rho_n, g(\tau_n,\rho_n)] \\ &\qquad \text{for some } n \geq 1 \text{ and terms } \tau_1,\, \rho_1,\, \ldots,\, \tau_n,\, \rho_n.\end{aligned} \tag{4}$$

In the direction ($\Rightarrow$) we assume $\pi : \;\vdash \exists x\exists z\phi[x,f(x),z,g(x,z)]$. We remove from the tableau π all conclusions $\exists z\phi[\tau,f(\tau),z,g(\tau,z)]*$ of $(\exists*)$-instantiation rules applied to $\exists x\exists z\phi[x,f(x),z,g(x,z)]*$ and then remove also all conclusions $\phi[\tau,f(\tau),\rho,g(\tau,\rho)]*$ of $(\exists*)$-instantiation rules applied to $\exists z\phi[\tau,f(\tau),z,g(\tau,z)]*$ whereby we obtain a tableau π_1 such that

$$\pi_1 : \;\vdash [\phi[\tau_1, f(\tau_1), \rho_1, g(\tau_1,\rho_1)]*, \ldots, \phi[\tau_n, f(\tau_n), \rho_n, g(\tau_n,\rho_n)]*]$$

where the shown n formulas are all conclusions removed in the second step. Form this we clearly get

$$\pi_2 : \;\vdash \phi[\tau_1, f(\tau_1), \rho_1, g(\tau_1,\rho_1)] \vee \ldots \vee \phi[\tau_n, f(\tau_n), \rho_n, g(\tau_n,\rho_n)]$$

for a tableau π_2 obtained from π_1 by n generalized flatten rules $(G\vee_i*)$. Since the tableau π_2 cannot apply any quantifier rules, it must be an identity tableau.

In the direction ($\Leftarrow$) we assume the right-hand-side of (4). We clearly have

$$\vdash \phi[\tau_i, f(\tau_i), \rho_i, g(\tau_i,\rho_i)] \to \exists x\exists z\phi[x,f(x),z,g(x,z)]$$

for all $1 \leq i \leq n$ from which we get the left-hand-side.

The above instance of the Herbrand's theorem now follows by combining the results (3) and (4) and by using soundness and completeness theorems for both quantifier and identity tableaux.

6.5 Extensions by Contextually Defined Functions

We can extend theories by explicit definitions of functions: $f(\vec{x}) = \tau[\vec{x}]$. That this is conservative can be then proved similarly as the conservativity of explicit definitions of predicates. In contrast to such definitions of predicates, explicitly defined functions do not fully use the power of first-order logic because the terms τ do not posses the full expressiveness of formulas. Contextually defined functions utilize the full power of formulas.

As an example consider a formal theory of arithmetic which has multiplication, addition, and constant 1. We have seen in Sect. 6.3 how to extend such a theory by explicit definition of the predicate $<$. We can further define the binary predicate $x \leq y \leftrightarrow x < y \lor x = y$ and the unary square function $x^2 = x{\cdot}x$ by explicit definitions. Let us call such a theory T. We can extend T to S by extending its language with the unary function symbol $[\sqrt{\cdot}]$ intended to denote the whole part of square root. We can find a formula of $\mathcal{L}_T$ equivalent to the formula $[\sqrt{x}] = y$ applying the square root function in the context of an atomic formula. We can use the formula in the contextual definition:

$$[\sqrt{x}] = y \leftrightarrow y^2 \leq x \land x < (y+1)^2$$

This definition can be justified if we can prove in T that to every individual there will exactly one square root. This amounts to proving the following:

$$T \vdash \exists y(y^2 \leq x \land x < (y+1)^2)$$
$$T \vdash y_1^2 \leq x \land x < (y_1+1)^2 \land y_2^2 \leq x \land x < (y_2+1)^2 \to y_1 = y_2 \ .$$

We can then translate every formula of $\mathcal{L}_S$ into an equivalent formula of $\mathcal{L}_T$ where every application of $[\sqrt{\tau}]$ used in a context of an atomic formula $\phi[z]$ as $\phi[[\sqrt{\tau}]]$ is translated to the formula on the right for which S proves:

$$S \vdash \phi[[\sqrt{\tau}]] \leftrightarrow \exists z(z^2 \leq \tau \land \tau < (z+1)^2 \leftrightarrow \phi[z]) \ .$$

6.5.1 Extensions by contextually defined functions. Let T be a theory, $\phi[\vec{x}, y]$ a formula of $\mathcal{L}_T$ with the free variables among the indicated ones, and f a new n-ary function symbol ($n \geq 0$). If T proves the *existence*:

$$T \vdash \exists y\, \phi[\vec{x}, y] \tag{1}$$

and the *uniqueness*

$$T \vdash \phi[\vec{x}, y_1] \land \phi[\vec{x}, y_2] \to y_1 = y_2 \tag{2}$$

conditions then we can extend T to S by adding to $\mathcal{L}_T$ the function symbol f and to the axioms of T any closure of

$$f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y] \tag{3}$$

as the *defining axiom* for f. Because $S = T, \forall(3)$ we trivially have $S \vdash T$ and so S extends T. We call this kind of extension *extension by contextually defined function*. The term 'contextual' refers to the fact that although we are not able to find a term ρ of $\mathcal{L}_T$ identical to $f(\vec{x})$, we have a formula $\phi[\vec{\tau}, \rho]$ of $\mathcal{L}_T$ equivalent to an application of f in the context of an atomic formula $f(\vec{\tau}) = \rho$ for all terms $\vec{\tau}$, ρ of $\mathcal{L}_T$. Note that f cannot be applied in ϕ which is of $\mathcal{L}$ and so contextual definitions are not recursive. We have

$$S \vdash f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y] \tag{4}$$

by Thm. 5.3.8 because S trivially proves its axiom $\forall(3)$.

6.5.2 Translation function. Let S be the extended theory $T, \forall 6.5.1(3)$. For every atomic formula ψ of $\mathcal{L}_S$ we define by induction on the number k of applications of f in ψ a formula $\psi^\star$ of $\mathcal{L}_T$ called a *translation* of ψ. If $k = 0$ then we set $\psi^\star \equiv \psi$. Otherwise we have $\psi \equiv \psi_1[f(\vec{\tau})]$ for some terms $\vec{\tau}$ of $\mathcal{L}_T$ and a formula $\psi_1[z]$ of $\mathcal{L}_S$ with $< k$ applications of f. We then set

$$\psi^\star \equiv \exists z(\phi'[\vec{\tau}, z] \land \psi_1[z]^\star) \tag{1}$$

where ϕ' is a variant of ϕ with the bound variables different from z and those free in $\vec{\tau}$. Note that $\psi_1[z]^\star$ is a formula of $\mathcal{L}_T$ by IH and so is the formula $\psi^\star$. We extend the translation function to all formulas ψ of $\mathcal{L}_S$ by designating by $\psi^\star$ any formula obtained from ψ by replacing any of its atomic formulas ψ_1 by formulas $\psi_1^\star$.

6.5.3 Translation lemma. *If S is the extended theory $T, \forall 6.5.1(3)$ and ψ a formula of $\mathcal{L}_S$ then we have*

$$S \vdash \psi \leftrightarrow \psi^\star \ . \tag{1}$$

Proof. We first prove (1) for atomic ψ by metainduction on the number of applications of f in ψ. If there are none then the property is a tautology because $\psi^\star \equiv \psi$. Otherwise, using the notation of Par. 6.5.2 we have $\psi \equiv \psi_1[f(\vec{\tau})]$ and $\psi^\star \equiv 6.5.2(1)$ for some terms $\vec{\tau}$ of $\mathcal{L}_T$ and a formula $\psi_1[z]$ of $\mathcal{L}_S$ with $< k$ applications of f. Working in S we obtain $f(\vec{\tau}) = z \leftrightarrow \phi'[\vec{\tau}, z]$ by the Variant theorem (6.1.6) from an instantiation of the defining axiom for f. Hence $\exists z(f(\vec{\tau}) = z \land \psi_1[z]^\star) \leftrightarrow \psi^\star$ by the Equivalence theorem (6.1.5). We have $\psi[z] \leftrightarrow \psi_1[z]^\star$ by IH and so $\exists z(f(\vec{\tau}) = z \land \psi_1[z]) \leftrightarrow \psi^\star$. Thus $\psi_1[f(\vec{\tau})] \leftrightarrow \psi^\star$ by Identity theorem (6.1.4). ☐

6.5.4 Theorem. *The extension $S = T, \forall(f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y])$ of T by the contextually defined function f is conservative and for any formula ψ of $\mathcal{L}_T$ we have*

$$S \vdash \psi \Leftrightarrow T \vdash \psi^\star \ . \tag{1}$$

Proof. Designate by T_2 the Skolem extension of T with a closure of

$$\exists y\phi[\vec{x},y] \rightarrow \phi[\vec{x},f(\vec{x})]\ . \tag{2}$$

T_2 is conservative over T by Thm. 6.4.5 and $\mathcal{L}_S = \mathcal{L}_{T_2}$. If we succeed in proving

$$S \equiv T_2 \tag{3}$$

then for any ψ of $\mathcal{L}_T$ such that $S \vdash \psi$ we will have $T_2 \vdash \psi$ by (3) and $T \vdash \psi$ because T_2 is conservative over T.

(3): In order to prove that S extends T_2 it suffices to derive (2) in S. So working in S we instantiate its defining axiom for f with $y := f(\vec{x})$ and obtain $\phi[\vec{x},f(\vec{x})]$. from which (2) trivially follows.

That T_2 extends S follows from a proof in T_2 of $f(\vec{x}) = y \leftrightarrow \phi[\vec{x},y]$. In the direction ($\rightarrow$) it suffices to prove $\phi[\vec{x},f(\vec{x})]$. Since T_2 proves the existence condition 6.5.1(1) because it extends T and also the instance (2) of its Skolem axiom, we obtain $\phi[\vec{x},f(\vec{x})]$. In the direction ($\leftarrow$) and working in T_2 we assume $\phi[\vec{x},y]$ from which we get $\exists y\phi[\vec{x},y]$ and then $\phi[\vec{x},f(\vec{x})]$ from (2). We then get $f(\vec{x}) = y$ from the uniqueness condition 6.5.1(2) which holds in T_2.

(1): In the direction ($\rightarrow$) assume $S \vdash \psi$. We have $S \vdash \psi^\star$ by Lemma 6.5.3 and, since $\phi^\star$ is of $\mathcal{L}_T$, we obtain $T \vdash \psi^\star$ because S is conservative over T. In the direction ($\leftarrow$) assume $T \vdash \psi^\star$. Since S extends T, we have $S \vdash \psi^\star$ and so $S \vdash \psi$ by Lemma 6.5.3. ☐

6.6 Extensions by Definitions

Extensions of theories T to S by explicit definitions of predicates and by contextual definition of functions have the important property that any model of T is uniquely expanded to a model of S. This, and the property that the theorems of S can be translated to the theorems of T and back, are crucial to our treatment of formal arithmetic in the Part II of this text.

6.6.1 Extensions by definitions. Let T be a theory and T_1 its conservative extension either by explicit definition of a predicate P or by contextual definition of a function f. Let S be a theory in the same language as $\mathcal{L}_{T_1}$. We say that S is an *extension by definition* of T if S and T_1 are equivalent. This can be visualized as

$$S \vdash \psi_1 \Leftrightarrow T,\psi \vdash \psi_1 \qquad \text{for any formula } \psi_1 \text{ of } \mathcal{L}_S \tag{1}$$

where ψ is the defining axiom of T_1, i.e a universal closure of either $P(\vec{x}) \leftrightarrow \phi[\vec{x}]$ or $f(\vec{x}) = y \leftrightarrow \phi[\vec{x},y]$ for a suitable formula ϕ of $\mathcal{L}_T$.

A theory S is an *extension by definitions* of a theory T if S is obtained by a finite number of extensions by definition of T, i.e. if there is a number n and theories T_0, T_1, …, T_n such that $T = T_0$, T_{i+1} is an extension by definition of T_i for every $i < n$, and $S = T_n$.

6.6.2 Theorem (Extensions by definitions). *If the theory S is an extension by definitions of a theory T then S is conservative over T, every model of T has a unique expansion to the model of S, and there is an effective translation function taking formulas ψ of $\mathcal{L}_S$ to formulas $\psi^\star$ of $\mathcal{L}_T$ such that for every formula ψ of $\mathcal{L}_S$ we have*

$$S \vdash \psi \leftrightarrow \psi^\star \tag{1}$$

$$S \vdash \psi \Leftrightarrow T \vdash \psi^\star \ . \tag{2}$$

Proof. By induction on the number k of extensions by definition of T to obtain S. If $k = 0$ then $S = T$ and there is nothing to prove. If $k > 0$ then S is an extension by definition of a theory T_1 which is obtained by $k-1$ extensions by definition from T. By IH there is an effective translation function taking formulas ψ of $\mathcal{L}_{T_1}$ to formulas $\psi^{\star_1}$ of $\mathcal{L}_T$ such that

$$T_1 \vdash \psi \leftrightarrow \psi^{\star_1} \tag{3}$$

$$T_1 \vdash \psi \Leftrightarrow T \vdash \psi^{\star_1} \ . \tag{4}$$

Since S is an extension by definition of T_1, there is a defining axiom ψ_1 of $\mathcal{L}_S$ such that $S \equiv T_1, \forall\psi_1$. Depending on whether the new symbol of S is a predicate symbol P or a function symbol f, there is by Translation Lemma 6.3.3 or 6.5.3 an effective translation function, which takes formulas ψ of $\mathcal{L}_S$ to formulas $\psi^{\star_2}$ of $\mathcal{L}_{T_1}$, and such that

$$T_1, \forall\psi_1 \vdash \psi \leftrightarrow \psi^{\star_2} \ . \tag{5}$$

We also have

$$T_1, \forall\psi_1 \vdash \psi \Leftrightarrow T_1 \vdash \psi^{\star_2} \tag{6}$$

by Theorem 6.3.4 or 6.5.4.

We define the translation function taking formulas ψ of $\mathcal{L}_S$ to formulas $\psi^\star$ of $\mathcal{L}_T$ as $\psi^\star \equiv (\psi^{\star_2})^{\star_1}$. The translation function is clearly effective.

(1): We work in the theory $T_1, \forall\psi_1$ and take any formula ψ of $\mathcal{L}_S$. We have ψ iff $\psi^{\star_2}$ by (5) iff, since $T_1, \forall\psi_1$ is an extension of T_1, $(\psi^{\star_2})^{\star_1}$, i.e. $\psi^\star$, by (3). We have just proved $T_1, \forall\psi_1 \vdash \psi \leftrightarrow \psi^\star$. Thus also (1) because S is equivalent to $T_1, \forall\psi_1$.

(2): Take any formula ψ of $\mathcal{L}_S$. We have $S \vdash \psi$ iff, by the equivalence, $T_1, \forall\psi_1 \vdash \psi$ iff, by (6), $T_1 \vdash \psi^{\star_2}$ iff, by (4), $T \vdash (\psi^{\star_2})^{\star_1}$ iff $T \vdash \psi^\star$.

We now prove that S is conservative over T. So we take any formula ψ of $\mathcal{L}_T$ and assume $S \vdash \psi$. We have $T \vdash \psi^\star$ by (2) and, since $\psi^\star \equiv \psi$, also $T \vdash \psi$.

Now suppose that a structure $\mathcal{M}$ for $\mathcal{L}_T$ with a domain D is a model of T: $\mathcal{M} \vDash T$. There is a unique expansion $\mathcal{M}_1$ of $\mathcal{M}$ which is a model of

T_1 by IH. We expand $\mathcal{M}_1$ to the structure $\mathcal{N}$ for $\mathcal{L}_S$ by choosing a suitable interpretation of the new symbol P or f. For any such interpretation we will have $\mathcal{N} \models S$ iff, by the completeness and by $S \equiv T_1, \forall\psi_1$, $\mathcal{N} \models T_1, \forall\psi_1$ iff, since $\mathcal{N} \models T_1$ by Thm. 5.2.7, $\mathcal{N} \models \forall\psi$.

We now consider two cases. If $\psi \equiv P(\vec{x}) \leftrightarrow \phi[\vec{x}]$ then $\mathcal{N} \models \forall\psi$ iff $\mathcal{N} \models \forall\vec{x}(P(\vec{x}) \leftrightarrow \phi[\vec{x}])$ iff for all $\vec{d} \in D$

$$P^{\mathcal{N}}(\vec{d}) \Leftrightarrow \mathcal{N} \models P(\vec{x})[\vec{d}] \Leftrightarrow \mathcal{N} \models \phi[\vec{d}] \overset{5.2.7}{\Leftrightarrow} \mathcal{M}_1 \models \phi[\vec{d}]$$

which means that the unique interpretation $P^{\mathcal{N}}(\vec{d}) \Leftrightarrow \mathcal{M}_1 \models \phi[\vec{d}]$ is both sufficient and necessary for $\mathcal{N}$ to be a model of S.

If $\psi \equiv f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y]$ then for all $\vec{d} \in D$ there is a $k \in d$ such that $\mathcal{M}_1 \models \phi[\vec{d}, k]$ by the existence condition and this k is unique because for any k_1 we have

$$\mathcal{M}_1 \models \phi[\vec{d}, k] \text{ and } \mathcal{M}_1 \models \phi[\vec{d}, k_1] \Rightarrow k = k_1$$

by the uniqueness condition. We have $\mathcal{N} \models \forall\psi$ iff $\mathcal{N} \models \forall\vec{x}\forall y(f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y])$ iff for all $\vec{d}, k \in D$

$$f^{\mathcal{N}}(\vec{d}) = k \Leftrightarrow \mathcal{N} \models (f(\vec{x}) = y)[\vec{d}, k] \Leftrightarrow \mathcal{N} \models \phi[\vec{d}, k] \overset{5.2.7}{\Leftrightarrow} \mathcal{M}_1 \models \phi[\vec{d}, k] \ .$$

But this means that interpreting $f^{\mathcal{N}}$ for $\vec{d} \in D$ as the unique $k \in D$ such that $\mathcal{M}_1 \models \phi[\vec{d}, k]$ is both sufficient and necessary for $\mathcal{N}$ to be a model of S. □

6.6.3 Theorem (Implicit definition of functions). *For any theory T and any formula $\phi[\vec{x}, y]$ of $\mathcal{L}_T$ with the free variables among the $n+1$ indicated ones and satisfying the existence and uniqueness conditions the extension of $\mathcal{L}_T$ with a new n-ary function symbol f and of T with a new axiom:*

$$\forall\vec{x}\phi[\vec{x}, f(\vec{x})]$$

is an extension by definition.

Proof. Designate by S the extended theory. It is sufficient to prove that S is equivalent to the extension T_1 of T by the contextual definition $\forall\vec{x}\forall y(f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y])$ because T_1 is an extension by definition of T. By instantiating the defining axiom of T_1 with $y := f(\vec{x})$ and generalizing we obtain $T_1 \vdash \forall\vec{x}\phi[\vec{x}, f(\vec{x})]$ and so T_1 extends S.

In order to demonstrate that S extends T_1 it suffices to show $S \vdash f(\vec{x}) = y \leftrightarrow \phi[\vec{x}, y]$. Working in S we assume in the direction $(\rightarrow)$ $f(\vec{x}) = y$. We then obtain $\phi[\vec{x}, y]$ because $\phi[\vec{x}, f(\vec{x})]$ follows from the new axiom of S. In the direction $(\leftarrow)$ we assume $\phi[\vec{x}, y]$ and, since $\phi[\vec{x}, f(\vec{x})]$, we obtain $f(\vec{x}) = y$ by the uniqueness condition which is provable in S because S extends T. □

6.6.4 Theorem (Explicit definition of functions). *For any theory T and any term $\tau[\vec{x}]$ of $\mathcal{L}_T$ with the free variables among the n indicated ones the extension of $\mathcal{L}_T$ with a new n-ary function symbol f and of T with a new axiom:*

$$\forall \vec{x}\, f(\vec{x}) = \tau[\vec{x}]$$

is an extension by definition.

Proof. Designate by S the extended theory. We first show that T proves the existence and uniqueness conditions for the formula $\phi[\vec{x}, y] \equiv f(\vec{x}) = \tau[\vec{x}]$ The existence condition $\exists y\, y = \tau[\vec{x}]$ follows from $\tau[\vec{x}] = \tau[\vec{x}]$. For the uniqueness condition assume $y_1 = \tau[\vec{x}]$ and $y_2 = \tau[\vec{x}]$ and obtain $y_1 = y_2$ by the properties of identity. We now use Thm. 6.6.3 to extend by definition T to S with the new axiom $\forall \vec{x}\, f(\vec{x}) = \tau[\vec{x}]$. □

7. Peano Arithmetic

7.1 Basic Theorems in PA

In this section we introduce and prove basic theorems of the formal system of arithmetic called Peano arithmetic.

7.1.1 Language of Peano arithmetic. The language $\mathcal{L}_{\mathrm{PA}}$ of Peano arithmetic consists of the constant 0, the unary function symbol x', and of two binary function symbols $x+y$ and $x{\cdot}y$. Both $+$ and $\cdot$ associate to the left and $\cdot$ has greater precedence than $+$.

We will abbreviate $0'$ as 1 but only in this section.

7.1.2 Axioms of Peano arithmetic. The axioms of Peano arithmetic consist of universal closures of the following six formulas:

$$\vdash_{\overline{\mathrm{PA}}} 0 \neq x' \tag{1}$$
$$\vdash_{\overline{\mathrm{PA}}} x' = y' \to x = y \tag{2}$$
$$\vdash_{\overline{\mathrm{PA}}} 0 + y = y \tag{3}$$
$$\vdash_{\overline{\mathrm{PA}}} x' + y = (x+y)' \tag{4}$$
$$\vdash_{\overline{\mathrm{PA}}} 0{\cdot}y = y \tag{5}$$
$$\vdash_{\overline{\mathrm{PA}}} x'{\cdot}y = x{\cdot}y + y \tag{6}$$

and for every formula $\phi[x]$ of $\mathcal{L}_{\mathrm{PA}}$ and an indicated variable x a universal closure of the *induction axiom* $I_x\phi[x]$:

$$\vdash_{\overline{\mathrm{PA}}} \phi[0] \land \forall x(\phi[x] \to \phi[x']) \to \phi[x] \ . \tag{7}$$

The *induction formula* $\phi[x]$ can contain, in addition to the *induction* variable x, zero or more free variables as *parameters*.

We use the symbol $\vdash_{\overline{\mathrm{PA}}} \phi$ of *provability in* PA as an abbreviation for $\mathrm{PA} \vdash \phi$.

7.1.3 The standard model $\mathcal{N}$ of PA. The *standard model* $\mathcal{N}$ of Peano arithmetic is the structure for $\mathcal{L}_{\mathrm{PA}}$ whose domain is the set of natural numbers $\mathbb{N}$ and the interpretations $0^{\mathcal{N}}$, ${}'^{\mathcal{N}}$, $+^{\mathcal{N}}$, and $\cdot^{\mathcal{N}}$ of the function symbols of

$\mathcal{L}_{\mathrm{PA}}$ are in that order the number 0, the *successor* function $S(x) = x + 1$, the addition, and multiplication functions. We leave to the reader the obvious demonstration that $\mathcal{N}$ satisfies the six axioms 7.1.2(1) through 7.1.2(6).

We now prove that also the induction axioms 7.1.2(7) are satisfied in $\mathcal{N}$. So take any formula $\phi[x, \vec{y}]$ of $\mathcal{L}_{\mathrm{PA}}$ with all its free variables among the indicated ones. We wish to show $\mathcal{N} \vDash \forall x \forall \vec{y} I_x \phi[x, \vec{y}]$. For that we take any $\vec{d} \equiv d_1, \ldots, d_n \in \mathbb{N}$ and it clearly suffices to show $\mathcal{N} \vDash \forall x \phi[x, \vec{d}]$. So assume on the contrary that $\mathcal{N} \nvDash [m, \vec{d}]$ for some $m \in \mathbb{N}$. Furthermore, assume that m is the least such number. We thus have the base case assumption $\mathcal{N} \vDash \phi[0, \vec{d}]$, the inductive assumption: $\mathcal{N} \vDash \forall x(\phi[x, \vec{d}] \to \phi[x, \vec{d}])$, and $\mathcal{N} \nvDash \phi[m, \vec{d}]$. Consider now two cases. If $m = 0$ then we get a contradiction with the base case assumption. If $m > 0$ then we have $\mathcal{N} \vDash \phi[m - 1, \vec{d}]$ by the minimality of m and we get a contradiction $\mathcal{N} \vDash \phi[(m - 1) + 1, \vec{d}]$ from the inductive assumption.

7.1.4 Informal reasoning by induction. Induction axioms of PA can be used anywhere in the proofs in PA. The typical situation is that we use an axiom $I_x \phi[x]$ in an instantiation $x := \tau$:

$$\phi[0] \land \forall x(\phi[x] \to \phi[x']) \to \phi[\tau]$$

under certain assumptions $\psi_1, \ldots, \psi_k$. The informal use of this axiom is to derive the formula $\phi[\tau]$ by considering two cases.

In the *base* case we prove $\phi[0]$ under the above assumptions.

In the *inductive* case we prove $\phi[x']$ for a new eigen-variable x under the same assumptions $\psi_1, \ldots, \psi_k$ to which we add *inductive hypothesis* $\phi[x]$, shortly IH, as an additional assumption.

Both cases taken together then prove $\phi[\tau]$ from $I_x \phi[\tau]$ by modus ponens.

7.1.5 Case analysis on 0 and positive numbers. The base case analysis is on 0 and on positive numbers:

$$\vdash_{\mathrm{PA}} x = 0 \lor \exists y\, x = y' \tag{1}$$

which is proved by induction on x. In the base case there is nothing to prove. In the inductive case we get $\exists y\, x' = y'$ from $x' = x'$.

7.1.6 Successor versus addition. We have

$$\vdash_{\mathrm{PA}} 1 + x = x' \tag{1}$$

because

$$1 + x = 0' + x \stackrel{7.1.2(4)}{=} (0 + x)' \stackrel{7.1.2(3)}{=} x' \ .$$

7.1.7 Nullpoints of addition. We have the following property of addition:

$$\vdash_{\mathrm{PA}} x + y = 0 \leftrightarrow x = 0 \land y = 0 \tag{1}$$

In the direction ($\rightarrow$) assume $x + y = 0$ and consider two cases by 7.1.5(1). If $x = 0$ then we have $0 = 0 + y \overset{7.1.2(3)}{=} 0$. The case $x = x_1'$ for some x_1 cannot hold because it leads to a contradiction: $0 = x_1' + y \overset{7.1.2(4)}{=} (x + y)'$ by 7.1.2(1). In the direction ($\leftarrow$) the property is a direct consequence of 7.1.2(3).

7.1.8 Addition is commutative. In order to prove that $+$ commutes

$$\vdash_{\mathrm{PA}} x + y = y + x \tag{1}$$

we need two lemmas

$$\vdash_{\mathrm{PA}} x + 0 = x \tag{2}$$

$$\vdash_{\mathrm{PA}} x + y' = x' + y. \tag{3}$$

(2) is proved by induction on x. In the base case we have $0 + 0 \overset{7.1.2(3)}{=} 0$ and in the inductive case:

$$x' + 0 \overset{7.1.2(4)}{=} (x + 0)' \overset{IH}{=} x' \; .$$

(3) is proved by induction on x. In the base case we have

$$0 + y' \overset{7.1.2(3)}{=} y' \overset{7.1.2(3)}{=} (0 + y)' \overset{7.1.2(4)}{=} 0' + y \; .$$

In the inductive case we have

$$x' + y' \overset{7.1.2(4)}{=} (x + y')' \overset{IH}{=} (x' + y)' \overset{7.1.2(4)}{=} x'' + y \; .$$

We now prove (1) by induction on x. In the base case we have

$$0 + y \overset{7.1.2(3)}{=} y \overset{(2)}{=} y + 0 \; .$$

In the inductive case we have

$$x' + y \overset{7.1.2(4)}{=} (x + y)' \overset{IH}{=} (y + x)' \overset{7.1.2(4)}{=} y' + x \overset{(3)}{=} y + x' \; .$$

From now on we will not explicitly indicate the uses of the two axioms of addition 7.1.2(3)(4).

7.1.9 Addition is associative. That the addition is associative

$$\vdash_{\mathrm{PA}} (x + y) + z = x + (y + z) \tag{1}$$

is proved by induction on x. In the base case we have:

$$(0 + y) + z = y + z = 0 + (y + z) \; .$$

In the inductive case we have:

$$(x' + y) + z = (x + y)' + z = ((x + y) + z)' \overset{IH}{=} (x + (y + z))' = x' + (y + z) \; .$$

7.1.10 Cancellation rules for addition. *Cancellation* rules for the addition are:

$$\vdash_{\mathrm{PA}} z + x = z + y \to x = y \tag{1}$$
$$\vdash_{\mathrm{PA}} x + z = y + z \to x = y \ . \tag{2}$$

(1) is proved by induction on z. In the base case we have

$$0 + x = 0 + y \Rightarrow x = y \ .$$

In the inductive case we have

$$z' + x = z' + y \Rightarrow (z + x)' = (z + y)' \overset{7.1.2(2)}{\Rightarrow} z + x = z + y \overset{IH}{\Rightarrow} x = y \ .$$

(2) is proved as follows:

$$x + z = y + z \overset{7.1.8(1)}{\Rightarrow} z + x = z + y \overset{(1)}{\Rightarrow} x = y \ .$$

From now on we will not explicitly indicate the properties of addition proved until now.

7.1.11 Multiplication by 0 and 1. We have

$$\vdash_{\mathrm{PA}} x{\cdot}0 = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} x{\cdot}1 = 1 \ . \tag{2}$$

(1) is proved by induction on x. In the base case we have $0{\cdot}0 \overset{7.1.2(5)}{=} 0$. In the inductive case we have:

$$x'{\cdot}0 \overset{7.1.2(6)}{=} x{\cdot}0 + 0 = x{\cdot}0 \overset{IH}{=} 0 \ .$$

(2) is proved by induction on x. In the base case we have $0{\cdot}1 \overset{7.1.2(5)}{=} 0$. In the inductive case we have

$$x'{\cdot}1 \overset{7.1.2(6)}{=} x{\cdot}1 + 1 = 1 + x{\cdot}1 \overset{IH}{=} 1 + x = x + 1 = x' \ .$$

7.1.12 Units of multiplication. Multiplication has the following property

$$\vdash_{\mathrm{PA}} x{\cdot}y = 1 \leftrightarrow x = 1 \land y = 1 \ . \tag{1}$$

Indeed, in the direction ($\to$) we assume $x{\cdot}y = 1$ and consider three cases for x. The case $x = 0$ leads to the contradiction $0' = 1 = 0{\cdot}y \overset{7.1.2(5)}{=} 0$. If $x = 1$ then we have

$$1 = 1{\cdot}y = 0'{\cdot}y \overset{7.1.2(6)}{=} 0{\cdot}y + y \overset{7.1.2(5)}{=} 0 + y = y \ .$$

The case $x = x_1''$ for some x_1 cannot happen, This is shown by considering two cases for y. The case $y = 0$ leads to a contradiction

$$0' = 1 = x_1''{\cdot}0 \overset{7.1.11(1)}{=} 0\ .$$

Also the second case $y = y_1'$ for some y_1 leads to a contradiction:

$$0' = 1 = x_1''{\cdot}y_1' \overset{7.1.2(6)}{=} x_1'{\cdot}y_1' + y_1' \overset{7.1.2(6)}{=} x_1{\cdot}y_1' + y_1' + y_1' = (x_1{\cdot}y_1' + y_1 + y_1)''\ .$$

The direction $(\leftarrow)$ follows from the following

$$1{\cdot}1 = 0'{\cdot}1 \overset{7.1.2(6)}{=} 0{\cdot}1 + 1 \overset{7.1.2(5)}{=} 0 + 1 = 1\ .$$

7.1.13 Multiplication distributes over addition. The *distributive* property of the multiplication:

$$\vdash_{\mathrm{PA}}\ z{\cdot}(x + y) = z{\cdot}x + z{\cdot}y \tag{1}$$

is proved by induction on z. In the base case we have

$$0{\cdot}(x + y) \overset{7.1.2(5)}{=} 0 = 0 + 0 \overset{7.1.2(5)}{=} 0{\cdot}x + 0{\cdot}y\ .$$

In the inductive case we have

$$\begin{aligned} z'{\cdot}(x + y) &\overset{7.1.2(6)}{=} z{\cdot}(x + y) + (x + y) \overset{IH}{=} (z{\cdot}x + z{\cdot}y) + (x + y) = \\ &z{\cdot}x + (z{\cdot}y + (x + y)) = z{\cdot}x + (z{\cdot}y + (y + x)) = z{\cdot}x + ((z{\cdot}y + y) + x) \overset{7.1.2(6)}{=} \\ &z{\cdot}x + (z'{\cdot}y + x) = z{\cdot}x + (x + z'{\cdot}y) = (z{\cdot}x + x) + z'{\cdot}y \overset{7.1.2(6)}{=} z'{\cdot}x + z'{\cdot}y\ . \end{aligned}$$

From now on we will not explicitly indicate the uses of the two axioms of multiplication 7.1.2(5)(6).

7.1.14 Multiplication is commutative. That the multiplication commutes:

$$\vdash_{\mathrm{PA}}\ x{\cdot}y = y{\cdot}x \tag{1}$$

is proved by induction on x. In the base case we have

$$0{\cdot}y = 0 \overset{7.1.11(1)}{=} y{\cdot}0\ .$$

In the inductive case we have

$$x'{\cdot}y = x{\cdot}y + y \overset{7.1.11(2)}{=} x{\cdot}y + y{\cdot}1 \overset{IH}{=} y{\cdot}x + y{\cdot}1 \overset{7.1.11(1)}{=} y{\cdot}(x + 1) = y{\cdot}x'\ .$$

7.1.15 Multiplication is associative. The proof that the multiplication is associative:

$$\vdash_{\mathrm{PA}} (x{\cdot}y){\cdot}z = x{\cdot}(y{\cdot}z) \tag{1}$$

is by induction on x. In the base case we have

$$(0{\cdot}y){\cdot}z = 0{\cdot}z = 0 = 0{\cdot}(y{\cdot}z) \ .$$

In the inductive case we have

$$(x'{\cdot}y){\cdot}z = (x{\cdot}y + y){\cdot}z \overset{7.1.14(1)}{=} z{\cdot}(x{\cdot}y + y) \overset{7.1.11(1)}{=} z{\cdot}(x{\cdot}y) + z{\cdot}y \overset{7.1.14(1)}{=}$$
$$(x{\cdot}y){\cdot}z + y{\cdot}z \overset{IH}{=} x{\cdot}(y{\cdot}z) + y{\cdot}z = x'{\cdot}(y{\cdot}z) \ .$$

7.1.16 Cancellation rules for multiplication. *Cancellation* rules for the multiplication are:

$$\vdash_{\mathrm{PA}} \ z \neq 0 \land z{\cdot}x = z{\cdot}y \rightarrow x = y \tag{1}$$
$$\vdash_{\mathrm{PA}} \ z \neq 0 \land x{\cdot}z = y{\cdot}z \rightarrow x = y \ . \tag{2}$$

(1) follows by the commutativity of multiplication from (2) which is proved by assuming $z = z_1'$ for some z_1 and continuing by induction on x with the induction formula $\forall y(x{\cdot}z_1' = y{\cdot}z_1' \rightarrow x = y)$. In the base case we take any y, assume $0{\cdot}z_1' = y{\cdot}z_1'$, and consider two cases. If $y = 0$ then we have $x = 0 = y$ trivially. The case $y = y_1'$ for some y_1 leads to a contradiction:

$$0 = 0{\cdot}z_1' = y_1'{\cdot}z_1' = y{\cdot}z_1' + z_1' = (y_1{\cdot}z_1' + z_1)' \ .$$

In the inductive case we take any y, assume $x'{\cdot}z_1' = y{\cdot}z_1'$, and consider two cases again. If $y = 0$ then the assumption is shown contradictory similarly as above. If $y = y_1'$ then we have

$$x{\cdot}z_1' + z_1' = x'{\cdot}z_1' = y_1'{\cdot}z_1' = y_1{\cdot}z_1' + z_1'$$

and so $x{\cdot}z_1' = y_1{\cdot}z_1'$. We obtain $x = y_1$ by IH and so we get $x' = y_1'$.

From now on we will not explicitly refer to the properties of multiplication proved until now.

7.2 Extensions of PA

We study in this section the effect of extensions by definitions of PA on the axioms of induction.

7.2.1 Proper extensions of PA. We are interested in *proper* extensions T of PA which prove all induction axioms of T, i.e. $T \vdash I_x\phi[x]$ for all fromulas ϕ of $\mathcal{L}_T$.

Clearly, the basic theory PA is proper. The following theorem asserts that extensions by definitions yield proper theories from proper ones.

7.2.2 Theorem. *If S is an extension by definitions of a proper extension T of PA then also S is proper.*

Proof. Take the induction axiom $I_x\phi[x]$:

$$\phi[0] \land \forall x(\phi[x] \to \phi[x']) \to \phi[x]$$

for an arbitrary formula ϕ of $\mathcal{L}_S$. We use the Theorem on Extensions by definitions 6.6.2 and translate away the predicate or function symbols introduced into S. The translation $(I_x\phi[x])^\star$ of $I_x\phi[x]$ is the following formula of $\mathcal{L}_T$:

$$\phi^\star[0] \land \forall x(\phi^\star[x] \to \phi^\star[x']) \to \phi^\star[x] \ .$$

We thus have $(I_x\phi[x])^\star \equiv I_x\phi^\star[x]$ and, since ϕ^* is a formula of the proper extension T, we have $T \vdash (I_x\phi[x])^\star$. Hence $S \vdash I_x\phi[x]$ by 6.6.2(2). $\square$

7.2.3 Peano arithmetic in wider sense. In order to escape the irritating references to extensions of extensions of PA we will relativize our terminology. We will designate by PA not only the basic theory of Peano arithmetic, i.e. the six axioms for the function symbols of PA and infinitely many induction axioms, but also the current extension of Peano arithmetic. We will also designate by $\mathcal{L}_{\mathrm{PA}}$ the language of the current extension of PA. Thus both the language and the axioms of PA will be relative notions depending on the context where the symbols $\mathcal{L}_{\mathrm{PA}}$ and PA are used. It will be always possible to determine the meaning of both symbols.

Only in situations where we will be introducing new schemas of extension of PA such as minimalization (see Par. 7.4.3), primitive recursion (see Sect. 8.2), or course of values recursion with measure (see Sect. 8.4) we will temporary revert to designating the extensions of PA by symbols T, S, etc.

We will also have to be specific about concrete extensions of PA when we will be introducing new induction schemas such as complete induction (see Thm. 7.3.8), the least number principle (see Par. 7.3.10), or measure induction (see Par. 8.4.5). The new induction schemas will be reduced to the induction axioms $I_x\phi$ of PA. All extensions of PA in this text will be extensions by definitions, which are proper extensions. As a consequence, the new induction principles will be always provable in the extensions.

We will also use the expression *standard model* of PA in the relativized sense to designate the unique expansion of the standard model $\mathcal{N}$ of PA to the model of the current extension of PA. The uniqueness of expansion is guaranteed by Thm. 6.6.2.

We will be using the symbol of provability $\vDash_{\mathrm{PA}} \phi$ in the relativized sense as $T \vdash \phi$ where T is the current extension of PA. We will also use the symbol $\vDash_{\mathrm{PAx}} \phi$ with the meaning of $\vDash_{\mathrm{PA}} \phi$ when we will wish to emphasize that the formula ϕ is the defining axiom of the new extension of PA.

7.3 Introduction of Basic Predicates into PA

We define in PA the four relations of comparison and prove their basic properties.

7.3.1 Comparison predicates. We introduce into PA the binary *comparison* predicates $<$, $\leq$, $>$, and $\geq$ by explicit definitions:

$$\vdash_{\mathrm{PAx}} x < y \leftrightarrow \exists z\, x + z' = y \tag{1}$$
$$\vdash_{\mathrm{PAx}} x \leq y \leftrightarrow x < y \lor x = y \tag{2}$$
$$\vdash_{\mathrm{PAx}} x > y \leftrightarrow y < x \tag{3}$$
$$\vdash_{\mathrm{PAx}} x \geq y \leftrightarrow y \leq x \ . \tag{4}$$

The relation $\leq$ has the following property:

$$\vdash_{\mathrm{PA}} x \leq y \leftrightarrow \exists z\, x + z = y \ . \tag{5}$$

Indeed, in the direction ($\rightarrow$) assume $x \leq y$ and consider two cases by the definition (2). If $x < y$ then we have $x + z' = y$ from the definition and so $\exists z\, x + z = y$ holds. If $x = y$ then we have $x + 0 = y$ and $\exists z\, x + z = y$ holds again.

In the direction ($\leftarrow$) assume $x + z = y$ for some z and consider two cases for z. If $z = 0$ we have $x = x + 0 = y$. If $z = z_1'$ for some z_1 then we have $x + z_1' = y$ and so $x < y$ holds from the definition. In either case we have $x \leq y$ from the definition.

7.3.2 The relation $<$ is a linear order. The relation $<$ (and also $>$) is a linear order because we have

$$\vdash_{\mathrm{PA}} \neg x < x \tag{1}$$
$$\vdash_{\mathrm{PA}} x < y \land y < z \rightarrow x < z \tag{2}$$
$$\vdash_{\mathrm{PA}} x < y \lor x = y \lor y < x \ . \tag{3}$$

The properties are called in that order *irreflexivity*, *transitivity*, and *linearity*.

Irreflexivity is proved by induction on x. In the base case we have: $0 + z' = (0+z)' \neq 0$ and so $\neg\exists z\, 0 + z' = 0$ from which we get $\neg 0 < 0$ from definition. In the inductive case we derive a contradiction by assuming $x' < x'$ as follows. We have $x' + z' = x'$ for some z from the definition and from $(x + z')' = x' + z' = x'$ we obtain $x + z' = x$ from which we get $x < x$ contradicting IH.

Transitivity is proved by assuming $x < y$ and $y < z$ from which we get $x + a' = y$ and $y + b' = z$ for some a and b from the definitions. Hence, $x + (a + b')' = x + a' + b' = y + b' = z$, i.e. $\exists c\, x + c' = z$ and so we have $x < z$.

For the linearity we need an auxiliary property

$$\vdash_{\mathrm{PA}} 0 < x' \tag{4}$$

which follows from $0 + x' = x'$ by existential instantiation and the definition.

Linearity is proved by induction on x. In the base case we wish to prove $0 < y \lor 0 = y \lor y < 0$ for which we consider two cases. If $y = 0$ the property holds trivially. If $y = y_1'$ for some y_1 then we have $0 \overset{(4)}{<} y_1' = y$. In the inductive case we wish to prove $x' < y \lor x' = y \lor y < x'$. From the inductive hypothesis (3) we consider three cases. If $x < y$ then we have $x' + z = x + z' = y$ for some z from the definition and so $x' \le y$ by 7.3.1(5). From this we get $x' < y$ or $x' = y$ from the definition.

If $x = y$ we have $y + 0' = x + 0' = x' + 0 = x'$ and so $y < x'$ from the definition.

Finally, if $y < x$ we have $y + z' = x$ for some z from the definition and so $y + z'' = (y + z')' = x'$ from which we get $y < x'$ from the definition.

7.3.3 Trichotomy and dichotomy laws. The laws of trichotomy and dichotomy are in that order the following formulas:

$$\vdash_{\mathrm{PA}} x < y \lor x = y \lor x > y \tag{1}$$

$$\vdash_{\mathrm{PA}} x \le y \lor x > y \ . \tag{2}$$

The laws are typically used for case analysis and they directly follow from the linearity 7.3.2(3) of $<$ by the definitions.

7.3.4 Ordering properties of relation $\le$. The predicate $\le$ constitutes a (total) *ordering relation* which is reflexive, transitive, *antisymmetric*, and linear. This is expressed in that order as follows:

$$\vdash_{\mathrm{PA}} x \le x \tag{1}$$

$$\vdash_{\mathrm{PA}} x \le y \land y \le z \to x \le z \tag{2}$$

$$\vdash_{\mathrm{PA}} x \le y \land y \le x \to x = y \tag{3}$$

$$\vdash_{\mathrm{PA}} x \le y \lor y \le y \ . \tag{4}$$

Property (1) follows directly from the definition. Property (2) follows from the transitivity of $<$.

(3): If $x \le y$, $y \le x$, and $x \ne y$ hold then we obtain $x < y$ and $y < x$ from the definitions. From this we get $x < x$ by transitivity which contradicts the irreflexivity of $<$.

Property (4) is a direct consequence of linearity 7.3.2(3) of $<$.

7.3.5 Additional properties of comparisons. We have the following additional properties of the comparison relations:

$$\vdash_{\mathrm{PA}} x \not< 0 \tag{1}$$

$$\vdash_{\mathrm{PA}} 0 \le x \tag{2}$$

$$\vdash_{\mathrm{PA}} x < x' \tag{3}$$

$$\vdash_{\mathrm{PA}} x < y \leftrightarrow x' \le y \ . \tag{4}$$

(1) Assume on the contrary $x < 0$. We then have $x + z' = 0$ for some z from the definition and we get the contradiction $z' = 0$ by 7.1.7(1).

(2) is a direct consequence of (1) and 7.3.3(2).

(3): We have $x + 0' = (x + 0)' = x'$ and so $\exists z\, x + z = x'$ holds. We now get $x < x'$ from the definition.

For (4) we have $x < y$ iff $x + z' = y$ for some z iff $x' + z = y$ for some z iff $x' \leq y$ by 7.3.1(5).

7.3.6 Monotonicity of addition and multiplication. Addition and multiplication are monotone:

$$\vdash_{\mathrm{PA}} x < y \leftrightarrow z + x < z + y \tag{1}$$

$$\vdash_{\mathrm{PA}} x < y \leftrightarrow x + z < y + z \tag{2}$$

$$\vdash_{\mathrm{PA}} z > 0 \rightarrow x < y \leftrightarrow z{\cdot}x < z{\cdot}y \tag{3}$$

$$\vdash_{\mathrm{PA}} z > 0 \rightarrow x < y \leftrightarrow x{\cdot}z < y{\cdot}z\ . \tag{4}$$

(1): We have $x < y$ iff $x + u' = y$ for some u iff, by 7.1.10(1) and properties of identity, $z + (x + u') = z + y$ for some u iff $(z + x) + u' = z + y$ for some u iff $z + x < z + y$.

Property (2) follows from (1) by commutativity of addition.

(3): In the direction ($\rightarrow$) assume $z = z_1'$ and $x + u' = y$ for some z_1 and u. We have

$$z_1'{\cdot}y = z_1'{\cdot}(x + u') = z_1'{\cdot}x + z_1'{\cdot}u' = z_1'{\cdot}x + (z_1{\cdot}u' + u') = z_1'{\cdot}x + (z_1{\cdot}u' + u)'$$

and so $z_1'{\cdot}x < z_1'{\cdot}y$ holds by definition.

In the direction ($\leftarrow$) assume $z = z_1'$ and prove

$$\forall y(z_1'{\cdot}x < z_1'{\cdot}y \rightarrow x < y)$$

by induction on x. In the base case take any y and assume $z_1'{\cdot}0 < z_1'{\cdot}y$. We then have $0 < z_1'{\cdot}y$. If it were the case that $y = 0$ we would get a contradiction $0 < z_1'{\cdot}0 = 0$ with 7.3.2(1). Hence $y = y_1'$ for some y_1 and we have $0 < y$ by 7.3.2(4).

In the inductive case take any y and assume $z_1'{\cdot}x' < z_1'{\cdot}y$. If it were the case that $y = 0$ we would get a contradiction $z_1'{\cdot}x' < z_1'{\cdot}0 = 0$ with 7.3.5(1). Hence $y = y_1'$ for some y_1 and we have

$$x{\cdot}z_1' + z_1' = x'{\cdot}z_1' = z_1'{\cdot}x' < z_1'{\cdot}y_1' = y_1'{\cdot}z_1' = y_1{\cdot}z_1' + z_1'\ .$$

We now obtain $x{\cdot}z_1' < y_1{\cdot}z_1'$ by (2) and $x < y_1$ by IH. Hence $x' = x + 1 \overset{(2)}{<} y_1 + 1 = y_1'$.

Property (4) follows from (3) by the commutativity of multiplication.

7.3.7 Complete induction. Let T be a proper extension of PA containing the predicate $<$, $\phi[x]$ a formula of $\mathcal{L}_T$ with the indicated variable x free and with possibly additional parameters, and y a new variable. The formula of *complete induction on x for $\phi[x]$* is the following one:

$$\forall x(\forall y(y < x \to \phi[y]) \to \phi[x]) \to \phi[x] \ . \qquad (1)$$

7.3.8 Theorem. *Every proper extension T of PA containing the predicate $<$ proves the schema of complete induction 7.3.7(1).*

Proof. We prove 7.3.7(1) in T from an auxiliary property

$$T \vdash \forall x(\forall y(y < x \to \phi[y]) \to \phi[x]) \to \forall y(y < x \to \phi[y])$$

which is proved by assuming the formula expressing that ϕ *is progressive*:

$$\forall x(\forall y(y < x \to \phi[y]) \to \phi[x]) \qquad (1)$$

and proving

$$\forall y(y < x \to \phi[y]) \qquad (2)$$

by induction on x. In the base case there is nothing to prove. In the inductive case we take any y s.t. $y < x'$ and consider two cases by dichotomy. If $y < x$ we obtain $\phi[y]$ from IH: (2). If $y \geq x$ then we have $y = x$ and note that IH, i.e. (2), is the antecedent of (1) from which we obtain $\phi[x]$, i.e. $\phi[y]$.

We obtain $T \vdash$ 7.3.7(1) from the auxiliary property by instantiating its consequent with $x := x'$ and $y := x$. □

7.3.9 The least number principle. Let T be a proper extension of PA containing the predicate $<$, $\phi[x]$ a formula of $\mathcal{L}_T$ with the indicated variable x free and with possibly additional parameters, and y a new variable. The formula of the *least number principle for ϕ* is the following one:

$$\exists x \phi[x] \to \exists x(\phi[x] \land \forall y(y < x \to \neg\phi[y])) \ . \qquad (1)$$

The least number principle says that if the property $\phi[x]$ holds for some x then it holds for the least such x.

7.3.10 Theorem. *Every proper extension T of PA containing the predicate $<$ proves the schema of the least number principle 7.3.9(1).*

Proof. We prove 7.3.9(1) in T from the complete induction for $\neg\phi$:

$$T \vdash \forall x(\forall y(y < x \to \neg\phi[y]) \to \neg\phi[x]) \to \neg\phi[x]$$

which is a theorem of T by Thm. 7.3.8. Its converse is

$$\phi[x] \to \exists x(\forall y(y < x \to \neg\phi[y]) \land \phi[x])$$

and 7.3.9(1) logically follows by quantifier operations. □

7.4 Introduction of Basic Functions into PA

We will extend PA by some basic functions such as division, introduce extensions by minimalization, and prove that they are extensions by definition.

7.4.1 Small constants. We have used 1 as abbreviation for the term $0'$ in Sect. 7.1. We now introduce the symbols 1, 2, 3, and 4 into PA as constants by explicit definitions:

$$\models_{\text{PA}} 1 = 0' \tag{1}$$
$$\models_{\text{PA}} 2 = 1' \tag{2}$$
$$\models_{\text{PA}} 3 = 2' \tag{3}$$
$$\models_{\text{PA}} 4 = 3' \;. \tag{4}$$

7.4.2 Extensions by minimalization. Let T be a proper extension of PA containing the predicate $<$ and $\phi[\vec{x}, y]$ a formula of $\mathcal{L}_T$ with all free variables among the indicated ones where $\vec{x}$ contains $n \geq 0$ variables. If T proves the existence condition:

$$T \vdash \exists y \phi[\vec{x}, y] \tag{1}$$

then the extension of T to S with the n-ary function symbol f and the defining axiom a universal closure of

$$\phi[\vec{x}, f(\vec{x})] \land \forall y(y < f(\vec{x}) \to \neg\phi[\vec{x}, y]) \;. \tag{2}$$

is called *extension by minimalization*.

We will use a more suggestive notation as an abbreviation for the above defining axiom:

$$f(\vec{x}) = \mu_y[\phi[\vec{x}, y]] \;. \tag{3}$$

The idea is that the function f defined by this definition yields for every $\vec{x}$ the minimal y such that $\phi[\vec{x}, y]$ holds because on accord of the existence condition $\exists y \phi[\vec{x}, y]$ there is at least one such y.

The defining axiom clearly implies $S \vdash \phi[\vec{x}, f(\vec{x})]$ and

$$S \vdash y < f(\vec{x}) \to \neg\phi[\vec{x}, y] \;,$$

which is equivalent to

$$S \vdash \phi[\vec{x}, y] \to f(\vec{x}) \leq y$$

whenever T contains the predicate $\leq$.

7.4.3 Theorem. *If T is a proper extension of PA containing the predicate $<$ then an extension of T by minimalization is an extension by definition.*

Proof. Let S be the extension of T by minimalization as in Par. 7.4.2 and S_1 an extension of T with f implicitly defined by $\psi[\vec{x}, f(\vec{x})]$ for the formula

$$\psi[\vec{x}, y] \equiv \phi[\vec{x}, y] \wedge \forall z(z < y \to \neg\phi[\vec{x}, z]) \ .$$

Since $\psi[\vec{x}, f(\vec{x})]$ and 7.4.2(2) are variants, S will be an extension by definition of T by Thm. 6.6.3 provided T proves the existence and uniqueness conditions for ψ. We note that the existence condition $\exists y \psi[\vec{x}, y]$ is the consequent of the instance of the least number principle

$$T \vdash \exists y \phi[\vec{x}, y] \to \exists y(\phi[\vec{x}, y] \wedge \forall z(z < y \to \neg\phi[\vec{x}, z])) \ ,$$

which is provable in T by Thm. 7.3.10. We thus get $\exists y \psi[\vec{x}, y]$ in T from 7.4.2(1).

For the proof of the uniqueness condition we work in T, assume $\psi[\vec{x}, y_1]$, $\psi[\vec{x}, y_2]$, and consider three cases. If $y_1 < y_2$ then we obtain $\neg\phi[\vec{x}, y_1]$ from $\psi[\vec{x}, y_2]$ which contradicts $\phi[\vec{x}, y_1]$ implied by $\psi[\vec{x}, y_1]$. If $y_1 > y_2$ we derive a contradiction similarly. Thus it must be the case that $y_1 = y_2$. □

7.4.4 Modified subtraction. We wish to extend Peano arithmetic with a binary *modified subtraction* function $x \dot{-} y$ with the basic properties

$$\vdash_{\mathrm{PA}} y \le x \to x = y + (x \dot{-} y) \ . \tag{1}$$

$$\vdash_{\mathrm{PA}} y > x \to x \dot{-} y = 0 \ . \tag{2}$$

The modified subtraction function is introduced by minimalization

$$\vdash_{\mathrm{PA}_\times} x \dot{-} y = \mu_z[y \le x \to x = y + z] \tag{3}$$

with the existence condition

$$\vdash_{\mathrm{PA}} \exists z(y \le x \to x = y + z) \ ,$$

which is equivalent to $y \le x \to \exists z\, x = y + z$, holding by 7.3.1(5).

The defining axiom for $\dot{-}$ directly implies Property (1) and

$$\vdash_{\mathrm{PA}} z < x \dot{-} y \to \neg(y \le x \to x = y + z) \ . \tag{4}$$

From this we obtain $0 < x \dot{-} y \to y \le x$, which is equivalent to (2) by dichotomy and 7.3.5(1).

7.4.5 Maximum. The *maximum* function $\max(x, y)$ with the basic properties

$$\vdash_{\mathrm{PA}} x \leq \max(x,y) \tag{1}$$
$$\vdash_{\mathrm{PA}} y \leq \max(x,y) \tag{2}$$
$$\vdash_{\mathrm{PA}} x = \max(x,y) \lor y = \max(x,y) \tag{3}$$

is introduced into PA by minimalization

$$\vdash_{\mathrm{PAx}} \max(x,y) = \mu_z[x \leq z \land y \leq z] \tag{4}$$

whose existence condition

$$\vdash_{\mathrm{PA}} \exists z(x \leq z \land y \leq z)$$

is proved by case analysis. If $x \leq y$ then we take $z := y$. If $x > y$ then we take $z := x$.

The defining axiom for the maximum function directly implies Properties (1) and (2) as well as

$$\vdash_{\mathrm{PA}} x \leq z \land y \leq z \to \max(x,y) \leq z \ .$$

Property (3) is proved from the last by case analysis. If $x \leq y$ then for $z := y$ we get $\max(x,y) \leq y$ and we obtain $\max(x,y) = y$ from (2) by antisymmetry. If $x > y$ then for $z := x$ we get $\max(x,y) \leq x$ and we obtain $\max(x,y) \leq y$ similarly.

7.4.6 The square function. We introduce the unary function x^2 yielding the square of x into PA by explicit definition:

$$\vdash_{\mathrm{PAx}} x^2 = x{\cdot}x \ . \tag{1}$$

7.4.7 Whole part of square root. We wish to introduce into PA the function $[\sqrt{x}]$ yielding the whole part of the square root of x which satisfies

$$\vdash_{\mathrm{PA}} [\sqrt{x}]^2 \leq x < ([\sqrt{x}]+1)^2 \ . \tag{1}$$

The function is defined by minimalization:

$$\vdash_{\mathrm{PAx}} [\sqrt{x}] = \mu_y[x < (y+1)^2] \tag{2}$$

whose existence condition

$$\vdash_{\mathrm{PA}} \exists y\, x < (y+1)^2$$

holds for $y := x$ because

$$x = x{\cdot}1 \leq x{\cdot}(x+1) < (x+1){\cdot}(x+1) = (x+1)^2 \ .$$

The defining axiom for $[\sqrt{x}]$ implies

$$\vdash_{\mathrm{PA}} x < ([\sqrt{x}]+1)^2 \tag{3}$$
$$\vdash_{\mathrm{PA}} y < [\sqrt{x}] \to (y+1)^2 \le x\ . \tag{4}$$

From (3) we can see that for the proof of (1) it suffices to show $[\sqrt{x}]^2 \le x$. For that we consider two cases. If $[\sqrt{x}] = 0$ then we have $0^2 = 0 \le x$. If $[\sqrt{x}] = y'$ for some y then, since $y < [\sqrt{x}]$, we obtain $[\sqrt{x}]^2 = (y+1)^2 \le x$ from (4).

7.4.8 Integer division and remainder. We wish to introduce into PA *integer division* $x \div y$ and *remainder* $x \bmod y$ functions satisfying the following

$$\vdash_{\mathrm{PA}} y > 0 \to x = x \div y \cdot y + x \bmod y \land x \bmod y < y \tag{1}$$
$$\vdash_{\mathrm{PA}} y > 0 \land x = q \cdot y + r \land r < y \to q = x \div y \land r = x \bmod y \tag{2}$$
$$\vdash_{\mathrm{PA}} x \div 0 = 0 \tag{3}$$
$$\vdash_{\mathrm{PA}} x \bmod 0 = 0\ . \tag{4}$$

We claim that the functions can be introduced by minimalization:

$$\vdash_{\mathrm{PA}\times} x \div y = \mu_q[y > 0 \to x < (q+1) \cdot y] \tag{5}$$
$$\vdash_{\mathrm{PA}\times} x \bmod y = \mu_z[y > 0 \to z = x \dot{-} x \div y \cdot y] \tag{6}$$

The existence condition for the division function (5) is

$$\vdash_{\mathrm{PA}} \exists q (0 < y \to x < (q+1) \cdot y)\ .$$

This holds because if $y = 0$ then set $q := 0$ and if $y > 0$ then set $q := x$ because we have

$$x = x \cdot 1 \le x \cdot y < (x+1) \cdot y\ .$$

The defining axiom for $\div$ implies:

$$\vdash_{\mathrm{PA}} y > 0 \to x < (x \div y + 1) \cdot y \tag{7}$$
$$\vdash_{\mathrm{PA}} q < x \div y \to (q+1) \cdot y \le x \tag{8}$$
$$\vdash_{\mathrm{PA}} y = 0 \to x \div y \le q \tag{9}$$

The existence condition for the remainder function (6) is equivalent to $\vdash_{\mathrm{PA}} y > 0 \to \exists z\, z = x \dot{-} x \div y \cdot y$ and it is proved trivially. The defining axiom for mod implies

$$\vdash_{\mathrm{PA}} y > 0 \to x \bmod y = x \dot{-} x \div y \cdot y \tag{10}$$
$$\vdash_{\mathrm{PA}} z = x \dot{-} x \div y \cdot y \to x \bmod y \le z \tag{11}$$
$$\vdash_{\mathrm{PA}} y = 0 \to x \bmod y \le z\ . \tag{12}$$

For the proof of Property (1) we assume $y > 0$ and prove an auxiliary property

$$\vdash_{\mathrm{PA}} x \div y \cdot y \leq x \tag{13}$$

by considering two cases. If $x \div y = 0$ then we have

$$x \div y \cdot y = 0 \cdot y = 0 \leq x \; .$$

If $x \div y = q'$ for some q then, since $q < x \div y$, we obtain

$$x \div y \cdot y = (q+1) \cdot y \overset{(8)}{\leq} x \; .$$

We then have

$$x \div y \cdot y + x \bmod y \overset{(10)}{=} x \div y \cdot y + (x \dot{-} x \div y \cdot y) \overset{(13),7.4.4(1)}{=} x \overset{(7)}{<} (x \div y + 1) \cdot y = x \div y \cdot y + y \; .$$

Note that $x \bmod y < y$ holds by 7.3.6(1).

Property (2) is proved by assuming $y > 0$, $x = q \cdot y + r$ with $r < y$, and considering three cases by trichotomy. If $x \div y < q$ then we have $q = x \div y + z'$ for some z. We then obtain

$$x \div y \cdot y + x \bmod y \overset{(1)}{=} x = q \cdot y + r = x \div y \cdot y + z' \cdot y + r$$

and hence $x \bmod y = z' \cdot y + r$ by 7.3.6(1). Thus $x \bmod y = y + z \cdot y + r$ from which we have $x \bmod y \geq y$ which contradicts $x \bmod y < y$.

If $q < x \div y$ then we have $x \div y = q + z'$ for some z. We then similarly obtain

$$q \cdot y + r = x \overset{(1)}{=} x \div y \cdot y + x \bmod y = q \cdot y + z' \cdot y + x \bmod y$$

from which we get $r = z' \cdot y + x \bmod y = y + z \cdot y + x \bmod y$ and thus $r \geq y$ which contradicts $r < y$.

Thus the third case $x \div y = q$ must obtain and, since then

$$q \cdot y + r = x \overset{(1)}{=} x \div y \cdot y + x \bmod y = q \cdot y + x \bmod y \; ,$$

we get $r = x \bmod y$ by 7.3.6(1).

(3): Take $y := 0$ and $q := 0$ in (9) and obtain $x \div 0 \leq 0$, i.e. $x \div 0 = 0$.

(4): Take $y := 0$ and $z := 0$ in (12) and obtain $x \bmod 0 \leq 0$, i.e. $x \bmod 0 = 0$.

7.5 The Lattice of Divisibility

7.5.1 Divisibility predicate. The binary *divisibility* predicate $x \mid y$, read as x *divides* y is defined in PA by an explicit definition:

$$\vdash_{\mathrm{PAx}} x \mid y \leftrightarrow \exists z\, y = z{\cdot}x \ . \tag{1}$$

The predicate of divisibility is a relation of *partial order* (similar to $\leq$ but without the linearity 7.3.4(4)) which satisfies the reflexivity, transitivity, and antisymmetry. The partial order is with the least element 1 and the greatest element 0:

$$\vdash_{\mathrm{PA}} x \mid x \tag{2}$$
$$\vdash_{\mathrm{PA}} x \mid y \land y \mid z \to x \mid z \tag{3}$$
$$\vdash_{\mathrm{PA}} x \mid y \land y \mid x \to x = y \tag{4}$$
$$\vdash_{\mathrm{PA}} 1 \mid x \tag{5}$$
$$\vdash_{\mathrm{PA}} x \mid 0 \ . \tag{6}$$

(2): We have $x = 0 + x = 0{\cdot}x + x = 0'{\cdot}x$ and so $\exists z\, x = z{\cdot}x$.

(3): Assume $x \mid y$ and $y \mid z$, i.e. $y = a{\cdot}x$ and $z = b{\cdot}y$ for some a and b. Then $z = b{\cdot}y = b{\cdot}a{\cdot}x$ and so for $u := b{\cdot}a$ we have $\exists u\, z = u{\cdot}x$.

(4): Assume $x \mid y$ and $y \mid x$, i.e. $y = a{\cdot}x$ and $x = b{\cdot}y$ for some a and b. Then $x = b{\cdot}y = b{\cdot}a{\cdot}x$. We consider two cases. If $x = 0$ then also $y = a{\cdot}0 = 0$. If $x > 0$ then, since $x = b{\cdot}a{\cdot}x + 0$ and $x = 1{\cdot}x + 0$, we obtain $b{\cdot}a = x \div x = 1$ by 7.4.8(2). But then $a = 1$ and $b = 1$ by 7.1.12(1) and so $x = y$.

(5): We have $x = x{\cdot}1$ and so $\exists z\, x = z{\cdot}1$.

(6): We have $0 = 0{\cdot}x$ and so $\exists z\, 0 = z{\cdot}x$.

7.5.2 Additional properties of divisibility. The relation between the divisibility predicate and the remainder function is given by the following property:

$$\vdash_{\mathrm{PA}} y \neq 0 \to y \mid x \leftrightarrow x \bmod y = 0 \ . \tag{1}$$

Indeed, assume $y > 0$. In the direction ($\to$) also assume $y \mid x$, i.e. $x = z{\cdot}y = z{\cdot}y + 0$ for some z. We get $x \bmod y = 0$ by 7.4.8(2). In the direction ($\leftarrow$) also assume $x \bmod y = 0$. We then have

$$x \overset{7.4.8(1)}{=} x \div y{\cdot}y + x \bmod y = x \div y{\cdot}y$$

and for $z := x \div y$ we have $\exists z\, x = z{\cdot}y$. We also have

$$\vdash_{\mathrm{PA}} x \neq 0 \land y \mid x \to y \leq x \tag{2}$$

because if $x > 0$ and $x = z{\cdot}y$ for some z then it must be the case that $z > 0$. If it were the case that $x < y$ then we would have $z{\cdot}x < z{\cdot}y = x = 1{\cdot}x$ and hence $z < 1$ by the monotonicity of multiplication.

We will need the following property:

$$\vdash_{\mathrm{PA}} a + b = c \land x \mid a \land x \mid c \to x \mid b \tag{3}$$

which is proved by assuming its antecedent and considering two cases. If $x = 0$ then from $x \mid a$ and $x \mid c$ we get $a = b = 0$ and hence $b = 0$ from which we have $x \mid b$ by 7.5.1(6).

If $x > 0$ then for some a_1 and c_1 we have $a_1 \cdot x = a \leq c = c_1 \cdot x$ and so $a_1 \leq c_1$, i.e. $a_1 + u = c_1$ for some u. We then get

$$a + u \cdot x = a_1 \cdot x + u \cdot x = (a_1 + u) \cdot x = c_1 \cdot x = c\ .$$

Thus $b = u \cdot x$, i.e. $x \mid b$.

7.5.3 The lattice of divisibility. A set with a partial order where for every two elements x and y exists their least upper bound $x \cup y$ (called the *join* of x and y) and their greatest lower bound $x \cap y$ (called the *meet* of x and y) is a *lattice*. The partial order on natural numbers given by the relation of divisibility $x \mid y$ forms a lattice where the join $x \cup y$ is the *least common multiple of x and y* and the meet $x \cap y$ is the *greatest common divisor of x and y*. We wish to introduce the operations into PA to satisfy:

$$\vdash_{\mathrm{PA}} x \mid x \cup y \land y \mid x \cup y \tag{1}$$

$$\vdash_{\mathrm{PA}} x \mid z \land y \mid z \to x \cup y \mid z \tag{2}$$

$$\vdash_{\mathrm{PA}} x \cap y \mid x \land x \cap y \mid y \tag{3}$$

$$\vdash_{\mathrm{PA}} z \mid x \land z \mid y \to z \mid x \cap y\ . \tag{4}$$

We claim that the least common multiple $x \cup y$ can be introduced by minimalization:

$$\vdash_{\mathrm{PAx}} x \cup y = \mu_z[x = 0 \lor y = 0 \lor z > 0 \land x \mid z \land y \mid z] \tag{5}$$

whose existence condition

$$\vdash_{\mathrm{PA}} \exists z(x = 0 \lor y = 0 \lor z > 0 \land x \mid z \land y \mid z)$$

is proved by taking any x, y and considering two cases. If $x = 0$ or $y = 0$ then it suffices to take $z := 0$. If $x > 0$ and $y > 0$ then also $x \cdot y > 0$ and, since $x \mid x \cdot y$ and $y \mid x \cdot y$, it suffices to take $z := x \cdot y$. The defining axiom for $\cup$ implies

$$\vdash_{\mathrm{PA}} x > 0 \land y > 0 \to x \cup y > 0 \land x \mid x \cup y \land y \mid x \cup y \tag{6}$$

$$\vdash_{\mathrm{PA}} x = 0 \lor y = 0 \to x \cup y \leq z \tag{7}$$

$$\vdash_{\mathrm{PA}} z > 0 \land x \mid z \land y \mid z \to x \cup y \leq z\ . \tag{8}$$

We prove (1) by taking any x, y and considering two cases. If $x = 0$ or $y = 0$ then we have $x \cup y = 0$ from (7) by taking $z := 0$ and the property holds on account of 7.5.1(6). If $x > 0$ and $y > 0$ then (1) follows from (6).

We prove (2) by taking any x, y and considering two cases. If $x = 0$ or $y = 0$ then if $x \mid z$ and $y \mid z$ we obtain $z = 0$ and thus $x \cup y \mid z$ by 7.5.1(6).

If $x > 0$ and $y > 0$ then we prove (2) by complete induction on z. Assume $x \mid z$, $y \mid z$ and consider two cases. If $z = 0$ then also $x \cup y \mid z$ by 7.5.1(6). If $z > 0$ then we have

$$0 \overset{(6)}{<} x \cup y \overset{(8)}{\leq} z$$

and so $(x \cup y) + u = z$ for some u. Since $x \mid x \cup y$, we obtain $x \mid u$ by 7.5.2(3). We get $y \mid u$ similarly and, since $u < z$, we obtain $x \cup y \mid u$ by IH, i.e $u = a \cdot (x \cup y)$ for some a. From this, since

$$z = (x \cup y) + u = (x \cup y) + a \cdot (x \cup y) = (1 + a) \cdot (x \cup y) \ ,$$

we get $x \cup y \mid z$.

We claim that the greatest common divisor $x \cap y$ can be introduced by minimalization:

$$\vdash_{\mathrm{PAx}} x \cap y = \mu_z[z \mid x \land z \mid y \land \forall u(u \mid x \land u \mid y \to u \mid z)] \tag{9}$$

whose existence condition is implied by

$$\vdash_{\mathrm{PA}} \forall y \exists z(z \mid x \land z \mid y \land \forall u(u \mid x \land u \mid y \to u \mid z))$$

which is proved by complete induction on x. We take any y and consider two cases. If $x = 0$ then it clearly suffices to take $z := y$. If $x > 0$ then, since $x > y \bmod x$, we use IH with $y := x$ to obtain a z s.t. $z \mid y \bmod x$, $z \mid x$, and

$$\forall u(u \mid y \bmod x \land u \mid x \to u \mid z) \ . \tag{10}$$

We have $x = a \cdot z$ and $y \bmod x = b \cdot z$ for some a and b. We claim that

$$z \mid x \land z \mid y \land \forall u(u \mid x \land u \mid y \to u \mid z)$$

holds for the same z. For that we note

$$y \overset{7.4.8(1)}{=} y \div x \cdot x + y \bmod x = y \div x \cdot a \cdot z + b \cdot z = (y \div x \cdot a + b) \cdot z$$

and so $z \mid y$. Now take any u and assume $u \mid x$ and $u \mid y$. Since $y = y \div x \cdot x + y \bmod x$, we see that $u \mid y \bmod x$ by 7.5.2(3). We now get $u \mid z$ from (10).

Properties (3) and (4) are a direct consequence of the defining axiom for $x \cap y$.

7.5.4 Joins and meets versus the partial order. In every lattice we have $x \cup y = x$ iff $y \leq x$ iff $x \cap y = y$. This has the following form in the lattice of divisibility:

$$\vdash_{\mathrm{PA}} x \cup y = x \leftrightarrow y \mid x \tag{1}$$

$$\vdash_{\mathrm{PA}} x \cap y = y \leftrightarrow y \mid x \tag{2}$$

and the proof is solely by using the four properties 7.5.3(3) through 7.5.3(4) of $\cup$ and $\cap$ as well as the fact that $\mid$ is a partial order satisfying 7.5.1(2) through 7.5.1(4).

(1): In the direction ($\rightarrow$) assume $x \cup y = x$ and get $y \mid x \cup y = x$ from 7.5.3(1). In the direction ($\leftarrow$) assume $y \mid x$. Since $x \mid x$ by 7.5.1(2) we get $x \cup y \mid x$ by 7.5.3(2). We have $x \mid x \cup y$ by 7.5.3(1) and so $x \cup y = x$ by 7.5.1(4).

Property (2) is proved similarly.

7.5.5 The lattice of divisibility is atomic. An element p of a lattice is an *atom* if the only element strictly less than p is the least element of the lattice. The divisibility lattice has 1 as the least element and so the predicate $Prime(p)$ is explicitly introduced to hold exactly of its atoms:

$$\vdash_{\mathrm{PAx}} Prime(p) \leftrightarrow p \neq 1 \wedge \forall x(x \mid p \rightarrow x = 1 \vee x = p) \tag{1}$$

Thus p is an atom of the divisibility lattice iff it is a prime number. For $2 = 1' = 0''$ we have

$$\vdash_{\mathrm{PA}} \neg Prime(0) \tag{2}$$

$$\vdash_{\mathrm{PA}} Prime(2)\ . \tag{3}$$

(2): We have $2 \mid 0$ by 7.5.1(6) and $1 \neq 2 \neq 0$.

(3): We have $2 \neq 1$ and if $x \mid 2$ then $x \leq 2$ by 7.5.2(2). Since $0 \nmid 2$ we can have at most $1 \mid 2$ or $2 \mid 2$.

A lattice with the least element is *atomic* if to every non-minimal element x which is not an atom there is an atom p less than x. The divisibility lattice is atomic because we have:

$$\vdash_{\mathrm{PA}} x \neq 1 \rightarrow \exists p(Prime(p) \wedge p \mid x)\ . \tag{4}$$

This is proved by complete induction on x. We consider three cases for x. If $x = 0$ then it suffices to take $p := 2$ by (3) and 7.5.1(6). If $x = 1$ there is nothing to prove. Finally, if $x > 1$ then we consider two cases again. If $Prime(x)$ then it suffices to take $p := x$ because of 7.5.1(2). If $\neg Prime(x)$ then there is a number $q \mid x$ s.t. $x \neq 1$ and $q \neq x$ from the definition. We have $q \leq x$ by 7.5.2(2) and, since $q < x$, there is a prime p s.t. $p \mid q$ by IH for which we get $p \mid x$ by 7.5.1(3).

7.5.6 The lattice of divisibility is distributive. In every lattice we have $(x \cap y) \cup (x \cap z) \leq x \cap (y \cup z)$. We prove this and its dual for the lattice of divisibility solely from the seven properties given in Par. 7.5.4:

$$\vdash_{\mathrm{PA}} y \mid z \rightarrow x \cap y \mid x \cap z \tag{1}$$

$$\vdash_{\mathrm{PA}} (x \cap y) \cup (x \cap z) \mid x \cap (y \cup z)\ . \tag{2}$$

(1): Assume $y \mid z$. We have $x \cap y \mid x$ and $x \cap y \mid y$ and so $x \cap y \mid z$ by transitivity. Hence $x \cap y \mid x \cap z$ by 7.5.3(4).

(2): Since $y \mid y \cup z$ and $z \mid y \cup z$, we obtain $x \cap y \mid x \cap (y \cup z)$ and $x \cap z \mid x \cap (y \cup z)$ by (1). The property now follows by 7.5.3(2).

UNFINISHED

$$\vdash_{\mathrm{PA}} x \cap (y \cup z) = (x \cap y) \cup (x \cap z) \tag{3}$$

$$\vdash_{\mathrm{PA}} x \cup (y \cap z) = (x \cup y) \cap (x \cup z)\ . \tag{4}$$

7.5.7 A property of prime divisors. We will need Property (2) which is a simple consequence of distributivity of the lattice of divisibility.

$$\vdash_{\mathrm{PA}} x \cup x = x \tag{1}$$

$$\vdash_{\mathrm{PA}} Prime(p) \land p \mid x \cup y \to p \mid x \lor p \mid y\ . \tag{2}$$

(1): This follows from $x \mid x$ by 7.5.4(1).

(2): Assume that p is a prime s.t. $p \mid x \cup y$. If it were the case that $p \nmid x$ and $p \nmid y$ then we would get $p \cap x \neq p$, $p \cap y \neq p$ by 7.5.4(2). But $p \cap x \mid p$ and $p \cap y \mid p$ by 7.5.3(3) and so $p \cap x = 1 = p \cap y$ by the definition of primes. But then we could derive a contradiction:

$$p \overset{7.5.4(2)}{=} p \cap (x \cup y) \overset{7.5.6(3)}{=} (p \cap x) \cup (p \cap y) = 1 \cup 1 \overset{(1)}{=} 1$$

with the definition of primes.

7.5.8 Coprime numbers. Two numbers x and y are *coprime* (relatively prime) if $x \cap y = 1$. We will need the following property which says that every two successive numbers are coprime:

$$\vdash_{\mathrm{PA}} x \cap (x+1) = 1\ . \tag{1}$$

We claim that (1) follows from

$$\vdash_{\mathrm{PA}} z \mid x \land z \mid x+1 \to z = 1\ . \tag{2}$$

Indeed, take $z := x \cap x+1$ and use 7.5.3(3). For the proof of (2) assume $z \mid x$, $z \mid x+1$, and consider three cases. If $z = 0$ then, since $x + 1 = b{\cdot}z$ for some b, we obtain a contradiction $x + 1 = b{\cdot}z = 0$. If $z > 1$ then, since $x = a{\cdot}z$ for some a, we get $x + 1 = a{\cdot}z + 1$ and so $(x + 1) \bmod z = 1$ by 7.4.8(2). We now obtain contradiction $z \nmid x + 1$ by 7.5.2(1). Thus it must be the case that $z = 1$.

7.5.9 Least common multiple of interval $[1..x]$. We will need a function $\bigcup_{i=1}^{x} i$ yielding finitely many least common multiples of numbers in the (possibly empty) interval $[1..x]$. The function should satisfy:

$$\vdash_{\text{PA}} \bigcup_{i=1}^{0} i = 1 \tag{1}$$

$$\vdash_{\text{PA}} \bigcup_{i=1}^{x'} i = (\bigcup_{i=1}^{x} i) \cup x' \ . \tag{2}$$

We claim that the function can be defined by minimalization

$$\begin{aligned}\vdash_{\text{PAx}} \bigcup_{i=1}^{x} i = \mu_m[x = 0 \land m = 1 \lor \\ x \neq 0 \land \forall y(0 < y \leq x \to y \mid m) \land \\ \forall z(\forall y(0 < y \leq x \to y \mid z) \to m \mid z)]\end{aligned}$$

whose existence condition

$$\begin{aligned}&\vdash_{\text{PA}} \exists m(x = 0 \land m = 1 \lor \\ &\quad x > 0 \to \forall y(0 < y \leq x \to y \mid m) \land \forall z(\forall y(0 < y \leq x \to y \mid z) \to m \mid z))\end{aligned}$$

is proved by iduction on x. In the base case we take $m := 1$. In the inductive case we obtain an m_1 s.t.

$$\begin{aligned}&x = 0 \land m_1 = 1 \lor \\ &x \neq 0 \land \forall y(0 < y \land y \leq x \to y \mid m_1) \land \forall z(\forall y(0 < y \leq x \to y \mid z) \to m_1 \mid z)\end{aligned} \tag{3}$$

by IH. We claim that it suffices to take $m := m_1 \cup x'$. We consider two cases for x. If $x = 0$ then $m_1 = 1$ and $m = 1 \cup 1 \overset{7.5.7(1)}{=} 1$. We now take any y s.t. $0 < y \leq x' = 1$, i.e. $y = 1$, and we have $y \mid m$. We also have $m = 1 \mid z$ for any z.

If $x \neq 0$ then for any y s.t. $0 < y \leq x'$ we consider two cases agian. If $y < x'$ then $y \mid m_1$ by (3) and, since $m_1 \mid m$, we get $y \mid m$ by transitivity. If $y \geq x'$ then $y = x'$ and we have $y = x' \mid m$. If for any z we have $\forall y(0 < y \leq x' \to y \mid z)$ then we have $x' \mid z$ directly and $m_1 \mid z$ by (3). Hence $m = m_1 \cup x' \mid z$ by 7.5.3(2).

The defining axiom for $\bigcup_{i=1}^{x} i$ directly implies Property (1) and also

$$\vdash_{\text{PA}} 0 < y \leq x \to y \mid \bigcup_{i=1}^{x} i \tag{4}$$

$$\vdash_{\text{PA}} x \neq 0 \land \forall y(0 < y \leq x \to y \mid u) \to \bigcup_{i=1}^{x} i \mid u \ . \tag{5}$$

We prove Property (2) by showing first

$$\vdash_{\mathrm{PA}} \bigcup_{i=1}^{x'} i \mid (\bigcup_{i=1}^{x} i) \cup x' \tag{6}$$

by taking any y s.t. $0 < y \leq x'$ and considering two cases. If $y \leq x$ then $y \mid \bigcup_{i=1}^{x} i$ by (4) and, since $\bigcup_{i=1}^{x} i \mid (\bigcup_{i=1}^{x} i) \cup x'$, we obtain $y \mid (\bigcup_{i=1}^{x} i) \cup x'$ by transitivity. If $y = x'$ then we have $x' \mid (\bigcup_{i=1}^{x'} i) \cup x'$. (6) now follows by (5).

We then prove

$$\vdash_{\mathrm{PA}} (\bigcup_{i=1}^{x} i) \cup x' \mid \bigcup_{i=1}^{x'} i \tag{7}$$

by proving first $\bigcup_{i=1}^{x} i \mid \bigcup_{i=1}^{x'} i$ by considering two cases. If $x = 0$ then $\bigcup_{i=1}^{x} i \overset{(1)}{=} 1 \mid \bigcup_{i=1}^{x'} i$ by 7.5.1(5). If $x \neq 0$ we take any y s.t. $0 < y \leq x$. We have $y \mid \bigcup_{i=1}^{x'} i$ by (4) and hence $\bigcup_{i=1}^{x} i \mid \bigcup_{i=1}^{x'} i$ by (5). From $\bigcup_{i=1}^{x} i \mid \bigcup_{i=1}^{x'} i$ and from $x' \mid \bigcup_{i=1}^{x'} i$ which holds by (4) we get (7) by 7.5.3(2).

Property (2) now follows from (6) and (7) by antisymmetry.

Surprising as it is, we need a proof by induction on x of the following property:

$$\vdash_{\mathrm{PA}} \bigcup_{i=1}^{x} i \neq 0 \; . \tag{8}$$

In the base case the property follows from (1). In the inductive case we have $\bigcup_{i=1}^{x} i \neq 0$ by IH and

$$0 \overset{7.5.3(6)}{\neq} (\bigcup_{i=1}^{x} i) \cup x' \overset{(2)}{=} \bigcup_{i=1}^{x'} i \; .$$

We will need the following lower bound on our function:

$$\vdash_{\mathrm{PA}} x \leq \bigcup_{i=1}^{x} i \tag{9}$$

which is proved by considering two cases. If $x = 0$ then (9) holds by (1). If $x \neq 0$ then $x \mid \bigcup_{i=1}^{x} i$ by (4). Since $\bigcup_{i=1}^{x} i \neq 0$ by (8), the property follows from 7.5.2(2).

7.5.10 Euclid's theorem on prime numbers. The lattice of divisibility has infinitely many atoms by the famous second theorem of Euclid which asserts that there are infinitely many prime numbers:

$$\vdash_{\mathrm{PA}} \exists p(p > x \land \mathit{Prime}(p)) \tag{1}$$

This is proved by taking any x and considering the number $q = (\bigcup_{i=1}^{x} i) + 1$. For every $y > 1$ s.t. $y \leq x$ we have $y \mid \bigcup_{i=1}^{x} i$ by 7.5.9(4). If it were the case that $y \mid q$ then by 7.5.3(4) we would have a contradiction $y = 1$ by 7.5.8(2). We have just proved:

$$\forall y(y > 1 \land y \leq x \to y \nmid q) \tag{2}$$

Since $q \neq 1$ by 7.5.9(8) there is a prime p s.t. $p \mid q$ by 7.5.5(4). By (2) we have $p = 1$, $p = 0$, or $p > x$. But $p \neq 1$ by the definition of primes, $p \neq 0$ by 7.5.5(2), and so it must be the case that $p > x$.

8. Recursive Bootstrapping of PA

8.1 Exponentiation Function

8.1.1 Binary successors. We introduce two *binary successor* functions by explicit definitions:

$$\vdash_{\text{PAx}} x\mathbf{0} = 2{\cdot}x \tag{1}$$

$$\vdash_{\text{PAx}} x\mathbf{1} = 2{\cdot}x + 1\ . \tag{2}$$

Binary successors are interesting because of *binary discrimination*:

$$\vdash_{\text{PA}} \exists y(x = y\mathbf{0} \lor x = y\mathbf{1}) \tag{3}$$

which directly follows from $x = x \div 2{\cdot}2 + x \bmod 2$ with $x \bmod 2 < 2$ holding by 7.4.8(1).

8.1.2 The plan for the introduction of 2^x into PA. We wish to introduce into PA the *exponentiation* function 2^x satisfying the natural recurrences:

$$\vdash_{\text{PA}} 2^0 = 1 \tag{1}$$

$$\vdash_{\text{PA}} 2^{x'} = 2{\cdot}2^x\ . \tag{2}$$

We will not be able to express the computation of 2^x by these recurrences but we will succeed in encoding the computation of 2^x by the following exponentially faster recurrences by *recursion on binary notation*:

$$\begin{aligned} 2^0 &= 1 \\ 2^{x\mathbf{0}} &= (2^x)^2 \quad \text{if } x > 0 \\ 2^{x\mathbf{1}} &= 2{\cdot}(2^x)^2\ . \end{aligned}$$

We will do this by introducing in Par. 8.1.3 the predicate $Pow_2(p)$ of being a power of two satisfying

$$\vdash_{\text{PA}} Pow_2(p) \leftrightarrow \exists x\, 2^x = p$$

and with its help to define in Par. 8.1.10 the log function as the inverse of 2^x by encoding its computation from the following recurrences:

$$\begin{aligned} Pow_2(p) \wedge p = 1 &\rightarrow \log(p) = 0 \\ Pow_2(p) \wedge p = q^2 \wedge p > 1 &\rightarrow \log(p) = \log(q)\mathbf{0} \\ Pow_2(p) \wedge p = 2{\cdot}q^2 &\rightarrow \log(p) = \log(q)\mathbf{1} \ . \end{aligned}$$

That the recurrences cover all cases for p and that they are exclusive will be proved in Par. 8.1.5.

Only then we will be able to introduce in Par. 8.1.11 the exponentiation function satisfying

$$\vdash_{\mathrm{PA}} 2^x = p \leftrightarrow Pow_2(p) \wedge \log(p) = x \ .$$

8.1.3 The predicate of being a power of two. The predicate $Pow_2(p)$ of p *being a power of two*, i.e. such that $\exists x\, 2^x = p$, can be presented in a clausal form with binary recurrences:

$$\begin{aligned} &Pow_2(x\mathbf{0}) \leftarrow x > 0 \wedge Pow_2(x) \\ &Pow_2(x\mathbf{1}) \leftarrow x = 1 \ . \end{aligned}$$

We claim that we can introduce into PA the predicate Pow_2 to satisfy the clauses properties by the following explicit definition:

$$\vdash_{\mathrm{PAx}} Pow_2(p) \leftrightarrow p \neq 0 \wedge \forall x(x \mid p \rightarrow x = 1 \vee 2 \mid x) \ . \tag{1}$$

Since $Pow_2(p) \rightarrow p > 0$ holds directly from the definition, the above clauses are equivalent to the following properties:

$$\vdash_{\mathrm{PA}} Pow_2(x\mathbf{0}) \leftrightarrow Pow_2(x) \tag{2}$$

$$\vdash_{\mathrm{PA}} Pow_2(x\mathbf{1}) \leftrightarrow x = 0 \ . \tag{3}$$

(2): In the direction ($\rightarrow$) assume $Pow_2(x\mathbf{0})$. We have $x\mathbf{0} > 0$ and thus $x > 0$ from the definition. Now take any z s.t. $z \mid x$. Since then $z \mid 2{\cdot}x$ we get $z = 1$ or $2 \mid z$ from the assumption $Pow_2(x\mathbf{0})$ and so $Pow_2(x)$ holds. In the direction ($\leftarrow$) assume $Pow_2(x)$. Since $x > 0$, we have $2{\cdot}x > 0$ and we take any z s.t. $z \mid 2{\cdot}x$. We wish to prove $z = 1$ or $2 \mid z$. We consider two cases according to 8.1.1(3). If $z = 2{\cdot}z_1$ for some z_1 then $2 \mid z$. If $z = 2{\cdot}z_1 + 1$ for some z_1 then, since $2{\cdot}x = a{\cdot}z$ for some a, we have $2{\cdot}x = 2{\cdot}a{\cdot}z_1 + a$ and we get $a = a_1{\cdot}2$ for some a_1 by 7.5.2(3). Thus $x = a_1{\cdot}2{\cdot}z_1 + a_1 = a_1{\cdot}(2{\cdot}z_1 + 1)$ and so $z \mid x$. We now get $z = 1$ or $2 \mid x$ from the assumption $Pow_2(x)$.

(3): In the direction ($\rightarrow$) assume $Pow_2(2{\cdot}x+1)$. Since $2{\cdot}x+1 \mid 2{\cdot}x+1$, we get from the assumption $2{\cdot}x + 1 = 1$ or $2 \mid 2{\cdot}x + 1$. The latter cannot be the case by 7.5.2(1) and so $2{\cdot}x + 1 = 1$ must hold. Hence $x = 0$. In the direction ($\leftarrow$) it suffice to prove $Pow_2(1)$. We have $1 \neq 0$ and we take any z s.t. $z \mid 1$. Since $1 \mid z$ by 7.5.1(5), we obtain $z = 1$ by antisymmetry.

We have the following property of powers of two:

$$\vdash_{\mathrm{PA}} Pow_2(p) \to (Pow_2(q) \leftrightarrow Pow_2(p{\cdot}q)) \tag{4}$$

which is proved by complete induction on p. Assume $Pow_2(p)$ and consider the two cases implied by 8.1.11(3). If $p = 2{\cdot}u + 1$ for some u then $p = 1$ by (3) and the consequent of the property holds trivially. If $p = 2{\cdot}u$ for some u then $Pow_2(u)$ by (2) and we have $0 < u < p$. Hence

$$Pow_2(q) \overset{\mathrm{IH}}{\Leftrightarrow} Pow_2(u{\cdot}q) \overset{(2)}{\Leftrightarrow} Pow_2(2{\cdot}u{\cdot}q) \ .$$

8.1.4 Order of powers. We will need the following ordering properties of powers of two:

$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge Pow_2(q) \to (p < q \leftrightarrow \exists u\, q = 2{\cdot}u{\cdot}p) \tag{1}$$

$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge Pow_2(q) \to (p \leq q \leftrightarrow \exists u\, q = u{\cdot}p) \tag{2}$$

$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge Pow_2(q) \to ((p < q \leftrightarrow 2{\cdot}p \leq q) \wedge (p < 2{\cdot}q \leftrightarrow p \leq q)) \ . \tag{3}$$

(1): In the direction $(\to)$ we prove

$$\vdash_{\mathrm{PA}} \forall p\, (Pow_2(p) \wedge Pow_2(q) \wedge p < q \to \exists u\, q = 2{\cdot}u{\cdot}p)$$

by complete induction on q. We take any p, assume $Pow_2(p)$, $Pow_2(q)$, $p < q$, and consider two cases for q implied by 8.1.11(3). The case $q = 2{\cdot}q_1 + 1$ for some q_1 leads to a contradiction because then $p < q = 1$ by 8.1.3(3). If $q = 2{\cdot}q_1$ for some q_1 then we consider two similar cases for p. If $p = 2{\cdot}p_1 + 1$ for some p_1 then $p = 1$ by 8.1.3(3) and it suffices to take $u := q_1$. If $p = 2{\cdot}p_1$ for some p_1 then we have $Pow_2(p_1)$ and $Pow_2(q_1)$ by 8.1.3(2) and, since $0 < p_1 < q_1 < q$, we have $q_1 = 2{\cdot}u{\cdot}p_1$ for some u by IH. It now suffices to take the same u because $q = 2{\cdot}q_1 = 2{\cdot}2{\cdot}u{\cdot}p_1 = 2{\cdot}u{\cdot}p$.

In the direction $(\leftarrow)$ assume $Pow_2(p)$, $Pow_2(q)$, and $q = 2{\cdot}u{\cdot}p$. Since $q \neq 0$ and $p \mid q$, we get $p \leq q$ by 7.5.2(2) and it cannot be the case $p = q$ because then $p = q = a = 0$.

(2): In the direction $(\to)$ assume $Pow_2(p)$, $Pow_2(q)$, $p \leq q$, and consider two cases. If $p < q$ then the conclusion of the property holds by (1). If $p = q$ then it suffices to take $u := 1$. In the direction $(\leftarrow)$ assume $Pow_2(p)$, $Pow_2(q)$, and $q = u{\cdot}p$. We now consider two cases for u implied by 8.1.11(3). If $u = 2{\cdot}u_1$ for some u_1 then $p < q$ by (1). If $u = 2{\cdot}u_1 + 1$ for some u_1 then, since $Pow_2(p{\cdot}u)$, we have $Pow_2(u)$ by (4). Hence $u = 1$ by 8.1.3(3) and we have $p = q$.

(3): Assume $Pow_2(p)$ and $Pow_2(q)$. For the first conjunct we have $p < q$ iff, by (1), $q = 2{\cdot}u{\cdot}p$ for some u, since $Pow_2(2{\cdot}p)$ by 8.1.3(2), iff, by (2) $2{\cdot}p \leq q$.

For the second conjunct we have $p \leq q$ iff not $q < p$ iff, by the first conjunct, not $2{\cdot}q \leq p$ iff $p < 2{\cdot}q$.

We will also often use the following easy to prove property of powers of two:

$$\vdash_{\text{PA}} Pow_2(u) \wedge Pow_2(p) \wedge u \geq p \wedge u > s \wedge p > t \rightarrow \\ (\exists b(a{\cdot}u + s = b{\cdot}p + t) \leftrightarrow \exists c(s = c{\cdot}p + t)) \tag{4}$$

which is proved by assuming its antecedent and noting that $u = d{\cdot}p$ for some d by (2). In the direction $(\rightarrow)$ assume also $a{\cdot}u + s = b{\cdot}p + t$ for some b and, since $p > 0$, we get

$$b{\cdot}p + t = a{\cdot}u + s = a{\cdot}d{\cdot}p + s \div p{\cdot}p + s \bmod p = (a{\cdot}d + s \div p){\cdot}p + s \bmod p \ .$$

Because $t < p$ we have $t = s \bmod p$ by 7.4.8(2) and, since then

$$s = s \div p{\cdot}p + s \bmod p = s \div p{\cdot}p + t \ ,$$

it suffices to take $c := s \div p$.

In the direction $(\leftarrow)$ assume also $s = c{\cdot}p + t$ for some c and, since

$$a{\cdot}u + s = a{\cdot}d{\cdot}p + c{\cdot}p + t = (a{\cdot}d + c){\cdot}p + t \ ,$$

it suffices to take $b := a{\cdot}d + c$.

8.1.5 Fast computation of Pow_2. The clausal form for the predicate Pow_2 given in Par. 8.1.3 has a 'slow' recursion. We need the recursion exponentially speeded up to that for the log function discussed in Par. 8.1.2. The predicate Pow_2 with fast recursion has the following clausal form:

$$\begin{aligned}
&Pow_2(p) \leftarrow p = 1 \\
&Pow_2(p) \leftarrow p > 1 \wedge p = [\sqrt{p}]^2 \wedge Pow_2([\sqrt{p}]) \\
&Pow_2(p) \leftarrow p > 1 \wedge p = 2{\cdot}[\sqrt{p \div 2}]^2 \wedge Pow_2([\sqrt{p \div 2}]) \ .
\end{aligned}$$

We wish to prove that the three clauses cover all cases and that they are mutually exclusive. In other words we wish to prove that for every power of two p we have either $p = 1$ or else there is a unique power of two $q < p$ such that either $p = q^2$ or $p = 2{\cdot}q^2$ and that at most one of the cases applies.

The existence part of the discrimination is expressed by

$$\vdash_{\text{PA}} Pow_2(p) \rightarrow p = 1 \vee p > 1 \wedge \exists q(q < p \wedge Pow_2(q) \wedge (p = q^2 \vee p = 2{\cdot}q^2)) \tag{1}$$

which is proved by complete induction on p. Thus assume $Pow_2(p)$ and consider two cases for p implied by 8.1.11(3). If $p = 2{\cdot}p_1 + 1$ for some p_1 we have $p = 1$ by 8.1.3(3). If $p = 2{\cdot}p_1$ for some p_1 then we have $Pow_2(p_1)$ by 8.1.3(2). Note that $p > p_1 \geq 1$. Since $p_1 < p$, one of the three cases obtains by IH. If $p_1 = 1$ then we have $p = 2{\cdot}p_1 = 2{\cdot}1 = 2{\cdot}1^2$. It now suffices to take $q := 1$ because we also have $1 < p$ and $Pow_2(1)$ by 8.1.3(3).

If $p_1 > 0$, $p_1 = q_1^2$, $q_1 < p_1$, and $Pow_2(q_1)$ for some q_1 then it suffices to take $q := q_1$ because we have $q = q_1 < p_1 < p$, $Pow_2(q)$, and $p = 2{\cdot}p_1 = 2{\cdot}q_1^2 = 2{\cdot}q^2$.

If $p_1 > 0$, $p_1 = 2{\cdot}q_1^2$, $q_1 < p_1$, and $Pow_2(q_1)$ for some q_1 then it suffices to take $q := 2{\cdot}q_1$ because we have $Pow_2(q)$ by 8.1.3(2), $q = 2{\cdot}q_1 < 2{\cdot}p_1 = p$, and $p = 2{\cdot}p_1 = 2{\cdot}2{\cdot}q_1^2 = (2{\cdot}q_1)^2 = q^2$.

The uniqueness part of the discrimination follows from

$$\vdash_{\mathrm{PA}} Pow_2(p) \land (p = q_1^2 \lor p = 2{\cdot}q_1^2) \land (p = q_2^2 \lor p = 2{\cdot}q_2^2) \to q_1 = q_2 \ . \qquad (2)$$

This property follows from two auxiliary properties

$$\vdash_{\mathrm{PA}} x^2 = y^2 \to x = y \qquad (3)$$

$$\vdash_{\mathrm{PA}} x^2 = 2{\cdot}y^2 \to x = 0 \land y = 0 \qquad (4)$$

because when we assume the antecedent of (2) there are four cases to consider. For the cases $p = q_1^2$ and $p = q_2^2$ or $p = 2{\cdot}q_1^2$ and $p = 2{\cdot}q_2^2$ the conclusion $q_1 = q_2$ follows by (3).

The cases $p = q_1^2$ and $p = 2{\cdot}q_2^2$ or $p = 2{\cdot}q_1^2$ and $p = q_2^2$ cannot happen because we obtain $p = q_1 = q_2 = 0$ by (4) which contradicts the assumption $Pow_2(p)$.

We now prove the two auxiliary properties: (3): This follows by trichotomy from

$$x < y \to x^2 < y^2$$

proved by assuming $x < y$ and considering two cases. If $x = 0$ then, $0^2 = 0{\cdot}y < y{\cdot}y = y^2$. If $x > 0$ then, since also $y > 0$, we get

$$x^2 = x{\cdot}x < y{\cdot}x < y{\cdot}y = y^2 \ .$$

(4): This is proved as $\forall y(4)$ by complete induction on x. Thus assume $x^2 = 2{\cdot}y$ and consider two cases for x implied by 8.1.11(3). If $x = 2{\cdot}x_1 + 1$ for some x_1 then we obtain a contradiction from $x^2 = 4{\cdot}x_1^2 + 4{\cdot}x_1 + 1 = 2{\cdot}y_2$ because the left-hand side is odd.

If $x = 2{\cdot}x_1$ some x_1 then we get $2{\cdot}x_1^2 = y^2$ and we consider two cases for y implied by 8.1.11(3). The case $y = 2{\cdot}y_1 + 1$ leads to a contradiction similarly as above and when $y = 2{\cdot}y_1$ for some y_1 we obtain $x_1^2 = 2{\cdot}y_1^2$. If it were the case that $x_1 > 0$ then we would have $x_1 < x$ and we would obtain a contradiction $x_1 = y_1 = 0$ by IH. Thus it must be the case that $x_1 = 0$ and then from $0 = 2{\cdot}y_1^2$ we get $y_1 = 0$. Hence $x = y = 0$.

We will also need the following property:

$$\vdash_{\mathrm{PA}} Pow_2(p) \land (p > 1 \land p = q^2 \lor p = 2{\cdot}q^2) \to p > 1 \land q < p \land Pow_2(q) \ . \qquad (5)$$

whis is proved by assuming the antecedent. In either case we have $p > 1$ and from (1) we get

$$q_1 < p \land Pow_2(q_1) \land (p = q_1^2 \lor p = 2{\cdot}q_1^2)$$

for some q_1. But then $q = q_1$ by (2).

8.1.6 Sequences of powers. We wish to encode the sequence of powers needed in the computation of $Pow_2(p)$ by the clauses given in Par. 8.1.5. If $p = 2^x$ then the sequence is given by $2^{x_k}, 2^{x_{k-1}}, \ldots, 2^{x_0}$ for some $k \geq 0$ such that $x_k = x$, $x_i = x_{i+1} \div 2$ for all $i < k$, and $x_0 = 0$ where $x_1 > 0$ if $k > 0$. We encode the sequence of powers by its sum $s = \sum_{i \leq k} 2^{x_i}$. The reader can convince himself that the following explicitly defined predicate:

$$\vdash_{\mathrm{PAx}} Ps(s) \leftrightarrow \forall p \forall a \forall t (Pow_2(p) \land s = a{\cdot}2{\cdot}p + p + t \land p > t \rightarrow p = 1 \lor \exists q \exists t_1 (t = q + t_1 \land q > t_1 \land (p{>}1 \land p = q^2 \lor p = 2{\cdot}q^2))) \quad (1)$$

is true in the standard interpretation of PA whenever s is a sequence of powers determined as above. The main idea is that when p and q are two adjacent powers in s then either $p = q^2$ or $p = 2{\cdot}q^2$ holds. We will need the following properties of sequences of powers:

$$\vdash_{\mathrm{PA}} Ps(0) \quad (2)$$

$$\vdash_{\mathrm{PA}} Ps(1) \quad (3)$$

$$\vdash_{\mathrm{PA}} Pow_2(u) \land u > 1 \land u > s \land \vdash_{\mathrm{PA}} Ps(u + s) \rightarrow Ps(u^2 + u + s) \quad (4)$$

$$\vdash_{\mathrm{PA}} Pow_2(u) \land u > s \land \vdash_{\mathrm{PA}} Ps(u + s) \rightarrow Ps(2{\cdot}u^2 + u + s) \quad (5)$$

$$\vdash_{\mathrm{PA}} Pow_2(u) \land u > s \land Ps(u + s) \rightarrow Ps(u)\ . \quad (6)$$

(2): This holds trivially because $0 = a{\cdot}2{\cdot}p + p + t$ for no p such that $Pow_2(p)$.

(3): Take any p, a, t such that $Pow_2(p)$, $1 = a{\cdot}2{\cdot}p + p + t$ and $p > t$ holds. We then clearly have $p = 1$ and $a = t = 0$.

(4): Assume the antecedent of the property and note that $Pow_2(u^2)$ by 8.1.3(4) and $Pow_2(2{\cdot}u^2)$ by 8.1.3(2). For the proof of $Ps(u^2 + u + s)$ take any p, a, t such that $Pow_2(p)$, $u^2 + u + s = a{\cdot}2{\cdot}p + p + t$, $p > t$, and note that $Pow_2(2{\cdot}p)$ by 8.1.3(2). We consider two cases by dichotomy. If $u^2 \geq 2{\cdot}p$ then, since $u^2 > u$, we have $u^2 \geq 2{\cdot}u > u + s$ by 8.1.4(3). We also have $2{\cdot}p > p + t$ and so $u + s = a_1{\cdot}2{\cdot}p + p + t$ for some a_1 by 8.1.4(4). We now obtain from $Ps(u + s)$

$$p = 1 \lor \exists q \exists t_1 (t = q + t_1 \land q > t_1 \land (p{>}1 \land p = q^2 \lor p = 2{\cdot}q^2))$$

which is the consequent of $Ps(u^2 + u + s)$.

If $u^2 < 2{\cdot}p$ then $u^2 \leq p$ by 8.1.4(3). If it were the case that $a > 0$ then we would obtain contradiction

$$u^2 + u + s < 2{\cdot}u^2 \leq 2{\cdot}p < a{\cdot}2{\cdot}p + p + t\ .$$

We thus have $u^2 + u + s = p + t$ and if it were the case that $u^2 < p$ then we would obtain contradiction

$$u^2 + u + s < 2{\cdot}u^2 \overset{8.1.4(3)}{\leq} p \leq p + t\ .$$

This means that $p = u^2$ and so $u + s = t$, $p > 1$. Thus it suffices to take $q := u$ and $t_1 := s$ to satisfy the consequent of $Ps(u^2 + u + s)$:

$$\exists q \exists t_1 (t = q + t_1 \wedge q > t_1 \wedge (p{>}1 \wedge p = q^2 \vee p = 2{\cdot}q^2)) \ .$$

Property (5) is proved similarly.

(6): Assume $Pow_2(u)$, $u > s$, $Ps(u + s)$, and for the proof of $Ps(s)$ take any p, a, t such that $Pow_2(p)$, $s = a{\cdot}2{\cdot}p + p + t$, $p > t$, and note that $Pow_2(2{\cdot}p)$ by 8.1.3(2). We consider two cases by dichotomy. If $u \geq 2{\cdot}p$ then $u + s = a_1{\cdot}2{\cdot}p + p + t$ for some a_1 by 8.1.4(4). The consequent of $Ps(s)$ now follows from that of $Ps(u + s)$. The case $u < 2{\cdot}p$ cannot happen because it would lead to contradiction by

$$s < u \overset{8.1.4(3)}{\leq} p \leq a{\cdot}2{\cdot}p + p + t \ .$$

8.1.7 The function $ps(p)$ yielding the power sequence for p. The function $ps(p)$ yielding the sequence of powers starting from $p = 2^k$, i.e. such that $ps(p) = \sum_{i \leq k} 2^{x_i}$ (see Par. 8.1.6), is introduced into PA by minimalization:

$$\vdash_{\text{PAx}} ps(p) = \mu_s[Pow_2(p) \rightarrow p \leq s \wedge Ps(s)]$$

whose existence condition follows from the stronger property

$$\vdash_{\text{PA}} Pow_2(p) \rightarrow \exists s(Ps(p + s) \wedge p > s) \tag{1}$$

proved by complete induction on p where we assume $Pow_2(p)$ and continue by the case analysis implied by 8.1.5(1). If $p = 1$ then it suffices to take $s := 0$ by 8.1.6(3). If $p > 1$ then there is a q s.t. $q < p$, $Pow_2(q)$, and either $p = q^2$ or $p = 2{\cdot}q^2$. In either case we have a t s.t. $Ps(q+t)$ and $q > t$ by IH. If $q > 1$ then we have $2{\cdot}q \leq q^2 \leq p$ and if $q = 1$ then $p = 2$ and we have $2{\cdot}q = p$. In either case it suffices to take $s := q + t < 2{\cdot}q \leq p$ because we have $Ps(p + s)$ by 8.1.6(4) when $p = q^2$ and by 8.1.6(5) when $p = 2{\cdot}q^2$.

The defining axiom for ps implies:

$$\vdash_{\text{PA}} Pow_2(p) \rightarrow p \leq ps(p) \wedge Ps(ps(p)) \tag{2}$$

$$\vdash_{\text{PA}} p \leq s \wedge Ps(s) \rightarrow ps(p) \leq s \ . \tag{3}$$

The basic properties of the power sequence function are:

$$\vdash_{\text{PA}} Pow_2(p) \rightarrow ps(p) < 2{\cdot}p \tag{4}$$

$$\vdash_{\text{PA}} ps(1) = 1 \tag{5}$$

$$\vdash_{\text{PA}} \forall s(Pow_2(p) \wedge Ps(p + s) \wedge p > s \rightarrow ps(p) = p + s) \tag{6}$$

$$\vdash_{\text{PA}} Pow_2(p) \wedge (p > 1 \wedge p = q^2 \vee p = 2{\cdot}q^2) \rightarrow ps(p) = p + ps(q) \ . \tag{7}$$

(4): Assume $Pow_2(p)$ and obtain an s s.t. $Ps(p + s)$ and $p > s$ by (1). Thus

$$ps(p) \overset{(3)}{\leq} p + s < 2{\cdot}p\ .$$

(5): We have $Pow_2(1)$ by 8.1.3(3) and so $1 \leq ps(1)$ by (2). We have $ps(1) < 2$ by (4) and so $ps(1) = 1$.

(6): By complete induction on p. Take any s, assume $Pow_2(p)$, $Ps(p+s)$, $p > s$, and consider two cases. If $p = 1$ then we have $s = 0$ and $ps(1) \overset{(5)}{=} 1+0$. If $p > 1$ then for $s := p + s = 0{\cdot}2{\cdot}p + p + s$ we obtain from $Ps(p+s)$

$$s = q + t_1 \wedge q > t_1 \wedge (p > 1 \wedge p = q^2 \vee p = 2{\cdot}q^2)$$

for some q and t_1. We have $Pow_2(q)$ and $q < p$ by 8.1.5(5), $Ps(s)$ by 8.1.6(6), and so $ps(q) = q + t_1 = s$ by IH.

We also have $p \leq ps(p)$ and $Ps(ps(p))$ by (2) and $ps(p) < 2{\cdot}p$ by (4). Hence $ps(p) = p + t$ for some t s.t. $p > t$. For $s := p + t = 0{\cdot}2{\cdot}p + p + t$ we obtain from $Ps(p+t)$

$$t = q_1 + t_2 \wedge q_1 > t_2 \wedge (p > 1 \wedge p = q_1^2 \vee p = 2{\cdot}q_1^2)$$

for some q_1 and t_2. We have $q = q_1$ by 8.1.5(2) and, since $Ps(t)$ holds by 8.1.6(6), we get $ps(q) = q+t_2 = t$ by IH. Thus $ps(p) = p+t = p+ps(q) = p+s$.

(7): Assume the antecedent of the property. We have $Pow_2(q)$, $q < p$, and $p > 1$ by 8.1.5(5). From (1) there is an s s.t. $Ps(p+s)$ and $p > s$. Hence $ps(p) = p + s$ by (6). For $s := p + s = 0{\cdot}2{\cdot}p + p + s$ we obtain from $Ps(p+s)$

$$s = q_1 + t_1 \wedge q_1 > t_1 \wedge (p > 1 \wedge p = q_1^2 \vee p = 2{\cdot}q_1^2)$$

for some q_1 and t_1. We get $q = q_1$ by 8.1.5(2), and, since $Ps(s)$ holds by 8.1.6(6), we get $ps(q) = q + t_1 = s$ by (6).

8.1.8 Course of values sequences for the log **function.** We will encode the computation of the log function such that for $p = 2^x$ we have $\log(p) = x$ by the fast recurrences discussed in Par. 8.1.2. To that end we take the power sequence $ps(p) = \sum_{i \leq k} 2^{x_i}$, use the fact that each $x_i < 2^{x_i}$, that there are at least x_i bits in $ps(p)$ between the bit postions $2^{x_{i+1}}$ and 2^{x_i}, and encode the *course of values* sequence $x_k, x_{k-1}, \ldots, x_0$ for the successive values of $\log(2^{x_i})$ at the corresponding bits of the power sequence. We will define in Par. 8.1.9 a *course of values* function $\overline{\log}(p)$ to yield the course of values sequence such that $\overline{\log}(p) = \sum_{i \leq k} x_i{\cdot}2^{x_i}$.

We recall that two neighboring powers p and q in the power sequence $ps(u)$ are such that either $p = q^2$ or $p = 2{\cdot}q^2$. The relation between the values x and y stored in the course of values sequence $\overline{\log}(u)$ at the powers p and q respectively, i.e. when $\overline{\log}(u) = a{\cdot}p^2 + x{\cdot}p + y{\cdot}q + u_1$ for $x < p$, $y < q$, and $q > u_1$, is expressed by $Nbs(\overline{\log}(u), p, q)$ where the predicate is explicitly introduced into PA as follows:

$$\vdash_{\mathrm{PAx}} Nbs(s,p,q) \leftrightarrow \exists b \exists x \exists y \exists s_1 (s = b{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s_1 \wedge$$
$$x < p \wedge y < q \wedge q > s_1 \wedge (p > 1 \wedge p = q^2 \wedge x = y\mathbf{0} \vee p = 2{\cdot}q^2 \wedge x = y\mathbf{1}))\ . \quad (1)$$

The reader can convince himself that the following explicitly defined predicate:

$$\vdash_{\mathrm{PAx}} Cs(u,s) \leftrightarrow \forall p \forall a \forall t (Pow_2(p) \wedge ps(u) = a{\cdot}2{\cdot}p + p + t \wedge p > t \rightarrow p = 1 \wedge 2 \mid s \vee \exists q\, Nbs(s,p,q)) \tag{2}$$

is true in the standard interpretation of PA whenever s is the course of values sequence for u, i.e. $\overline{\log}(u) = s$. We will need the following properties of Cs:

$$\vdash_{\mathrm{PA}} Cs(1,0) \tag{3}$$

$$\vdash_{\mathrm{PA}} Pow_2(u) \wedge u > 1 \wedge Cs(u, z{\cdot}u + s) \wedge z < u \wedge u > s \rightarrow Cs(u^2, z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s) \tag{4}$$

$$\vdash_{\mathrm{PA}} Pow_2(u) \wedge Cs(u, z{\cdot}u + s) \wedge z < u \wedge u > s \rightarrow Cs(2{\cdot}u^2, z\mathbf{1}{\cdot}2{\cdot}u^2 + z{\cdot}u + s) \tag{5}$$

$$\vdash_{\mathrm{PA}} Pow_2(u) \wedge Cs(u, z{\cdot}u + s) \wedge u > s \wedge (u > 1 \wedge u = u_1^2 \vee u = 2{\cdot}u_1^2) \rightarrow Cs(u_1, s)\ . \tag{6}$$

(3): Take any p, a, t such that $Pow_2(p)$, $ps(1) = a{\cdot}2{\cdot}p + p + t$ and $p > t$ holds. We have $ps(1) = 1$ by 8.1.7(5) and thus we clearly must have $p = 1$ and $a = t = 0$. Since $2 \mid 0$, we get $Cs(1,0)$.

(4): Assume the antecedent of the property and note that $Pow_2(2{\cdot}u)$ by 8.1.3(2) and $Pow_2(u^2)$ by 8.1.3(4). Since $u < u^2$, we also have

$$u < 2{\cdot}u \overset{8.1.4(3)}{\leq} u^2\ . \tag{7}$$

For the proof of $Cs(u^2, z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s)$ we take any p, a, t such that $Pow_2(p)$, $ps(u^2) = a{\cdot}2{\cdot}p + p + t$, $p > t$. We thus have

$$u^2 + ps(u) \overset{8.1.7(7)}{=} ps(u^2) = a{\cdot}2{\cdot}p + p + t\ . \tag{8}$$

We also have $Pow_2(2{\cdot}p)$ by 8.1.3(2) and

$$u^2 = u{\cdot}u \geq (z+1){\cdot}u = z{\cdot}u + z > z{\cdot}u + s\ . \tag{9}$$

We now consider two cases by dichotomy. If $u^2 > p$ then, since $u^2 \geq 2{\cdot}p$ by 8.1.4(3), we have $u^2 \geq 2{\cdot}u > ps(u)$ by 8.1.7(4). Since also $2{\cdot}p > p + t$, we obtain

$$ps(u) = a_1{\cdot}2{\cdot}p + p + t \tag{10}$$

for some a_1 by 8.1.4(4). From $Cs(u, z{\cdot}u + s)$ we now get two cases. If $p = 1$ and $2 \mid z{\cdot}u + s$ then, since $1 < u < u^2$, we have $u^2 = 2{\cdot}k{\cdot}u$ for some k by 8.1.4(1) and so $2 \mid z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s$. This proves $Cs(u^2, z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s)$.

If $Nbs(z{\cdot}u + s, p, q)$ for some q then we have

$$z{\cdot}u + s = b{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s_1 \wedge x < p \wedge y < q \wedge q > s_1 \wedge$$
$$(p > 1 \wedge p = q^2 \wedge x = y\mathbf{0} \vee p = 2{\cdot}q^2 \wedge x = y\mathbf{1}))\ .$$

for some b, x, y, and s_1. We then get

$$p^2 = p{\cdot}p \geq (x+1){\cdot}p = x{\cdot}p + p \geq x{\cdot}p + q^2 \geq x{\cdot}p + (y+1){\cdot}q =$$
$$x{\cdot}p + y{\cdot}q + q > x{\cdot}p + y{\cdot}q + s_1\ . \tag{11}$$

We have $2{\cdot}u \overset{8.1.7(4)}{>} ps(u) \overset{(10)}{\geq} p$ and so $u \geq p$ by 8.1.4(3). From $u^2 \geq p^2$, (9), and (11) we obtain

$$z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s = b_1{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s_1$$

for some b_1 by 8.1.4(4). But then $Nbs(z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s, p, q)$ which proves $Cs(u^2, z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s)$.

The other dichotomy case is $u^2 \leq p$. If $a > 0$ then we contradict (8) by

$$ps(u^2) \overset{8.1.7(4)}{<} 2{\cdot}u^2 \leq 2{\cdot}p \leq a{\cdot}2{\cdot}p + p + t\ .$$

We thus have $a = 0$ and by (8) we get $u^2 + ps(u) = p + t$. If it were the case that $u^2 < p$ then we would contradict (8) again:

$$u^2 + ps(u) = ps(u^2) \overset{8.1.7(4)}{<} 2{\cdot}u^2 \overset{8.1.4(3)}{\leq} p \leq p + t\ .$$

Thus $u^2 = p$ and for $q := u$, $b := 0$, $x := z\mathbf{0}$, $y := z$, and $s_1 := s$ we have $Nbs(z\mathbf{0}{\cdot}u^2 + z{\cdot}u + s, p, q)$ because then $y = z < u = q$, $q = u > s = s_1$, and $x = z\mathbf{0} < 2{\cdot}u \overset{(7)}{\leq} u^2 = p$.

(5): This is proved similarly as (4).

(6): Assume the antecedent of the property. We have $Pow_2(u_1)$ and $Pow_2(2{\cdot}u_1)$ by 8.1.3(2) and 8.1.3(4). If $u = u_1^2$ and $u_1 > 1$ then, since $u > u_1$, we get $u \geq 2{\cdot}u_1$ by 8.1.4(3). If $u = 2{\cdot}u_1^2$ then, since $u_1^2 \geq u_1$, we get $u \geq 2{\cdot}u_1$ again. For the proof of $Cs(u_1, s)$ we take any p, a, t such that $Pow_2(p)$, $ps(u_1) = a{\cdot}2{\cdot}p + p + t$, and $p > t$. Since $Pow_2(2{\cdot}p)$ by 8.1.3(2), $2{\cdot}p > p + t$, and

$$u \geq 2{\cdot}u_1 \overset{8.1.7(4)}{>} ps(u_1) \geq p\ , \tag{12}$$

i.e. $u \geq 2{\cdot}p$ by 8.1.4(3), we obtain

$$ps(u) \overset{8.1.7(7)}{=} u + ps(u_1) = a_1{\cdot}2{\cdot}p + p + t$$

for some a_1 by 8.1.4(4). From $Cs(u, z{\cdot}u + s)$ we now get two cases. If $p = 1$ and $2 \mid z{\cdot}u + s$ then from $u \geq 2{\cdot}u_1$ we obtain $2 \mid z{\cdot}u$ because $u = k{\cdot}2{\cdot}u_1$ for some k by 8.1.4(2). Thus $2 \mid s$ by 7.5.2(3) which proves $Cs(u_1, s)$.

If $Nbs(z{\cdot}u + s, p, q)$ for some q then we have

$$z{\cdot}u + s = b{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s_1 \wedge x < p \wedge y < q \wedge q > s_1 \wedge$$
$$(p > 1 \wedge p = q^2 \wedge x = y\mathbf{0} \vee p = 2{\cdot}q^2 \wedge x = y\mathbf{1}))\ .$$

for some b, x, y, and s_1. We have $Pow_2(p^2)$ by 8.1.3(4) and $p^2 > x{\cdot}p + y{\cdot}q + s_1$ similarly as in (11). We have $2{\cdot}u_1 > p$ by (12) and so $2{\cdot}u_1 \geq 2{\cdot}p$, i.e. $u_1 \geq p$, by 8.1.4(3). Hence $u \geq u_1^2 \geq p^2$ and, since $u > s$, we obtain $s = b_1{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s_1$ for some b_1 by 8.1.4(4). But then $Nbs(s, p, q)$ which proves $Cs(u_1, s)$.

8.1.9 The course of values function $\overline{\log}(p)$ for $\log(p)$. The function $\overline{\log}(p)$ yielding the course of values sequence from $p = 2^k$ for log, i.e. such that $\overline{\log}(p) = \sum_{i \leq k} x_i{\cdot}2^{x_i}$ (see Par. 8.1.8), is introduced into PA by minimalization:

$$\vdash_{\mathrm{PAx}} \overline{\log}(p) = \mu_s[Pow_2(p) \rightarrow Cs(p, s)] \tag{1}$$

whose existence condition follows from the stronger property

$$\vdash_{\mathrm{PA}} Pow_2(p) \rightarrow \exists s(Cs(p, s) \wedge p^2 > s) \tag{2}$$

proved by complete induction on p where we assume $Pow_2(p)$ and continue by the case analysis of p implied by 8.1.5(1). If $p = 1$ then it suffices to take $s := 0$ by 8.1.8(3). If $p > 1$ then there is a q s.t. $q < p$, $Pow_2(q)$, and either $p = q^2$ or $p = 2{\cdot}q^2$. We obtain a $t < q^2$ such that $Cs(q, t)$ by IH. We have $t = z{\cdot}q + s_1$ for $z = t \div q$ and $s_1 = t \bmod q < q$. Also $z < q$ because if $z \geq q$ we would get a contradiction $q^2 > t = z{\cdot}q + s_1 \geq q^2$. But then

$$z\mathbf{1} = 2{\cdot}z + 1 = z + z + 1 < q + z + 1 \leq q + q = 2{\cdot}q \overset{8.1.4(3)}{\leq} p\ . \tag{3}$$

Now, if $p = q^2$ then we have $Cs(p, s)$ for $s = z\mathbf{0}{\cdot}p + t$ by 8.1.8(4), and if $p = 2{\cdot}q^2$ then we have $Cs(p, s)$ for $s = z\mathbf{1}{\cdot}p + t$ by 8.1.8(5). In either case we have

$$s \leq z\mathbf{1}{\cdot}p + t < z\mathbf{1}{\cdot}p + q^2 \leq z\mathbf{1}{\cdot}p + p = (z\mathbf{1} + 1){\cdot}p \overset{(3)}{\leq} p^2\ .$$

The defining axiom for $\overline{\log}$ implies:

$$\vdash_{\mathrm{PA}} Pow_2(p) \rightarrow Cs(p, \overline{\log}(p)) \tag{4}$$
$$\vdash_{\mathrm{PA}} Cs(p, s) \rightarrow \overline{\log}(p) \leq s\ . \tag{5}$$

We will need the following basic properties of the function $\overline{\log}$:

$$\vdash_{\mathrm{PA}} Pow_2(p) \rightarrow \overline{\log}(p) < p^2 \tag{6}$$
$$\vdash_{\mathrm{PA}} \overline{\log}(1) = 0 \tag{7}$$
$$\vdash_{\mathrm{PA}} \forall z \forall s(Pow_2(p) \wedge Cs(p, z{\cdot}p + s) \wedge z < p \wedge p > s \rightarrow \overline{\log}(p) = z{\cdot}p + s) \tag{8}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge p > 1 \wedge p = q^2 \rightarrow \overline{\log}(p) = (\overline{\log}(q) \div q)\mathbf{0}{\cdot}p + \overline{\log}(q) \tag{9}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge p = 2{\cdot}q^2 \rightarrow \overline{\log}(p) = (\overline{\log}(q) \div q)\mathbf{1}{\cdot}p + \overline{\log}(q)\ . \tag{10}$$

(6): Assume $Pow_2(p)$. We have $Cs(p,s)$ for some $s < p^2$ by (2) and so $\overline{\log}(p) \le s < p^2$ by (5).

(7): We have $Cs(1,0)$ by 8.1.8(3) and so $\overline{\log}(1) \le 0$ by (5).

(8): By complete induction on p. Take any z, s, assume $Pow_2(p)$, $Cs(p, z{\cdot}p + s)$, $z < p$, and $p > s$. We have

$$ps(p) = p + t = 0{\cdot}2{\cdot}p + p + t \tag{11}$$

for some $t < p$ by 8.1.7(2) and 8.1.7(4). From $Cs(p, z{\cdot}p + s)$ we then obtain

$$p = 1 \wedge 2 \mid z{\cdot}p + s \vee \exists q Nbs(z{\cdot}p + s, p, q) \ .$$

If $p = 1$ then, since $z = s = 0$, we have

$$\overline{\log}(p) = \overline{\log}(1) \overset{(7)}{=} 0 = z{\cdot}p + s \ .$$

If $Nbs(z{\cdot}p + s, p, q)$ for some q then we have

$$\begin{aligned}&z{\cdot}p + s = b{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s_1 \wedge x < p \wedge y < q \wedge q > s_1 \wedge \\ &(p > 1 \wedge p = q^2 \wedge x = y\mathbf{0} \vee p = 2{\cdot}q^2 \wedge x = y\mathbf{1}))\end{aligned}$$

for some b, x, y, and s_1. We obtain $p > 1$, $q < p$, $Pow_2(q)$ by 8.1.5(5). Because $z < p$ we have $b = 0$ and, since $y{\cdot}q + s_1 < y{\cdot}q + q = (y+1){\cdot}q \le q^2 \le p$, we obtain $z = x$, and $s = y{\cdot}q + s_1$ by 7.4.8(1)(2). We have $Cs(q,s)$ by 8.1.8(6) and so $\overline{\log}(q) = y{\cdot}q + s_1 = s$ by IH.

We have $Cs(p, \overline{\log}(p))$ by (4) and from (11), since $p > 1$, we obtain $Nbs(\overline{\log}(p), p, q_1)$ for some q_1 for which we have $q = q_1$ by 8.1.5(2). Thus

$$\begin{aligned}&\overline{\log}(p) = b_1{\cdot}p^2 + x_1{\cdot}p + y_1{\cdot}q + s_2 \wedge x_1 < p \wedge y_1 < q \wedge q > s_2 \wedge \\ &(p > 1 \wedge p = q^2 \wedge x_1 = y_1\mathbf{0} \vee p = 2{\cdot}q^2 \wedge x_1 = y_1\mathbf{1}))\end{aligned}$$

for some b_1, x_1, y_1, and s_2. We have $b_1 = 0$ by (6) and, since $y_1{\cdot}q + s_2 < p$, we obtain $Cs(q, y_1{\cdot}q + s_2)$ by 8.1.8(6) and $\overline{\log}(q) = y_1{\cdot}q + s_2$ by IH. Since $\overline{\log}(q) = y{\cdot}q + s_1$, we obtain $y = y_1$ and $s_1 = s_2$ by 7.4.8(1)(2). Because of 8.1.5(4) we then have $x = x_1$ and so

$$\overline{\log}(p) = x_1{\cdot}p + y_1{\cdot}q + s_2 = x{\cdot}p + \overline{\log}(q) = z{\cdot}p + y{\cdot}q + s_1 = z{\cdot}p + s \ .$$

(9): Assume $Pow_2(p)$, $p > 1$, and $p = q^2$. We have $Pow_2(q)$ and $p > q$ by 8.1.5(5), $Pow_2(2{\cdot}q)$ by 8.1.3(2), and also

$$ps(p) \overset{8.1.7(7)}{=} p + ps(q) = 0{\cdot}2{\cdot}p + p + ps(q)$$

where

$$ps(q) \overset{8.1.7(4)}{<} 2{\cdot}q \overset{8.1.4(3)}{\le} p \ .$$

From (4) we thus obtain $Nbs(\overline{\log}(p), p, q_1)$ for some q_1 for which we have $q = q_1$ by 8.1.5(2). We thus have

$$\overline{\log}(p) = b{\cdot}p^2 + x{\cdot}p + y{\cdot}q + s \wedge x < p \wedge y < q \wedge q > s \wedge x = y\mathbf{0}$$

for some b, x, y, and s, since $p \neq 2{\cdot}q^2$ by 8.1.5(4). It must be the case that $b = 0$ by (6) and, since $p > y{\cdot}q + s$, we obtain $Cs(q, y{\cdot}q + s)$ from (4) by 8.1.8(6). Hence, $\overline{\log}(q) = y{\cdot}q + s$ by (8), from which we get $y = \overline{\log}(q) \div q$ and so

$$\overline{\log}(p) = x{\cdot}p + \overline{\log}(q) = y\mathbf{0}{\cdot}p + \overline{\log}(q) = (\overline{\log}(q) \div q)\mathbf{0}{\cdot}p + \overline{\log}(q) \ .$$

(10): This is proved similarly as (9).

8.1.10 Introduction of log **into PA.** We explicitly introduce into PA the logarithm function log by

$$\vdash_{\mathrm{PAx}} \log(p) = \overline{\log}(p) \div p \ . \tag{1}$$

The function satisfies the following:

$$\vdash_{\mathrm{PA}} \log(1) = 0 \tag{2}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge p = q^2 \wedge p > 1 \to \log(p) = \log(q)\mathbf{0} \tag{3}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge p = 2{\cdot}q^2 \to \log(p) = \log(q)\mathbf{1} \tag{4}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \to \log(2{\cdot}p) = \log(p) + 1 \tag{5}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \wedge Pow_2(q) \wedge p < q \to \log(p) < \log(q) \ . \tag{6}$$

(2): We have $\log(1) = \overline{\log}(1) \div 1 \overset{8.1.9(7)}{=} 0 \div 1 = 0$.

(3): Assume $Pow_2(p)$, $p = q^2$, and $p > 1$. We have $Pow_2(q)$ by 8.1.5(5) and by 8.1.9(9) we get $\overline{\log}(p) = (\overline{\log}(q) \div q)\mathbf{0}{\cdot}p + \overline{\log}(q)$. Since $\overline{\log}(q) < q^2 = p$ by 8.1.9(6) we have

$$\log(p) = \overline{\log}(p) \div p \overset{7.4.8(2)}{=} \log(q)\mathbf{0} \ .$$

(4): Assume $Pow_2(p)$ and $p = 2{\cdot}q^2$. We have $Pow_2(q)$ by 8.1.5(5) and by 8.1.9(10) we get $\overline{\log}(p) = (\overline{\log}(q) \div q)\mathbf{1}{\cdot}p + \overline{\log}(q)$. Since $\overline{\log}(q) < q^2 < p$ by 8.1.9(6) we have

$$\log(p) = \overline{\log}(p) \div p \overset{7.4.8(2)}{=} \log(q)\mathbf{1} \ .$$

(5): By complete induction on p. Assume $Pow_2(p)$ and obtain $Pow_2(2{\cdot}p)$ by 8.1.3(2). We now consider three cases implied by 8.1.5(1). If $p = 1$ then we have

$$\log(2{\cdot}p) = \log(2{\cdot}1) = \log(2{\cdot}1^2) \overset{(4)}{=} 2{\cdot}\log(1) + 1 \overset{(2)}{=} \log(1) + 1 = \log(p) + 1 \ .$$

If $p > 1$ and $p = q^2$ for some q such that $Pow_2(q)$ then we have

$$\log(2{\cdot}p) = \log(2{\cdot}q^2) \stackrel{(4)}{=} 2{\cdot}\log(q) + 1 \stackrel{(3)}{=} \log(q^2) + 1 = \log(p) + 1 \ .$$

If $p = 2{\cdot}q^2$ for some $q < p$ such that $Pow_2(q)$ then $p > 1$ and we have

$$\log(2{\cdot}p) = \log(2{\cdot}(2{\cdot}q^2)) = \log((2{\cdot}q)^2) \stackrel{(3)}{=} 2{\cdot}\log(2{\cdot}q) \stackrel{\text{IH}}{=} 2{\cdot}(\log(q) + 1) =$$
$$(2{\cdot}\log(q) + 1) + 1 \stackrel{(4)}{=} \log(2{\cdot}q^2) + 1 = \log(p) + 1 \ .$$

(6): By complete induction on q. Assume $Pow_2(p)$, $Pow_2(q)$, and $p < q$. We have $q = 2{\cdot}u{\cdot}p$ for some u by 8.1.4(1) and, since $Pow_2(u{\cdot}p)$ by 8.1.3(2), we obtain $p \leq u{\cdot}p < q$ by 8.1.4(2). Thus either $p < u{\cdot}p$ and then $\log(p) < \log(u{\cdot}p)$ by IH, or else $p = u{\cdot}p$ and then $\log(p) = \log(u{\cdot}p)$. In either case we have

$$\log(p) \leq \log(u{\cdot}p) < \log(u{\cdot}p) + 1 \stackrel{(5)}{=} \log(2{\cdot}u{\cdot}p) = \log(q) \ .$$

8.1.11 Introduction of 2^x into PA. We are now ready to introduce the exponentiation function by minimalization:

$$\vdash_{\text{PAx}} 2^x = \mu_p[Pow_2(p) \wedge \log(p) = x]$$

whose existence condition:

$$\vdash_{\text{PA}} \exists p(Pow_2(p) \wedge \log(p) = x)$$

is proved by induction on x. In the base case it suffices to take $p := 1$ because of 8.1.3(3) and 8.1.10(2). In the inductive case we obtain a p s.t. $Pow_2(p)$ and $\log(p) = x$ by IH. We then get $Pow_2(2{\cdot}p)$ by 8.1.3(2), $\log(2{\cdot}p) = \log(p) + 1 = x + 1$ by 8.1.10(5), and so it suffices to take $p := 2{\cdot}p$.

The following property asserts that the functions 2^x and log are inverse:

$$\vdash_{\text{PA}} 2^x = p \leftrightarrow Pow_2(p) \wedge \log(p) = x \ . \tag{1}$$

In the direction ($\rightarrow$) assume $2^x = p$ and from the first conjunct of the defining axiom for 2^x: $Pow_2(2^x) \wedge \log(2^x) = x$ we immediately obtain $Pow_2(p)$ and $\log(p) = x$.

In the direction ($\leftarrow$) assume $Pow_2(p)$ and $\log(p) = x$ and obtain $Pow_2(2^x)$ as well as $\log(2^x) = x$ from the defining axiom for 2^x. Consider three cases by trichotomy. If $2^x < p$ we obtain a contradiction $x = \log(2^x) < \log(p) = x$ by 8.1.10(6). We similarly derive a contradiction for the case $2^x > p$. This means that the third case $2^x = p$ must hold.

We are now ready to prove the two recurrences for the exponentiation function from Par. 8.1.2. Property 8.1.2(1) follows from (1) by 8.1.3(3) and 8.1.10(2).

Property 8.1.2(2) is proved as follows. From $2^x = 2^x$ we get $Pow_2(2^x)$ and $\log(2^x) = x$ by (1). We get $\log(2{\cdot}2^x) = \log(2^x) + 1 = x + 1$ by 8.1.10(5) and, since $Pow_2(2{\cdot}2^x)$ by 8.1.3(2), we get $2^{x+1} = 2{\cdot}2^x$ by (1).

8.1.12 Some properties of 2^x. We list some of the properties of the exponential function:

$$\vdash_{\mathrm{PA}} 2^0 = 1 \tag{1}$$
$$\vdash_{\mathrm{PA}} 2^{x+1} = 2{\cdot}2^x \tag{2}$$
$$\vdash_{\mathrm{PA}} Pow_2(p) \leftrightarrow \exists x\, 2^x = p \tag{3}$$
$$\vdash_{\mathrm{PA}} x < 2^x \tag{4}$$
$$\vdash_{\mathrm{PA}} x < y \to 2^x < 2^y \tag{5}$$
$$\vdash_{\mathrm{PA}} 2^{x+y} = 2^x{\cdot}2^y\ . \tag{6}$$

Properties (1) and (2) are just the properties 8.1.2(1)(2) proved in Par. 8.1.11.

(3): Follows directly from 8.1.11(1) because $\exists x\ \log(p) = x$ holds trivially.

(4): By induction on x. In the base case we have $0 < 1 = 2^0$. In the inductive case we have $x < 2^x$ by IH from which we get $x + 1 \leq 2^x < 2^{x+1}$.

(5): Assume $x < y$. By substituting $p := 2^x$ in 8.1.11(1) we obtain $Pow_2(2^x)$ and $\log(2^x) = x$. We get $Pow_2(2^y)$ and $\log(2^y) = y$ similarly. We thus have $\neg \log(2^y) < \log(2^x)$ and we obtain $\neg 2^y < 2^x$, i.e. $2^x \leq 2^y$, by 8.1.10(6). If it were the case that $2^x = 2^y$ then we would het a contradiction $x = \log(2^x) = \log(2^y) = y$.

(6): By induction on x. In the base case we have $2^{0+y} = 2^y = 1{\cdot}2^y = 2^0{\cdot}2^y$. In the inductive case we have

$$2^{x'+y} = 2^{(x+y)'} = 2{\cdot}2^{x+y} \overset{\mathrm{IH}}{=} 2{\cdot}2^x{\cdot}2^y = 2^{x'}{\cdot}2^y\ .$$

8.2 Primitive Recursion

8.2.1 Primitive recursive functions. The class of *primitive recursive* functions can be characterized as the smallest class obtained by explicit definitions:

$$f(\vec{x}) = \tau[\vec{x}] \tag{1}$$

and by *primitive recursion*:

$$f(0, \vec{y}) = g(\vec{y})$$
$$f(x', \vec{y}) = h(x, \vec{y}, f(x, \vec{y}))$$

where the term τ is formed from the constant 0, variables among the n ($n \geq 0$) variables of $\vec{x}$, applications of the successor function ρ', and of applications of previously introduced functions. In the scheme of primitive recursion the functions g and h are previously introduced functions, g is n-ary ($n \geq 0$) and h is $(n + 2)$-ary.

We already know that we can introduce into PA explicitly defined functions. In this section we show that PA is *closed* under primitive recursion, i.e. if functions g and h have been introduced into PA then we can introduce into PA by minimalization a function f to satisfy the above recurrences. The reader will note that by showing the closure of PA under primitive recursion will have proved more than that the primitive recursive functions can be introduced into PA. This is because we will be able to introduce into PA the function f defined by primitive recursion from any two functions g and h already in PA even if one or both of them will not be primitive recursive.

8.2.2 Bounded indexing function. For the introduction of primitive recursive functions into PA we will need to recover digits of numbers represented in the notation with the base 2^k for for a given $k \geq 1$. As is well-known, any number x can be uniquely written in such a representation as $x = \sum_i d_i{\cdot}2^{k\cdot i}$. We can recover the i-th digit d_i of x by a ternary *bounded indexing function* $d_i = (x)_i^{[k]}$ which can be explicitly introduced into PA by:

$$\vdash_{\mathrm{PAx}} (s)_i^{[k]} = s \div 2^{k\cdot i} \bmod 2^k \ . \tag{1}$$

We will need the following properties of the bounded indexing function:

$$\vdash_{\mathrm{PA}} b < 2^k \land t < 2^{k\cdot i} \to (a{\cdot}2^{k\cdot i'} + b{\cdot}2^{k\cdot i} + t)_i^{[k]} = b \tag{2}$$

$$\vdash_{\mathrm{PA}} i < j \land s < 2^{k\cdot j} \to (a{\cdot}2^{k\cdot j}{+}s)_i^{[k]} = (s)_i^{[k]} \ . \tag{3}$$

(2): Assume the antecedent of the property. Since

$$a{\cdot}2^{k\cdot i'} + b{\cdot}2^{k\cdot i} + t \overset{8.1.12(6)}{=} (a{\cdot}2^k + b){\cdot}2^{k\cdot i} + t \ ,$$

we have

$$(a{\cdot}2^{k\cdot i'}{+}b{\cdot}2^{k\cdot i}{+}t)_i^{[k]} = (a{\cdot}2^{k\cdot i'}{+}b{\cdot}2^{k\cdot i}{+}t){\div}2^{k\cdot i} \bmod 2^k = (a{\cdot}2^k{+}b) \bmod 2^k = b \, .$$

(3): Assume $s < 2^{k\cdot j}$ and $i < j$, i.e. $j = i + n'$ for some n. We have $s = b{\cdot}2^{k\cdot i} + t$ for some $b < 2^k$ and $t < 2^{k\cdot i}$. We then obtain

$$\begin{aligned}(a{\cdot}2^{k\cdot j}{+}s)_i^{[k]} &\overset{8.1.12(6)}{=} ((a{\cdot}2^{k\cdot n}){\cdot}2^{k\cdot i'} + b{\cdot}2^{k\cdot i} + t)_i^{[k]} \overset{(2)}{=} b \overset{(2)}{=} \\ &\quad (0{\cdot}2^{k\cdot i'} + b{\cdot}2^{k\cdot i} + t)_i^{[k]} = (s)_i^{[k]} \ .\end{aligned}$$

8.2.3 Extensions by primitive recursion. Let T be a proper extension of PA and $\tau_1[\vec{y}]$, $\tau_2[x, \vec{y}, v]$ terms of $\mathcal{L}_T$ with free variables among the indicated ones and where $\vec{y}$ is an n-tuple of variables ($n \geq 0$). The extension of the theory T into S with a new $(n + 1)$-ary function symbol f and with the axioms universal closures of

$$f(0, \vec{y}) = \tau_1[\vec{y}] \tag{1}$$

$$f(x', \vec{y}) = \tau_2[x, \vec{y}, f(x, \vec{y})] \tag{2}$$

$$I_x(\phi[x, \vec{y}, f(x, \vec{y})]) \ . \tag{3}$$

is called *extension by primitive recursion*. The formula $\phi[x, \vec{y}, z]$, which is of $\mathcal{L}_T$ and with all free variables indicated, will be effectively determined in Par. 8.2.6 as a graph of the function f. The formula is used in the induction axiom (3) which is the sole induction axiom of S containing the function symbol f.

We keep the notation introduced in this paragraph fixed until the end of the section where we prove in Thm. 8.2.7 that S is an extension by definition of T.

8.2.4 The outline of extensions. Pursuing our plan of introducing the function f into the theory S we first extend T to T_1 by definitions to contain the exponentiation function 2^x and the bounded indexing function $(s)_i^{[k]}$ if not already in T.

We plan to extend T_1 to T_2 by explicitly defining a a predicate Fs such that when f will be introduced into S we will have

$$Fs(k, s, x, \vec{y}) \leftrightarrow \exists k(s \bmod 2^{k \cdot x'} = \sum_{i \le x} f(i, \vec{y}) \cdot 2^{k \cdot i} \wedge \forall(i \le x \rightarrow f(i, \vec{y}) < 2^k))$$

in the standard model of S. The third argument s of Fs is a course of values sequence for the computation of f coded in the base 2^k representation.

The function f can be then introduced into S_1 by implicit definition which is equivalent to

$$S_1 \vdash \exists k \exists s(Fs(k, s, x, \vec{y}) \wedge (s)_x^{[k]} = f(x, \vec{y})) \ . \tag{1}$$

8.2.5 Course of values sequences for f. We extend T_1 to T_2 by an explicit definition of an $(n+3)$-ary predicate Fs:

$$T_2 \vdash Fs(k, s, x, \vec{y}) \leftrightarrow (s)_0^{[k]} = \tau_1[\vec{y}] \wedge \forall i(i < x \rightarrow (s)_{i+1}^{[k]} = \tau_2[i, \vec{y}, (s)_i^{[k]}]) \ . \tag{1}$$

Clearly, $Fs(k, s, x, \vec{y})$ holds in the standard model of T_2 iff s codes in the 2^k-representation the course of values sequence for $f(x, \vec{y})$ provided $f(i, \vec{y}) < 2^k$ holds for all $i \le x$.

The following properties of Fs express the fact that course of values sequences can be constructed for all arguments x, $\vec{y}$:

$$T_2 \vdash \tau_1[\vec{y}] < 2^k \to Fs(k, \tau_1[\vec{y}], 0, \vec{y}) \wedge (\tau_1[\vec{y}])^{[k]}_0 = \tau_1[\vec{y}] \tag{2}$$

$$T_2 \vdash Fs(k, s, x, \vec{y}) \wedge s{<}2^{k\cdot x'} \wedge a = \tau_2[x, \vec{y}, (s)^{[k]}_x]{<}2^k \to Fs(k, a{\cdot}2^{k\cdot x'}{+}s, x', \vec{y}) \tag{3}$$

$$T_2 \vdash Fs(k, a{\cdot}2^{k\cdot x'}{+}s, x', \vec{y}) \wedge s < 2^{k\cdot x'} \to Fs(k, s, x, \vec{y})\ . \tag{4}$$

$$T_2 \vdash \forall s_1 \forall s_2 \forall i (Fs(k_1, s_1, x, \vec{y}) \wedge Fs(k_2, s_2, x, \vec{y}) \wedge i \le x \to (s_1)^{[k_1]}_i = (s_2)^{[k_2]}_i) \tag{5}$$

$$T_2 \vdash \forall k_1 \forall k_2 (\exists s Fs(k_1, s, x, \vec{y}) \wedge k_1{\le}k_2 \to \exists s(s{<}2^{k_2\cdot x'} \wedge Fs(k_2, s, x, \vec{y})))\ . \tag{6}$$

(2): If $\tau_1[\vec{y}] < 2^k$ then, since $\tau_1[\vec{y}] = 0{\cdot}2^{k\cdot 1} + \tau_1[\vec{y}]{\cdot}2^{k\cdot 0} + 0$, we have $(\tau_1[\vec{y}])^{[k]}_0 = \tau_1[\vec{y}]$ by 8.2.2(2) and so $Fs(k, \tau_1[\vec{y}], 0, \vec{y})$ holds by (1).

(3): Assume the antecedent of the property and set $t = a{\cdot}2^{k\cdot x'}{+}s$. Since, $0 < x'$, we have

$$(t)^{[k]}_0 \overset{8.2.2(3)}{=} (s)^{[k]}_0 \overset{Fs(k,s,x,\vec{y})}{=} \tau_1[\vec{y}]\ .$$

For $i = x < x'$ we have

$$(t)^{[k]}_{i+1} \overset{8.2.2(2)}{=} a = \tau_2[i, \vec{y}, (s)^{[k]}_i] \overset{8.2.2(3)}{=} \tau_2[i, \vec{y}, (t)^{[k]}_i]$$

and for any $i < x < x'$ we have

$$(t)^{[k]}_{i+1} \overset{8.2.2(3)}{=} (s)^{[k]}_{i+1} \overset{Fs(k,s,x,\vec{y})}{=} \tau_2[i, \vec{y}, (s)^{[k]}_i] \overset{8.2.2(3)}{=} \tau_2[i, \vec{y}, (t)^{[k]}_i]\ .$$

(4): For $t = a{\cdot}2^{k\cdot x'}{+}s$ and $s < 2^{k\cdot x'}$ assume $Fs(k, t, x', \vec{y})$. Since $0 < x'$, we have

$$(s)^{[k]}_0 \overset{8.2.2(3)}{=} (t)^{[k]}_0 \overset{Fs(k,t,x',\vec{y})}{=} \tau_1[\vec{y}]$$

and for any $i < x < x'$ we have

$$(s)^{[k]}_{i+1} \overset{8.2.2(3)}{=} (t)^{[k]}_{i+1} \overset{Fs(k,t,x',\vec{y})}{=} \tau_2[i, \vec{y}, (t)^{[k]}_i] \overset{8.2.2(3)}{=} \tau_2[i, \vec{y}, (s)^{[k]}_i]\ .$$

But this means that $Fs(k, s, x, \vec{y})$ holds.

(5): By induction on x. In the base case take any s_1, s_2, and $i \le 0$, i.e. $i = 0$, s.t. $Fs(k_1, s_1, 0, \vec{y})$, and $Fs(k_2, s_2, 0, \vec{y})$ holds. We then have

$$(s_1)^{[k_1]}_0 \overset{Fs(k_1,s_1,0,\vec{y})}{=} \tau_1[\vec{y}] \overset{Fs(k_2,s_2,0,\vec{y})}{=} (s_2)^{[k_2]}_0\ .$$

In the inductive case take any s_1, s_2, and $i < x'$ s.t. $Fs(k_1, s_1, x', \vec{y})$, and $Fs(k_2, s_2, x', \vec{y})$. We have $s_1 = a_1{\cdot}2^{k_1\cdot x'} + t_1$, $t_1 < 2^{k_1\cdot x'}$ and $s_2 = a_2{\cdot}2^{k_2\cdot x'} + t_2$, $t_2 < 2^{k_2\cdot x'}$ for some a_1, a_2, t_1 and t_2. We then get $Fs(k_1, t_1, x, \vec{y})$ and $Fs(k_2, t_2, x, \vec{y})$ by (4). We now consider two cases for i. If $i \le x < x'$ then

$$(s_1)^{[k_1]}_i \overset{8.2.2(3)}{=} (t_1)^{[k_1]}_i \overset{\text{IH}}{=} (t_2)^{[k_2]}_i \overset{8.2.2(3)}{=} (s_2)^{[k_2]}_i\ .$$

If $i = x'$ then we have

$$(s_1)_{x+1}^{[k_1]} \overset{Fs(k_1,s_1,x',\vec{y})}{=} \tau_2[x,\vec{y},(s_1)_x^{[k_1]}] \overset{\mathrm{IH}}{=} \tau_2[x,\vec{y},(s_2)_x^{[k_2]}] \overset{Fs(k_2,s_2,x',\vec{y})}{=} (s_2)_i^{[k_2]} \ .$$

(6): By induction on x. In the base case take any k_1, k_2 s.t. $k_1 \leq k_2$ and $Fs(k_1,s_1,0,\vec{y})$ for some s_1. We then have

$$2_2^k \overset{8.1.12(5)}{\geq} 2_1^k > (s_1)_0^{[k_1]} = \tau_1[\vec{y}]$$

and for $s_2 = \tau_1[\vec{y}]$ we obtain $Fs(k_2,s_2,0,\vec{y})$ by (2).

In the inductive case take any k_1, k_2 s.t. $k_1 \leq k_2$ and $Fs(k_1,s_1,x',\vec{y})$ for some s_1. We have $s_1 = a{\cdot}2^{k_1\cdot x'} + t_1$ for some a and $t_1 < 2^{k_1\cdot x'}$. Thus $Fs(k_1,t_1,x,\vec{y})$ by (4) and $Fs(k_2,t,x,\vec{y})$ for some $t < 2^{k_2\cdot x'}$ by IH. We have

$$2^{k_2} \overset{8.1.12(5)}{\geq} 2_1^k > (s_1)_{x+1}^{[k_1]} \overset{Fs(k_1,s_1,x',\vec{y})}{=} \tau_2[x,\vec{y},(s_1)_x^{[k_1]}] \overset{8.2.2(3)}{=}$$
$$\tau_2[x,\vec{y},(t_1)_x^{[k_1]}] \overset{(5)}{=} \tau_2[x,\vec{y},(t)_x^{[k_2]}] \ .$$

We set $s := \tau_2[x,\vec{y},(t)_x^{[k_2]}]{\cdot}2^{k_2\cdot x'} + t$ and obtain $Fs(k_2,s,x',\vec{y})$ by (3) together with:

$$s = \tau_2[x,\vec{y},(t)_x^{[k_2]}]{\cdot}2^{k_2\cdot x'} + t < \tau_2[x,\vec{y},(t)_x^{[k_2]}]{\cdot}2^{k_2\cdot x'} + 2^{k_2\cdot x'} =$$
$$(\tau_2[x,\vec{y},(t)_x^{[k_2]}]+1){\cdot}2^{k_2\cdot x'} \leq 2^{k_2}{\cdot}2^{k_2\cdot x'} \overset{8.1.12(6)}{=} 2^{k_2\cdot x''} \ .$$

8.2.6 The graph ϕ of the function f. We could now extend T_2 to S_1 by the implicit definition of f:

$$S_1 \vdash \exists k \exists s(Fs(k,s,x,\vec{y}) \land (s)_x^{[k]} = f(x,\vec{y})) \tag{1}$$

but we will instead equivalently extend T in Thm. 8.2.7 with the help of a formula $\phi[x,\vec{y},z]$ of $\mathcal{L}_T$ which is a graph of f. Since T_2 is an extension by definitions of T, the formula ϕ is effectively obtained by translation from the formula

$$\exists k \exists s(Fs(k,s,x,\vec{y}) \land (s)_x^{[k]} = z)$$

of T_2 in such a way that we have

$$T_2 \vdash \phi[x,\vec{y},z] \leftrightarrow \exists k \exists s(Fs(k,s,x,\vec{y}) \land (s)_x^{[k]} = z) \ . \tag{2}$$

by the Theorem on Extensions by definitions 6.6.2. We will need in the proof of Thm. 8.2.7 the following properties of the formula:

$$T \vdash \phi[0,\vec{y},\tau_1[\vec{y}]] \tag{3}$$
$$T \vdash \phi[x,\vec{y},z] \to \phi[x',\vec{y},\tau_2[x,\vec{y},z]] \tag{4}$$
$$T \vdash \exists z \phi[x,\vec{y},z] \tag{5}$$
$$T \vdash \phi[x,\vec{y},z_1] \land \phi[x,\vec{y},z_2] \to z_1 = z_2 \ . \tag{6}$$

In the following proofs we work in T_2 and use the equivalence (2) without explicitly referring to it. Properties (3) through (6) are thus derived in T_2 but, since they all are in the language $\mathcal{L}_T$, they are also theorems of T because T_2 is conservative over T.

(3): We set $k = \tau_1[\vec{y}]$. Since $\tau_1[\vec{y}] < 2^k$ by 8.1.12(4), we get $Fs(k, \tau_1[\vec{y}], 0, \vec{y})$ and $(\tau_1[\vec{y}])_0^{[k]} = \tau_1[\vec{y}]$ by 8.2.5(2). We thus have $\phi[0, \vec{y}, \tau_1[\vec{y}]]$.

(4): We assume $\phi[x, \vec{y}, z]$, i.e. $Fs(k_1, t_1, x, \vec{y})$ and $(t_1)_x^{[k_1]} = z$ for some k_1 and t_1. We set $k := \max(k_1, \tau_2[x, \vec{y}, z])$ and, since $k_1 \leq k$, we obtain a $t < 2^{k \cdot x'}$ s.t. $Fs(k, t, x, \vec{y})$ by 8.2.5(6). We have $z = (t_1)_x^{[k_1]} = (t)_x^{[k]}$ by 8.2.5(5) and so

$$2^k \overset{8.1.12(5)}{\geq} 2^{\tau_2[x,\vec{y},z]} \overset{8.1.12(4)}{>} \tau_2[x, \vec{y}, z] = \tau_2[x, \vec{y}, (t)_x^{[k]}] \ .$$

Thus by setting $s := \tau_2[x, \vec{y}, (t)_x^{[k]}] \cdot 2^{k \cdot x'} + t$, we obtain $Fs(k, s, x', \vec{y})$ by 8.2.5(3) and $(s)_{x'}^{[k]} = \tau_2[x, \vec{y}, (t)_x^{[k]}] = \tau_2[x, \vec{y}, z]$ by 8.2.2(2). Hence $\phi[x', \vec{y}, \tau_2[x, \vec{y}, z]]$.

(5): By induction on x. The base case is implied by (3). In the inductive case we have $\phi[x, \vec{y}, z]$ for some z by IH, we get $\phi[x', \vec{y}, \tau_2[x, \vec{y}, z]]$ by (4), and it suffices to set $z := \tau_2[x, \vec{y}, z]$.

(6): We assume $\phi[x, \vec{y}, z_1]$ and $\phi[x, \vec{y}, z_2]$, i.e. $Fs(k_1, s_1, x, \vec{y})$, $(s_1)_x^{[k_1]} = z_1$, $Fs(k_2, s_2, x, \vec{y})$, and $(s_2)_x^{[k_2]} = z_2$ for some k_1, k_2, s_1, s_2. We then obtain

$$z_1 = (s_1)_x^{[k_1]} \overset{8.2.5(5)}{=} (s_2)_x^{[k_2]} = z_2 \ .$$

8.2.7 Theorem (Extensions by primitive recursion). *If T is a proper extension of PA then an extension of T by primitive recursion is an extension by definition.*

Proof. Let S be an extension of T by primitive recursion as in Par. 8.2.3 and S_1 an extension of T by implicit definition with the defining axiom an universal closure of $\phi[x, \vec{y}, f(x, \vec{x})]$. We have $\mathcal{L}_{S_1} = \mathcal{L}_S$ and S_1 is an extension by definition of T by Thm. 6.6.3 because T proves the existence 8.2.6(5) and uniqueness 8.2.6(6) conditions for f. Clearly

$$S_1 \vdash \phi[x, \vec{y}, f(x, \vec{y})] \ . \qquad (1)$$

In order to prove the theorem it suffices to prove that the theories S and S_1 are equivalent.

We prove first $S_1 \vdash S$. First of all, S_1 proves 8.2.3(1), i.e. $S_1 \vdash f(0, \vec{y}) = \tau_1[\vec{y}]$, because we have $\phi[0, \vec{y}, f(0, \vec{y})]$ by (1) and $\phi[0, \vec{y}, \tau_1[\vec{y}]]$ by 8.2.6(3). Thus $f(0, \vec{y}) = \tau_1[\vec{y}]$ by 8.2.6(6).

Secondly, S_1 proves 8.2.3(2), i.e. $S_1 \vdash f(x', \vec{y}) = \tau_2[x, \vec{y}, f(x, \vec{y})]$, because we have $\phi[x, \vec{y}, f(x, \vec{y})]$ and $\phi[x', \vec{y}, f(x', \vec{y})]$, by (1) and $\phi[x', \vec{y}, \tau[x, \vec{y}, f(x, \vec{y})]]$ by 8.2.6(4). Hence $f(x', \vec{y}) = \tau[x, \vec{y}, f(x, \vec{y})]$ by 8.2.6(6).

Finally, since S_1 is proper, it also proves the induction axiom 8.2.3(3) of S: $I_x \phi[x, \vec{y}, f(x, \vec{y})]$.

Vice versa, in order to prove $S \vdash S_1$ it suffices to show $S \vdash \phi[x, \vec{y}, f(x, \vec{y})]$. This is done by working in S and by using the induction axiom 8.2.3(3) of S. In the base case we have $\phi[0, \vec{y}, \tau_1[\vec{y}]]$ by 8.2.6(3) and hence $\phi[0, \vec{y}, f(0, \vec{y})]$ by 8.2.3(1). In the inductive case we have $\phi[x, \vec{y}, f(x, \vec{y})]$ by IH, from which we get $\phi[x', \vec{y}, \tau_2[x, \vec{y}, f(x, \vec{y})]]$ by 8.2.6(4), and hence $\phi[x', \vec{y}, f(x', \vec{y})]$ by 8.2.3(2). $\square$

8.3 Suitable Pairing Function

Our main task in this section will be to introduce the suitable pairing function from Par. 1.3.11 into PA and prove its properties 1.3.7(1) through 1.3.7(3) as theorems.

8.3.1 Dyadic size function $|x|_d$. We will introduce our suitable pairing function by arithmetizing the binary trees from Fig. 1.2 in the dyading notation.

Toward that end we introduce into PA the dyadic size function (see Par. 1.3.4) by minimalization:

$$\vdash_{\mathrm{PAx}} |x|_d = \mu_n[x + 1 < 2^{n+1}] \tag{1}$$

whose existence condition $\vdash_{\mathrm{PA}} \exists n\, x + 1 < n + 1$ is proved by taking $n := x$ and using 8.1.12(4). The defining axiom for the dyadic size function implies:

$$\vdash_{\mathrm{PA}} x + 1 < 2^{|x|_d+1} \tag{2}$$

$$\vdash_{\mathrm{PA}} n < |x|_d \to 2^{n+1} \leq x + 1 \tag{3}$$

and the function satisfies:

$$\vdash_{\mathrm{PA}} |x|_d > 0 \leftrightarrow x > 0 \tag{4}$$

$$\vdash_{\mathrm{PA}} |x|_d = n \leftrightarrow 2^n \leq x + 1 < 2^{n+1} \ . \tag{5}$$

(4): If $0 < |x|_d$ then $2^1 \leq x{+}1$ by (3) and so $1 \leq x$. Vice versa, if $0 < x$ then we cannot have $|x|_d = 0$ because we would then get $2 \leq x + 1 \overset{(2)}{<} 2^{0+1} = 2$.

(5): In the direction ($\to$) assume $|x|_d = n$ and consider two cases. If $n = 0$ then $x = 0$ by (4) and we have $2^0 = 1 \leq 0 + 1 < 2 = 2^{0+1}$. If $n > 0$ then

$$2^n = 2^{n \dot{-} 1+1} \overset{(3)}{\leq} x + 1 \overset{(2)}{<} 2^{n+1} \ .$$

In the direction ($\to$) assume $2^n \leq x + 1 < 2^{n+1}$ and consider three cases. If $n < |x|_d$ then we get a contradiction

$$2^{n+1} \overset{(3)}{\leq} x + 1 < 2^{n+1} \ .$$

If $n = |x|_d$ there is nothing to prove. If $|x|_d < n$ then $|x|_d + 1 \leq n$ and we get a contradiction:

$$x + 1 \overset{(2)}{<} 2^{|x|_d+1} \overset{8.1.12(5)}{\leq} 2^n \leq x + 1 \ .$$

8.3.2 Dyadic concatenation function $x \star y$. We will also need the dyadic concatenation function $x \star y$ (see Par. 1.3.5) which is explicitly introduced into PA as follows:

$$\vdash_{\mathrm{PAx}} x \star y = x{\cdot}2^{|y|_d} + y \tag{1}$$

The concatenation function satisfies the following:

$$\vdash_{\mathrm{PA}} x = 0 \star x \wedge x = x \star 0 \tag{2}$$
$$\vdash_{\mathrm{PA}} |x \star y|_d = |x|_d + |y|_d \tag{3}$$
$$\vdash_{\mathrm{PA}} (x \star y) \star z = x \star (y \star z) \tag{4}$$
$$\vdash_{\mathrm{PA}} n \le |x|_d \to \exists a \exists b (x = a \star b \wedge |b|_d = n) \tag{5}$$
$$\vdash_{\mathrm{PA}} a \star b = c \star d \wedge |b|_d = |d|_d \to a = c \wedge b = d\ . \tag{6}$$

(2): We have $0 \star x = 0{\cdot}2^{|x|_d} + x = x$ and $x \star 0 = x{\cdot}2^{|0|_d} + 0 \overset{8.3.1(4)}{=} x{\cdot}2^0 + 0 = x$.

(3): We have $2^{|x|_d} \le x + 1$ by 8.3.1(5). Since $2^{|y|_d} > 0$, we get

$$2^{|x|_d + |x|_d} = 2^{|x|_d}{\cdot}2^{|y|_d} \le x{\cdot}2^{|y|_d} + 2^{|y|_d} \overset{8.3.1(5)}{\le} x{\cdot}2^{|y|_d} + y + 1 = (x \star y) + 1\ .$$

We have $x + 1 < 2^{|x|_d + 1}$, i.e. $x + 2 \le 2{\cdot}2^{|x|_d}$, by 8.3.1(5). Since $2^{|y|_d} > 0$, we get

$$(x \star y) + 1 = x{\cdot}2^{|y|_d} + y + 1 \overset{8.3.1(5)}{<} x{\cdot}2^{|y|_d} + 2{\cdot}2^{|y|_d} \le 2{\cdot}2^{|x|_d}{\cdot}2^{|y|_d} = 2^{|x|_d + |x|_d + 1}\ .$$

Combining the two inequalities we obtain $|x \star y|_d = |x|_d + |x|_d$ by 8.3.1(5).

(4): We have

$$(x \star y) \star z = (x{\cdot}2^{|y|_d} + y){\cdot}2^{|z|_d} + z = x{\cdot}2^{|y|_d + |z|_d} + y{\cdot}2^{|z|_d} + z \overset{(3)}{=}$$
$$x{\cdot}2^{|y \star z|_d} + (y \star z) = x \star (y \star z)\ .$$

(5): Assume $n \le |x|_d$. We have

$$2^n \overset{8.1.12(5)}{\le} 2^{|x|_d} \overset{8.3.1(5)}{\le} x + 1$$

and for $a = (x + 1 \dot{-} 2^n) \div 2^n$, $c = (x + 1 \dot{-} 2^n) \bmod 2^n$ we get $x + 1 \dot{-} 2^n = a{\cdot}2^n + c$, $c < 2^n$ by 7.4.8(1). For $b = 2^n \dot{-} 1 + c$ we then get $x = a{\cdot}2^n + b$. We have $2^n \le 2^n + c < 2{\cdot}2^n$, i.e. $2^n \le b + 1 < 2^{n+1}$. Hence $|b|_d = n$ by 8.3.1(5) and thus $x = a \star b$.

(6): Assume $a \star b = c \star d$ and $|b|_d = |d|_d$. Thus

$$a{\cdot}2^{|d|_d} + b = a{\cdot}2^{|b|_d} + b = a \star b = c \star d = c{\cdot}2^{|d|_d} + d$$

and we get $a = c$, $b = d$ by 7.4.8(1)(2).

In the following we will use the associativity of the concatenation operation (4) without explicitly referring to it.

8.3.3 Counting function $\#(x)$. For the arithmetization of binary trees we will need a unary *counting* function $\#(x)$ yielding the number of digits $\mathbf{2}$ in the dyadic representation of x.

The counting function is introduced with the help of an auxiliary binary *dyadic indexing function* $[x]_i$ yielding the i-th dyadic digit in the dyadic representation of x decreased by one where the least significant digit is with the index 0. We intend to introduce the function into PA by contextual definition:

$$[x]_i = z \leftrightarrow \exists a \exists b(x = a \star (z+1) \star b \wedge z \leq 1 \wedge |b|_d = i) \vee i \geq |x|_d \wedge z = 0 \ . \tag{1}$$

Its existence condition follows from (2), (3) and its uniqueness condition from (4), (5):

$$\vdash_{\text{PA}} i < |x|_d \rightarrow \exists z \exists a \exists b(x = a \star (z+1) \star b \wedge z \leq 1 \wedge |b|_d = i) \tag{2}$$

$$\vdash_{\text{PA}} i \geq |x|_d \rightarrow \exists z\, z = 0 \tag{3}$$

$$\begin{aligned}\vdash_{\text{PA}}\ & x = a_1 \star (z_1+1) \star b_1 \wedge z_1 \leq 1 \wedge |b_1|_d = i \wedge \\ & \quad x = a_2 \star (z_2+1) \star b_2 \wedge z_1 \leq 1 \wedge |b_2|_d = i \rightarrow i < |x|_d \wedge z_1 = z_2\end{aligned} \tag{4}$$

$$\vdash_{\text{PA}} z_1 = 0 \wedge z_2 = 0 \rightarrow z_1 = z_2 \ . \tag{5}$$

(2): Assume $i < |x|_d$ and get $x = c \star b$ for some b, c such that $|b|_d = i$ by 8.3.2(5). We have $|x|_d = |c|_d + i$ by 8.3.2(3). Thus $1 \leq |c|_d$ and we get $c = a \star y$ for some a, y such that $|y|_d = 1$ by 8.3.2(5) again. We have $2^1 \leq y+1 < 2^2$ and so $1 \leq y \leq 2$ by 8.3.1(5). Hence $y = z+1$ for a z s.t. $z \leq 1$.

(3): This is trivial.

(4): Assume the antecedent. We get $b_1 = b_2$, and $a_1 \star (z_1+1) = a_2 \star (z_2+1)$ by 8.3.2(6). Since $|z_1+1|_d = 1 = |z_2+1|_d$ by 8.3.1(5), we get $a_1 = a_2$ and $z_1 = z_2$ by 8.3.2(6) again. We have $|x|_d = |a_1|_d + 1 + i$ by 8.3.2(3) and so $i < |x|_d$.

(5): This is trivial.

We will need the following simple properties of the dyadic indexing function:

$$\vdash_{\text{PA}} i < |b|_d \rightarrow [a \star b]_i = [b]_i \tag{6}$$

$$\vdash_{\text{PA}} [a \star b]_{i+|b|_d} = [a]_i \tag{7}$$

(6): Assume $i < |b|_d$ and obtain $b = b_1 \star (z+1) \star b_2$ for some b_1, b_2, $z \leq 1$ such that $|b_2|_d = i$ by (2). Since also $a \star b = (a \star b_1) \star (z+1) \star b_2$, we obtain $[b]_i = z = [a \star b]_i$ by (1).

(7): Consider two cases. If $i \geq |a|_i$ then also $i + |b|_d \geq |a|_i + |b|_d \overset{8.3.2(3)}{=} |a \star b|_s$ and we have $[a \star b]_{i+|b|_d} = 0 = [a]_i$ by (1). If $i < |a|_i$ then also $i + |b|_d < |a \star b|$ and we have $a = a_1 \star (z+1) \star a_2$ for some $a_1, a_2, z \leq 1$ such that $|a_2|_d = i$ by (2). Since also $a \star b = a_1 \star (z+1) \star (a_2 \star b)$ with $|a_2 \star b|_d = i + |b|_d$, we have $[a \star b]_{i+|b|_d} = z = [a]_i$ by (1) again.

We also need an auxiliary binary function f which is introduced into PA by primitive recursion:

$$\vdash_{\text{PAx}} f(0,x)=0 \tag{8}$$
$$\vdash_{\text{PAx}} f(i',x)=[x]_i+f(i,x)\ . \tag{9}$$

We will need the following properties of f:

$$\vdash_{\text{PA}} \forall a\forall b(i\le |b|_d \to f(i,a\star b)=f(i,b)) \tag{10}$$
$$\vdash_{\text{PA}} \forall a\forall b\, f(i+|b|_d,a\star b)=f(i,a)+f(|b|_d,b)\ . \tag{11}$$

(10): By induction on i. In the base case we have $f(0,a\star b)=0=f(0,b)$. In the inductive case we assume $i+1\le |b|_d$ and, since $i<|b|_d$, we obtain:

$$f(i+1,a\star b)=[a\star b]_i+f(i,a\star b)\overset{\text{IH}}{=}$$
$$[a\star b]_i+f(i,b)\overset{(6)}{=}[b]_i+f(i,b)=f(i+1,b)\ .$$

(11): By induction on i. In the base case we have

$$f(0+|b|_d,a\star b)=f(|b|_d,a\star b)\overset{(10)}{=}f(|b|_d,b)=f(0,a)+f(|b|_d,b)\ .$$

In the inductive case we have:

$$f(i+1+|b|_d,a\star b)=[a\star b]_{i+|b|_d}+f(i+|b|_d,a\star b)\overset{\text{IH}}{=}$$
$$[a\star b]_{i+|b|_d}+f(i,a)+f(|b|_d,b)\overset{(7)}{=}$$
$$[a]_i+f(i,a)+f(|b|_d,b)=f(i+1,a)+f(|b|_d,b)\ .$$

We introduce the function $\#(x)$ into PA by explicit definition:

$$\vdash_{\text{PAx}} \#(x)=f(|x|_d,x) \tag{12}$$

The counting function has the following properties which we will need below:

$$\vdash_{\text{PA}} \#(0)=0 \tag{13}$$
$$\vdash_{\text{PA}} \#(1)=0 \tag{14}$$
$$\vdash_{\text{PA}} \#(2)=1 \tag{15}$$
$$\vdash_{\text{PA}} \#(a\star b)=\#(a)+\#(b)\ . \tag{16}$$

(13): $\#(0)=f(|0|_d,0)\overset{8.3.1(4)}{=}f(0,0)=0$.

(14): We have $\#(1)=f(|1|_d,1)\overset{8.3.1(5)}{=}f(1,1)=[1]_0+f(0,0)=[1]_0$ and, since $1\overset{8.3.2(2)}{=}0\star(0+1)\star 0$, $|0|_d\overset{8.3.1(4)}{=}0$, we get $[1]_0=1$ by (1).

(15): Similarly as (14).

(16): We have

$$\#(a\star b)=f(|a\star b|_d,a\star b)\overset{8.3.2(3)}{=}f(|a|_d+|b|_d,a\star b)\overset{(11)}{=}$$
$$f(|a|_d,a)+f(|b|_d,b)=\#(a)+\#(b)\ .$$

Prefix Codes

We will define a subset *Prf* of natural numbers which code in the dyadic notation the binary trees from Fig. 1.2 expressed in the prefix notation.

8.3.4 Prefix notation of pair numerals. Recall that every pair numeral is either 0 or it has a form (τ_1, τ_2) for pair numerals τ_1 and τ_2. The right parentheses and commas in pair numerals are superfluous in the sense that when we omit them we are still able to represent every natural number uniquely.

The sequences of words over the two element alphabet (and 0 obtained in this way from pair numerals represent the same numbers as pair numerals in the (Polish) *prefix* notation. Thus the number zero 0 is represented by the pair numeral 0 and the prefix notation 0. The number 1 is represented by the pair numeral $(0, 0)$ and by the prefix notation (00. The number 2 is denoted by the pair numeral $(0, (0, 0))$ and by the prefix notation (0(00. The number 3 is denoted by the pair numeral $((0, 0), 0)$ and by the prefix notation ((000, and so on.

The reader will note that every number x with the pair size $|x|_p = n$ is represented by the prefix word of length $2{\cdot}n + 1$ which contains exactly n left parentheses and $n + 1$ zeroes. However, not every such word is a prefix notation. For instance out of $\binom{5}{2} = 10$ words of length 5 six words 0(00(, (00(0, 00(0(, 0(0(0 (000(, 000((, 00((0, and 0((00 are not prefix notations. It can be shown that there are

$$\frac{1}{2{\cdot}n+1}{\cdot}\binom{2{\cdot}n+1}{n} = \frac{1}{n+1}{\cdot}\binom{2{\cdot}n}{n}$$

prefix notations of numbers with the pair size n out of $\binom{2{\cdot}n+1}{n}$ possible words with n symbols (and $n + 1$ symbols 0.

A moment of thought shows that the word w with n symbols (and $n+1$ symbols 0 is a prefix notation iff for all $w = w_1 w_2$ where w_2 is not empty the count i of symbols (in w_2 is less than the count j of 0. We clearly have $i < j$ iff the size of w_2 is greater than $2{\cdot}i$, i.e. iff $i + j > 2{\cdot}i$.

The plan for the introduction of the pairing function x, y is as follows. We will first arithmetize (code) the prefix notation in the dyadic representation in Par. 8.3.5. We will then define a pairing function over prefix codes in Par. 8.3.6. We will well-order the prefix codes by a relation $<_p$ defined in Par. 8.3.8. We will then enumerate the prefix codes by a function π in Par. 8.3.13 such that $<$ and $<_p$ will be isomorphic. The isomorphism then defines in Par. 8.3.14 the pairing function x, y as the isomorphic image of the pairing function on the prefix codes.

8.3.5 Prefix codes. We arithmetize the prefix notation by coding into natural numbers where in the dyadic representation the symbol (is coded by the digit 2 and the symbol 0 by the digit 1. The unary predicate $\mathit{Prf}(x)$ holding iff x codes the prefix code of length $|x|_d$ is introduced into PA by explicit definition:

$$\vdash_{\mathrm{PAx}} \mathit{Prf}(x) \leftrightarrow |x|_d = 2{\cdot}\#(x) + 1 \wedge \forall a \forall b(x = a \star b \wedge b > 0 \to |b|_d > 2{\cdot}\#(b)) \tag{1}$$

We have

$$\vdash_{\mathrm{PA}} |x|_d > 2{\cdot}\#(x) \to \exists v \exists b(x = v \star b \wedge \mathit{Prf}(v)) \tag{2}$$

$$\vdash_{\mathrm{PA}} \mathit{Prf}(a \star b) \wedge \mathit{Prf}(a) \to b = 0\ . \tag{3}$$

$$\vdash_{\mathrm{PA}} \mathit{Prf}(x) \wedge \#(x) = 0 \leftrightarrow x = 1\ . \tag{4}$$

(2): Assume $|x|_d > 2{\cdot}\#(x)$ and consider the formula

$$\phi[x,k] \equiv \exists v \exists b(|v|_d = k \wedge x = v \star b \wedge |v|_d > 2{\cdot}\#(v))\ .$$

Since $x = x \star 0$ by 8.3.2(2), we have $\phi[x, |x|_d]$ for $v := x$ and $b := 0$. By the least number principle there is the smallest such k for which there are v and b such that $|v|_d = k$, $x = v \star b$,

$$|v|_d > 2{\cdot}\#(v)\ , \tag{5}$$

and for any $m < k$ we have $\neg\phi[x,m]$, i.e.

$$\forall v_1 \forall b_1(|v_1|_d < |v|_d \wedge x = v_1 \star b_1 \to |v_1|_d \leq 2{\cdot}\#(v_1))\ . \tag{6}$$

In order to prove $\mathit{Prf}(v)$ we assume $v = v_1 \star v_2$ for some v_1, $v_2 > 0$. We have

$$|v_1|_d + |v_2|_d \overset{8.3.2(3)}{=} |v|_d \overset{(5)}{>} 2{\cdot}\#(v) \overset{8.3.3(16)}{=} 2{\cdot}\#(v_1) + 2{\cdot}\#(v_2) \tag{7}$$

and, since $x = v_1 \star (v_2 \star b)$, $|v_1|_d < |v|$, we obtain

$$|v_1|_d \leq 2{\cdot}\#(v_1) \tag{8}$$

by (6). This means that

$$|v_2|_d > 2{\cdot}\#(v_2)\ . \tag{9}$$

It remains to derive $|v|_d = 2{\cdot}\#(v) + 1$. We have $|v|_d > 0$ by (5) and so $v = v_1 \star v_2$ for some v_1, v_2 s.t. $|v_2|_d = 1$ by 8.3.2(5). We then get $\#(v_2) = 0$ by (9) and $|v_1|_d + 1 > 2{\cdot}\#(v_1)$, i.e. $|v_1|_d \geq 2{\cdot}\#(v_1)$, by (7). Thus $|v_1|_d = 2{\cdot}\#(v_1)$ by (8) and hence $|v|_d = |v_1|_d + 1 = 2{\cdot}\#(v) + 1$.

(3): Assume $\mathit{Prf}(a \star b)$ and $\mathit{Prf}(a)$. If it were the case that $b > 0$ then we would have $|b|_d > 2{\cdot}\#(b)$ and we would obtain a contradiction

$$|a \star b|_d \overset{8.3.2(3)}{=} |a|_d + |b|_b = 2{\cdot}\#(a) + 1 + |b|_b > 2{\cdot}\#(a) + 1 + 2{\cdot}\#(b) =$$
$$2{\cdot}(\#(a) + \#(b)) + 1 \overset{8.3.3(16)}{=} 2{\cdot}\#(a \star b) + 1\ .$$

(4): If $Prf(x)$ and $\#(x) = 0$ then $|x|_d = 1$ and we get $x = 1$ or $x = 2$ by 8.3.1(5) and, since $\#(2) = 1$ by 8.3.3(15), it must be the case that $x = 1$.

Vice versa, if $x = 1$ then we have

$$|1|_d \overset{8.3.1(5)}{=} 1 \overset{8.3.3(14)}{=} 2{\cdot}\#(1) + 1 \ .$$

Take any $b > 0$ and a such that $1 = x = a \star b$. We have $1 = |1|_d \overset{8.3.2(3)}{=} |a|_d + |b|_d$ and so $a = 0$ by 8.3.1(4). But then $b = 1$ by 8.3.2(2) and so

$$|b|_d = 1 > 0 \overset{8.3.3(14)}{=} 2{\cdot}\#(b) \ .$$

8.3.6 Pairing function over prefix codes. We define the binary *prefix code pairing* function $x \,{,_p}\, y$ by explicit definition:

$$\vdash_{\mathrm{PAx}} \ x \,{,_p}\, y = 2 \star x \star y \ . \tag{1}$$

The basic properties of the function are that it is over prefix codes and that it satisfies there the pairing property:

$$\vdash_{\mathrm{PA}} \ Prf(x) \land Prf(y) \to Prf(x \,{,_p}\, y) \land \#(x \,{,_p}\, y) = \#(x) + \#(y) + 1 \tag{2}$$

$$\vdash_{\mathrm{PA}} \ Prf(x) \land Prf(v) \land x \,{,_p}\, y = v \,{,_p}\, w \to x = v \land y = w \ . \tag{3}$$

(2): Assume $Prf(x)$ and $Prf(y)$. We have

$$\#(x, {,_p}\, y) = \#(2 \star x \star y) = 1 + \#(x) + \#(y) \tag{4}$$

by the properties of the counting function and

$$|x \,{,_p}\, y|_d = |2 \star x \star y|_d = 1 + |x|_d + |y|_d = \\ 1 + 2{\cdot}\#(x) + 1 + 2{\cdot}\#(y) + 1 \overset{(4)}{=} 2{\cdot}\#(x \,{,_p}\, y) + 1 \tag{5}$$

by the properties of the dyadic size function. We now take any a and $b > 0$ such that $x \,{,_p}\, y = 2 \star x \star y = a \star b$ and, since $|b|_d \le |x \,{,_p}\, y|_d$, we consider three cases for the dyadic size of b:

$|b|_d \le |y|_d$: We have $y = y_1 \star y_2$ for some y_1, y_2 s.t. $|b|_d = |y_2|_d$ by 8.3.2(5), $y_2 = b$ by 8.3.2(6), and $|y_2|_d > 2{\cdot}\#(y_2)$, i.e. $|b|_d > 2{\cdot}\#(b)$, by $Prf(y)$. Hence $Prf(x \,{,_p}\, y)$.

$|y|_d < |b|_d \le |x|_d + |y|_d$: We have $b = b_1 \star b_2$ for some b_1, b_2 s.t. $|y|_d = |b_2|_d$ by 8.3.2(5) and, since $2 \star x \star y = a \star b_1 \star b_2$, we get $2 \star x = a \star b_1$ and $y = b_2$ by 8.3.2(6). From $|y|_d < |b|_d = |b_1|_d + |b_2|_d \le |x|_d + |y|_d$ we get $0 < |b_1|_d \le |x|_d$ and so $b_1 > 0$, by 8.3.1(4). Thus $x = x_1 \star x_2$ for some x_1, x_2 s.t. $|x_2|_d = |b_1|_d$ by 8.3.2(5) and, since $2 \star x_1 \star x_2 = a \star b_1$, we get $x_2 = b_1$ by 8.3.2(6). Now, $|x_2|_d > 2{\cdot}\#(x_2)$ by $Prf(x)$. Hence

$$|b|_d = |b_1 \star b_2|_d = |b_1|_d + |b_2|_d = |x_2|_d + 2{\cdot}m + 1 > 2{\cdot}\#(x_2) + 2{\cdot}m = \\ 2{\cdot}(\#(b_1) + m) = 2{\cdot}(\#(b_1) + \#(b_2)) = 2{\cdot}\#(b)$$

and thus $\mathit{Prf}(x\,,_p\,y)$.

$|b|_d = 1+|x|_d+|y|_d$: We have $0\star(x\,,_p\,y) \overset{8.3.2(2)}{=} x\,,_p\,y = a\star b$, $|x\,,_p\,y|_d = |b|_d$, and hence $x\,,_p\,y = b$ by 8.3.2(6). Thus

$$|b|_d = |x\,,_p\,y|_d \overset{(5)}{=} 2{\cdot}(1+\#(x)+\#(y))+1 > 2{\cdot}(1+\#(x)+\#(y)) \overset{(4)}{=} \\ 2{\cdot}\#(x\,,_p\,y) = 2{\cdot}\#(b)$$

and so $\mathit{Prf}(x\,,_p\,y)$ again.

(3): Assume $\mathit{Prf}(x)$, $\mathit{Prf}(v)$, and $x\,,_p\,y = v\,,_p\,w$. From $2\star x\star y = 2\star v\star w$ we get $|x\star y|_d = |v\star w|_d$ by 8.3.2(3) and then $x\star y = v\star w$ by 8.3.2(6). We now consider two cases. If $|y|_d \le |w|_d$ then we have $w = w_1\star w_2$ for some w_1, w_2 such that $|w_2|_d = |y|_d$ by 8.3.2(5). We obtain $x = v\star w_1$ and $w_2 = y$ by 8.3.2(6). But then $w_1 = 0$ by 8.3.5(3) and so $x = v$ as well as $w = w_2 = y$ by 8.3.2(2). The case $|y|_d \ge |w|_d$ is similar.

Additional property of the prefix code pairing function is that its range is the set of the prefix codes with positive counts of digits **2**:

$$\vdash_{\mathrm{PA}} 1 \ne x\,,_p\,y \tag{6}$$

$$\vdash_{\mathrm{PA}} \mathit{Prf}(x)\wedge\#(x)>0\to\exists v\exists w(x = v\,,_p\,w\wedge \mathit{Prf}(v)\wedge \mathit{Prf}(w))\ . \tag{7}$$

(6): This is because

$$\#(1) \overset{8.3.3(14)}{=} 0 < 1+\#(x\star y) \overset{8.3.3(15)}{=} \#(2)+\#(x\star y) \overset{8.3.3(16)}{=} \\ \#(2\star x\star y) = \#(x\,,_p\,y)\ .$$

(7): Assume $\mathit{Prf}(x)$ and $\#(x) > 0$. Since $2{\cdot}\#(x)+1 = |x|_d$, we have $x = x_1\star x_2$ for some x_1, x_2 s.t. $|x_2|_d = 2{\cdot}\#(x)$ by 8.3.2(5). Thus $|x_1|_d = 1$ by 8.3.2(3). Since $|x_2|_d > 0$ we have $x_2 > 0$ by 8.3.1(4) and from $\mathit{Prf}(x)$ we obtain

$$2{\cdot}\#(x) = |x_2|_d > 2{\cdot}\#(x_2)\ , \tag{8}$$

i.e. $\#(x_1)+\#(x_2) \overset{8.3.3(16)}{=} \#(x) > \#(x_2)$ and so $\#(x_1) > 0$. Since $x_1 = 1$ or $x_1 = 2$ by 8.3.1(5), it must be the case that $x_1 = 2$ by 8.3.3(14). We have $x_2 = v\star w$ for some v, w s.t. $\mathit{Prf}(v)$ by (8) and 8.3.5(2). We have $x = x_1\star x_2 = 2\star v\star w = v\,,_p\,w$ and it suffices to prove $\mathit{Prf}(w)$. For that we note that

$$2+2{\cdot}\#(v)+2{\cdot}\#(w)+1 = 2{\cdot}\#(2\star v\star w)+1 = 2{\cdot}\#(x)+1 = |x|_d = \\ |2\star v\star w|_d = 1+|v|_d+|w|_d = 1+2{\cdot}\#(v)+1+|w|_d$$

by the properties of the dyadic size and counting functions. Hence $2{\cdot}\#(w)+1 = |w|_d$. We now take any $a, b > 0$ such that $w = a\star b$. From $x = (2\star v\star a)\star b$ and $\mathit{Prf}(x)$ we get the desired $|b|_d > 2{\cdot}\#(b)$.

Order on Prefix Codes

We will now define a well-ordering relation $<_p$ on the prefix codes which will impose the structure of $\mathbb{N}$ on the codes.

8.3.7 Indexing properties of prefix codes. Following properties of prefix codes play central role in the definition of the order $<_p$:

$$\vdash_{\mathrm{PA}} \mathit{Prf}(x) \wedge i < |x|_d \to \exists a \exists v \exists b(x = a \star v \star b \wedge |a|_d = i \wedge \mathit{Prf}(v)) \tag{1}$$

$$\vdash_{\mathrm{PA}} \mathit{Prf}(x) \wedge x = a_1 \star v_1 \star b_1 \wedge \mathit{Prf}(v_1) \wedge x = a_2 \star v_2 \star b_2 \wedge \mathit{Prf}(v_2) \wedge$$
$$|a_1|_d = |a_2|_d \to a_1 = a_2 \wedge v_1 = v_2 \wedge b_1 = b_2 \ . \tag{2}$$

Property (1) says that in every prefix code x it is possible to find a prefix code v at an arbitrary distance $i < |x|_d$ from the beginning of x. Property (2) asserts that this v is uniquely determined. We can thus view the number i as an index selecting the *prefix code v at the position i of x.*

(1): Assume $\mathit{Prf}(x)$ and $i < |x|_d$. Since $0 < |x|_d \dot{-} i < |x|_d$, we get $x = a \star c$ for some a, c such that $0 < |c|_d = |x|_d \dot{-} i$ by 8.3.2(5). We have $|a|_d = i$ by 8.3.2(3) and $|c| > \#(c)$ because $\mathit{Prf}(x)$. Thus $c = v \star b$ for some v, b s.t. $\mathit{Prf}(v)$ by 8.3.5(2).

(2): Assume the antecedent of the property. We have $|v_1 \star b_1|_d = |v_2 \star b_2|_d$ by 8.3.2(3) and $a_1 = a_2$, $v_1 \star b_1 = v_2 \star b_2$ by 8.3.2(6). We now consider two cases. If $|b_1|_d \le |b_2|_d$ then $b_2 = c_1 \star c_2$ for some c_1, c_2 such that $|b_1|_d = |c_2|_d$ by 8.3.2(5), $v_1 = v_2 \star c_1$, $b_1 = c_2$ by 8.3.2(6), and $c_1 = 0$ by 8.3.5(3). Thus $v_1 = v_2$ and $b_1 = b_2$ by 8.3.2(2).

The case $|b_1|_d \ge |b_2|_d$ is similar.

8.3.8 Order on prefix codes. We will define $x <_p y$ to hold iff x and y code in the prefix notation binary trees t and s respectively and if in the order from left to right there is a subtree in t with a lesser number of inner nodes than the corresponding subtree in s while all corresponding subtrees to the left are identical and all corresponding ancestors subtrees have equal number of inner nodes.

This seemingly complicated property expresses the first-by-size-than-by-lexicographic-order enumeration of binary trees in Fig. 1.2. The property is arithmetized with the help of two auxiliary ternary predicates $x <_p^i y$ and $x =_p^i y$ introduced into PA by explicit definitions:

$$\vdash_{\mathrm{PAx}} x <_p^i y \leftrightarrow \exists a \exists v_1 \exists b_1 \exists v_2 \exists b_2(x = a \star v_1 \star b_1 \wedge \mathit{Prf}(v_1) \wedge |a|_d = i \wedge$$
$$y = a \star v_2 \star b_2 \wedge \mathit{Prf}(v_2) \wedge \#(v_1) < \#(v_2)) \tag{1}$$

$$\vdash_{\mathrm{PAx}} x =_p^i y \leftrightarrow \exists a \exists v_1 \exists b_1 \exists v_2 \exists b_2(x = a \star v_1 \star b_1 \wedge \mathit{Prf}(v_1) \wedge |a|_d = i \wedge$$
$$y = a \star v_2 \star b_2 \wedge \mathit{Prf}(v_2) \wedge \#(v_1) = \#(v_2)) \ . \tag{2}$$

For two prefix codes x and y we clearly have $x <_p^i y$ ($x =_p^i y$) iff the code at the position i of x has a lesser (equal) dyadic size than the code at the position i of y.

We now explicitly introduce into PA the binary predicate $x <_p y$:

$$\vdash_{\mathrm{PAx}} x <_p y \leftrightarrow Prf(x) \wedge Prf(y) \wedge \exists i(x <_p^i y \wedge \forall j(j < i \rightarrow x =_p^j y)) \tag{3}$$

and prove that it is a linear order over Prf:

$$\vdash_{\mathrm{PA}} Prf(x) \rightarrow x \not<_p x \tag{4}$$
$$\vdash_{\mathrm{PA}} x <_p y \wedge y <_p z \rightarrow x <_p z \tag{5}$$
$$\vdash_{\mathrm{PA}} Prf(x) \wedge Prf(y) \wedge x \neq y \rightarrow x <_p y \vee y <_p x \ . \tag{6}$$

(4): Assume $Prf(x)$ and take any $i < |x|_d$. By Par. 8.3.7 we have $x = a \star v \star b$ for the uniquely determined a, v, b s.t. $|a|_i = i$. We cannot have $\#(v) < \#(v)$, thus $\neg v <_p^i v$, and hence $x \not<_p x$.

(5): Suppose $x <_p y$ and $y <_p z$. We have $Prf(x)$, $Prf(y)$, $Prf(z)$, $x <_p^{i_1} y$, $y <_p^{i_2} z$ for some i_1, i_2 s.t. $i_1 < |x|_d$, $i_1 < |y|_d$, $i_2 < |y|_d$, $i_2 < |z|_d$. In the following we will use obvious transitivity properties of the auxiliary predicates which are direct consequences of the indexing of prefix codes (see Par. 8.3.7). We consider three cases. If $i_1 < i_2$ then for any $j < i_1$ we have $x =_p^j y$, $y =_p^j z$, and hence $x =_p^j z$. From $x <_p^{i_1} y$ and $y =_p^{i_1} z$ we get $x <_p^{i_1} z$. Thus $x <_p z$.

The case when $i_2 < i_1$ is similar, and if $i_1 = i_2$ then we clearly have $x <_p^{i_1} z$ and $x =_p^j z$ for any $j < i_1$. Hence $x <_p y$ again.

(6): Suppose $Prf(x)$, $Prf(y)$, $x \neq y$, and consider three cases. If $|x|_d < |y|_d$ then $x <_p^0 y$ and so $x <_p y$. If $|y|_d < |x|_d$ then $y <_p^0 x$ and so $y <_p x$. Finally, if $|y|_d = |x|_d = k$ then $\neg y =_p^i x$ for some $i < k$ and there is the least such i by the least number principle. We thus have $x =_p^j y$ for all $j < i$ and either $x <_p^i y$ or $y <_p^i x$. Hence $x <_p y$ or $y <_p x$.

8.3.9 Additional properties of $<_p$. We introduce the binary predicate $\leq_p$ by explicit definition:

$$\vdash_{\mathrm{PAx}} x \leq_p y \leftrightarrow x <_p y \vee x = y \wedge Prf(x) \ . \tag{1}$$

The reader will note that $x \leq x$ does not hold if x is not a prefix code.

We now prove the remaining properties of the order on Prf which we will need below:

$$\vdash_{\mathrm{PA}} Prf(x) \wedge Prf(y) \rightarrow \#(x) < \#(y) \rightarrow x <_p y \tag{2}$$
$$\vdash_{\mathrm{PA}} x \leq_p y \rightarrow \#(x) \leq \#(y) \tag{3}$$
$$\vdash_{\mathrm{PA}} Prf(x) \rightarrow 1 \leq_p x \tag{4}$$
$$\vdash_{\mathrm{PA}} Prf(x) \wedge Prf(y) \wedge Prf(v) \wedge Prf(w) \wedge \#(x) + \#(y) = \#(v) + \#(w) \rightarrow$$
$$(x \,,_p y <_p v \,,_p w \leftrightarrow x <_p v \vee x = v \wedge y <_p w) \ . \tag{5}$$

(2): Suppose $Prf(x)$, $Prf(y)$, and $\#(x) < \#(y)$. We have $x <_p^0 y$ and so $x <_p y$.

(3): Suppose $x \leq_p y$. We have $Prf(x)$, $Prf(y)$. If it were the case that $\#(x) > \#(y)$ we would have $y <_p x$ by (2) and $x <_p x$ by 8.3.8(5) thus contradicting 8.3.8(4).

(4): Suppose $Prf(x)$ and consider two cases. If $\#(x) = 0$ then $x = 1$ by 8.3.5(4) and we trivially have $1 \leq_p 1$. If $\#(x) > 0$ then, since $\#(1) = 0$, we have $1 <_p x$ by (2).

(5): Assume the antecedent of the property. We have $Prf(x \,,_p y)$, $Prf(v \,,_p w)$, and

$$\#(x \,,_p y) = \#(x) + \#(v) + 1 = \#(v) + \#(w) + 1 = \#(v \,,_p w) \qquad (6)$$

by 8.3.6(2). Set $k = 2{\cdot}\#(x \,,_p y) + 1 = |x \,,_p y|_d = |v \,,_p w|_d$ and in the direction ($\rightarrow$) assume $2 \star x \star y = x \,,_p y <_p v \,,_p w = 2 \star v \star w$. We now consider three cases. If $\#(x) < \#(v)$ then $x <_p v$ by (2) and we are done.

If $\#(x) > \#(v)$ then $v <_p x$ by (2) and we have $v <_p^i x$ for some $i < |v|_d = 2{\cdot}\#(v) + 1 < 2{\cdot}\#(x) + 1 = |x|_d$. Also $v =_p^j x$ for all $j < i$. But we then get a contradiction as we obtain $v \,,_p w = 2 \star v \star w <_p 2 \star x \star y = x \,,_p y$ from $2 \star v \star w <_p^{i+1} 2 \star x \star y$ and $2 \star v \star w <_p^j 2 \star x \star y$ for all $j < i + 1$.

The final case is $\#(x) = \#(v)$. Then $\#(y) = \#(w)$, $|x|_d = |v|_d$, and $|y|_d = |w|_d$. We cannot have $v <_p x$ by the same reasoning as in the preceding case. Thus $x \leq_p v$ by 8.3.8(6). If $x <_p v$ we are done. If $x = v$ then we have $2 \star x \star y <_p^i 2 \star v \star w$ for some $1 + |x|_d \leq i < k$ and $2 \star x \star y =_p^j 2 \star v \star w$ for all $j < i$. But then $y <_p^{i \,\dot{-}\, (1+|x|_d)} w$ and $y =_p^j w$ for all $j < i \,\dot{-}\, (1 + |x|_d)$. Hence $y <_p w$.

In the direction ($\leftarrow$) consider two cases. If $x <_p v$ then, since $\#(x) \leq \#(v)$ and so $|x|_d \leq |v|_d$ by (3), we have $x <_p^i v$ for some $i < |x|_d$ and $x =_p^j v$ for all $j < i$. We then get $x \,,_p y <_p v \,,_p w$ because $2 \star x \star y <_p^{i+1} 2 \star v \star w$ and $2 \star x \star y =_p^j 2 \star v \star w$ for all $j < i + 1$.

The second case is when $x = v$ and $y <_p w$. We similarly as in the preceding case get $y <_p^i w$ for some $i < |y|_d$ and $y =_p^j w$ for all $j < i$. But then $x \,,_p y <_p v \,,_p w$ because $2 \star x \star y <_p^{i+|x|_d+1} 2 \star v \star w$ and $2 \star x \star y =_p^j 2 \star v \star w$ for all $j < i + |x|_d + 1$.

8.3.10 The principle of the least prefix code. The ordering predicate of prefix codes $<_p$ is a well-order. This can be expressed in the first-order language of PA only as a theorem schema called the *principle of the least prefix code* with a formula $\phi[x]$ with one indicated variable x and y a variable not occurring in ϕ:

$$T \vdash \exists x \phi[x] \land \forall x(\phi[x] \rightarrow Prf(x)) \rightarrow \exists x(\phi[x] \land \forall y(y <_p x \rightarrow \neg\phi[y])) \,. \qquad (1)$$

Here T is any proper extension of PA which contains the functions and predicates involved with prefix codes.

Property (1) is proved by working in T. We assume $\forall x(\phi[x] \rightarrow Prf(x))$ and $\phi[z_0]$ for some z_0. For the formula $\psi_1[n, x] \equiv \phi[x] \land |x|_d = n$ we have

$\psi_1[|z_0|_d, z_0]$. Hence $\exists x \psi_1[m, x]$ for the least m by the least number principle. Thus $\phi[z]$ and $|z|_d = m$ for some z. Thus also $Prf(z)$ and $m = |z|_d = 2 \cdot \# z + 1 > 0$. By the minimality of m we have $m \le |y|_d$ for any y s.t. $\phi[y]$.

For the formula

$$\psi_2[n,x] \equiv \phi[x] \wedge |x|_d = m \wedge \\ \forall y \forall i (\phi[y] \wedge i < n \wedge \forall j (j < i \to x =_p^j y) \to \neg y <_p^i x)$$

we prove by induction on n

$$n \le m \to \exists x \psi_2[n,x] \; . \tag{2}$$

Roughly speaking, the property says that for every $n \le m$ there is an x satisfying $\phi[x]$ which is a minimal prefix code up to n.

The base case is trivially satisfied by $x := z$ because $i \not< 0$. In the inductive case assume $n+1 \le m$ and there is an x_0 s.t. $\psi_2[n, x_0]$ by IH. We have $Prf(x_0)$ and $n < m = |x_0|_d$ and let v_0 be the code at the position n of x_0. We thus have $\psi_3[|v_0|_d, x_0]$ for the formula

$$\psi_3[k,x] \equiv \psi_2[n,x] \wedge \forall a \forall v \forall b (x = a \star v \star b \wedge Prf(v) \wedge |a|_d = n \to |v|_d = k) \; .$$

Hence $\exists k \exists x \psi_3[k, x]$, and by the least number principle there is a smallest such k for which $\exists x \psi_3[k, x]$. Thus $\psi_3[k, x]$ for some x and so $\psi_2[n, x]$ and for the code v at the position n of x we have $|v|_d = k$. We claim that $\phi_2[n+1, x]$ holds. So take any y, i s.t. $\phi[y]$, $i < n+1$, and $\forall j (j < i \to x =_p^j y)$. We have $Prf(y)$ and we wish to show $\neg y <_p^i x$. If $i \ge |y|_d$ then we have $\neg y <_p^i x$. If $i < |y|_d$ we consider two cases. If $i < n$ then we have $\neg y <_p^i x$ from $\psi_2[n, x]$. If $i = n$ then let w be the code at the position n of y. By the minimality of k we have $|v_0|_d = k \le |w|_d$ and so we have $x <_p^n y$ or $x =_p^n y$ and hence $\neg y <_p^n x$. This ends the induction proof of (2).

From the just proved property we obtain $\psi_2[m, x]$ for some x and we claim that x is the least prefix code satisfying $\phi[x]$. So take any y s.t. $y <_p x$ and suppose on the contrary $\phi[y]$. We have $m \le |y|_d$ and so there is an i such that $i < m$, $y <_p^i x$, and $y =_p^j x$ for all $j < i$. We now get the contradiction $\neg \phi[x]$ from $\psi_2[m, x]$.

8.3.11 Minima and maxima of prefix codes of count n. We call the number a the *minimum of codes with the count* n if

$$Prf(a) \wedge \#(a) = n \wedge \forall x (Prf(x) \wedge \#(x) = n \to a \le_p x) \tag{1}$$

We call the number b the *maximum of codes with the count* n if

$$Prf(b) \wedge \#(b) = n \wedge \forall x (Prf(x) \wedge \#(x) = n \to x \le_p b) \tag{2}$$

The reader will note that because $<_p$ is a linear order over Prf there is at most one minimum (maximum) code of a given count n. For each n the maxima and minima exist:

$$\vdash_{\mathrm{PA}} \exists b(\mathit{Prf}(b) \land \#(b) = n \land \forall x(\mathit{Prf}(x) \land \#(x) = n \to x \leq_p b)) \tag{3}$$
$$\vdash_{\mathrm{PA}} \exists a(\mathit{Prf}(a) \land \#(a) = n \land \forall x(\mathit{Prf}(x) \land \#(x) = n \to a \leq_p x)) \;. \tag{4}$$

(3): By induction on n. In the base case we set $b := 1$ because $\#(b) = 0$ and for any x s.t. $\mathit{Prf}(x)$, $\#(x) = 0$ we have $x = 1$ by 8.3.5(4). In the inductive case we obtain the maximum b_1 of the count n by IH and we set $b = b_1 ,_p 1$. Since $\mathit{Prf}(1)$, $\#(1) = 0$ by 8.3.5(4), we get $\mathit{Prf}(b)$, $\#(b) = n + 1$ by 8.3.6(2). Let x be any number such that $\mathit{Prf}(x)$ and $\#(x) = n + 1$. We have $x = x_1 ,_p x_2$ for some x_1, x_2 such that $\mathit{Prf}(x_1)$, $\mathit{Prf}(x_2)$ by 8.3.6(7) and $\#(x_1) + \#(x_2) = n$ by 8.3.6(2). For the proof of $x = x_1 ,_p x_2 \leq_p b_1 ,_p 1 = b$ in which we use 8.3.9(5) we note that $\#(x_1) \leq n = \#(b_1)$. If $\#(x_1) < \#(b_1)$ then $x_1 <_p b_1$ by 8.3.9(2) and so $x <_p b$. If $\#(x_1) = \#(b_1)$ then $x_1 \leq_p b_1$ by the maximality of b_1. If $x_1 <_p b_1$ then $x <_p b$ again. If $x_1 = b_1$ then $\#(x_2) = 0$ and we get $x_2 = 1$ by 8.3.5(4) and so $x <_p b$.

(4): We use the principle of the least prefix code with the formula $\phi[x, n] \equiv \mathit{Prf}(x) \land \#(x) = n$. Let b be the maximum code with the count n existing by (3). We have $\phi[b, n]$ and so the antecedent of 8.3.10(1) is satisfied. Thus there is a number a s.t. $\phi[a, n]$ and for any $y <_p a$ we have $\neg\phi[y, n]$. To see that a is the minimum take any number x s.t. $\mathit{Prf}(x)$ and $\#(x) = n$, i.e. $\phi[x, n]$. We must have $x \not<_p a$ and so $a \leq_p x$ by 8.3.8(6).

8.3.12 Successor function over prefix codes. We wish to introduce the unary function $s_p(x)$ yielding the least prefix code after x in the order $<_p$ by the following contextual definition:

$$\vdash_{\mathrm{PA}x} s_p(x) = y \leftrightarrow x <_p y \land \forall z(x <_p z \to y \leq_p z) \lor \neg\mathit{Prf}(x) \land y = 0 \tag{1}$$

Its existence condition

$$\vdash_{\mathrm{PA}} \exists y(x <_p y \land \forall z(x <_p z \to y \leq_p z) \lor \neg\mathit{Prf}(x) \land y = 0) \tag{2}$$

is proved by taking any x and considering two cases. If $\neg\mathit{Prf}(x)$ then it suffices to set $y := 0$. If $\mathit{Prf}(x)$ then also $\mathit{Prf}(x ,_p x)$ and $\#(x, ,_p x) = 2\#(x) + 1 > \#(x)$ by 8.3.6(2). Hence $x <_p x ,_p x$ by 8.3.9(2) and thus $\exists y\, x <_p y$. The formula $\phi[x, y] \equiv x <_p y$ satisfies for y the antecedent of the principle of the least prefix code because we have $\exists y\, x <_p y$ and from $x <_p y$ we obtain $\mathit{Prf}(y)$. Hence there is a y s.t. $x <_p y$ and for any z such that $z <_p y$ we have $\neg x <_p z$. But then if $x <_p z$ we have $\neg z <_p y$, i.e. $y \leq_p z$ by 8.3.8(6).

The uniqueness condition for s_p follows from

$$\begin{aligned}\vdash_{\mathrm{PA}}\ & x <_p y_1 \land \forall z(x <_p z \to y_1 \leq_p z) \land \\ & x <_p y_2 \land \forall z(x <_p z \to y_2 \leq_p z) \to y_1 = y_2\end{aligned} \tag{3}$$
$$\vdash_{\mathrm{PA}} y_1 = 0 \land y_2 = 0 \to y_1 = y_2 \;. \tag{4}$$

(3): Assume the antecedent. We have $\mathit{Prf}(y_1)$ and $\mathit{Prf}(y_2)$. If it were the case that $y_1 \neq y_2$ then we would have $y_1 <_p y_2$ or $y_2 <_p y_1$ by 8.3.8(6). If

$y_1 <_p y_2$ then, since $x <_p y_1$, we instantiate the second quantifier formula in the antecedent with $z := y_1$ and get $y_2 \leq_p y_1$. Thus $y_2 <_p y_1$ and then $y_1 <_p y_1$ by 8.3.8(5) contradicting 8.3.8(4). The case $y_2 <_p y_1$ leads to a contradiction similarly.

(4): This is trivial.

The function s_p satisfies the following:

$$\vdash_{\mathrm{PA}} \ \mathit{Prf}(x) \to x <_p s_p(x) \wedge \forall z(x <_p z \to s_p(x) \leq_p z) \tag{5}$$

$$\vdash_{\mathrm{PA}} \ \mathit{Prf}(x) \leftrightarrow \mathit{Prf}(s_p(x)) \tag{6}$$

$$\vdash_{\mathrm{PA}} \ x <_p y \leftrightarrow s_p(x) <_p s_p(y) \tag{7}$$

$$\vdash_{\mathrm{PA}} \ \mathit{Prf}(x) \wedge \#(x) > 0 \to \exists y(\mathit{Prf}(y) \wedge s_p(y) = x)\ . \tag{8}$$

(5): If $\mathit{Prf}(x)$ then we get the consequent by instantiating (1) with $y := s_p(x)$.

(6): If $\mathit{Prf}(x)$ then $x <_p s_p(x)$ by (5) and we have $\mathit{Prf}(s_p(x))$. Vice versa, if $\mathit{Prf}(s_p(x))$ then if it were the case that $\neg\mathit{Prf}(x)$ we would get $s_p(x) = 0$ by instantiating (1) with $y := s_p(x)$. We would then get $\#(s_p(x)) = 0$ by 8.3.3(13) and a contradiction $s_p(x) = 1$ by 8.3.5(4).

(7): Assume $x <_p y$. We have $\mathit{Prf}(x)$ and $\mathit{Prf}(y)$ and we get $x <_p s_p(x) \leq_p y < s_p(y)$ by (5) and transitivity. Vice versa, assume $s_p(x) <_p s_p(y)$. We have $\mathit{Prf}(x)$ and $\mathit{Prf}(y)$ by 8.3.8(3) and (6). It cannot be the case that $x = y$ because then $s_p(x) = s_p(y)$ would contradict 8.3.8(4). Thus either $y <_p x$ or $x <_p y$ by 8.3.8(6). If the former then

$$s_p(y) \overset{(5)}{\leq_p} x \overset{(5)}{<_p} s_p(x) < s_p(y)$$

which by transitivity contradicts the irreflexivity of $<_p$.

(8): In the proof of this property we will repeatedly prove $s_p(x) = y$ for some $\mathit{Prf}(x)$ and $\mathit{Prf}(y)$ by using (1) where we will derive $x <_p y$ and then for any z such that $x <_p z$ we will prove $y \leq_p z$. The property follows from an auxiliary property

$$\vdash_{\mathrm{PA}} \ \forall x(\mathit{Prf}(x) \wedge k = \#(x) \wedge k > 0 \to \exists y(\mathit{Prf}(y) \wedge s_p(y) = x))$$

by instantiating $k := \#(x)$. The auxiliary property is proved by complete induction on k. So assume $\mathit{Prf}(x)$, $k = \#(x)$, and $k > 0$. We have $x = v \,,_p w$ for some v, w such that $\mathit{Prf}(v)$, $\mathit{Prf}(w)$ by 8.3.6(7) and $\#(x) = \#(v) + \#(w) + 1$ by 8.3.6(2). We consider two cases.

The first case is when w is not the minimum code with the count $\#(w)$, i.e. $a <_p w$ and $\#(a) = \#(w)$ for some a. We then have $w \neq 1$ by 8.3.9(4) and $\#(w) > 0$ by 8.3.5(4). Since $\#(w) < k$, we have $\mathit{Prf}(w_1)$, $s_p(w_1) = w$ for some w_1 by IH. Thus $w_1 <_p w$ by (5) and $\#(w_1) \leq \#(w)$ by 8.3.9(3). If it were the case that $\#(w_1) < \#(w)$ then we would have $w_1 <_p a$ by 8.3.9(2) and we would get a contradiction $w = s_p(w_1) \leq_p a <_p w$ by (5). Thus $\#(w_1) = \#(w)$ and we get $v \,,_p w_1 <_p v \,,_p w$ by 8.3.9(5). Note that we have $\#(v \,,_p w_1) = k$.

We claim that $s_p(v \,,_p w_1) = v \,,_p w = x$. For that it remains to show that if $w \,,_p w_1 <_p z$ for any z then $x \leq_p z$. Thus take any z s.t. $w \,,_p w_1 <_p z$. We have $k = \#(v \,,_p w_1) \leq \#(z)$ by 8.3.9(3). If $k < \#(z)$ then $x <_p z$ by 8.3.9(2). If $0 < k = \#(z)$ then $z = z_1 \,,_p z_2$ for some z_1, z_2 such that $Prf(z_1)$, $Prf(z_2)$ by 8.3.6(7) and $\#(z) = \#(z_1) + \#(z_2) + 1$ by 8.3.6(2). Since $v \,,_p w_1 <_p z_1 \,,_p z_2$ and $\#(v) + \#(w) = \#(v) + \#(w_1) = \#(z_1) + \#(z_2)$, we have either $v <_p z_1$ or $v = z_1$ and $w_1 <_p z_2$, i.e. $w = s_p(w_1) \leq_p z_2$ by 8.3.9(5). But then $x = v \,,_p w \leq_p z_1 \,,_p z_2 = z$ by 8.3.9(5) again.

The second case is that w is the minimum code with the count $\#(w)$ and we consider three subcases.

The first subcase is when $v = 1$. We obtain from 8.3.11(3) the maximum code b with the count $k \dot{-} 1$. We claim that $s_p(b) = x = 1 \,,_p w$. For that we note that $b <_p x$ by 8.3.9(2). We now take any z s.t. $b <_p z$. We have $Prf(z)$ and it must be the case that $k \dot{-} 1 \leq \#(z)$ by 8.3.9(3). We cannot have $k \dot{-} 1 = \#(z)$ by the maximality of b. If $k < \#(z)$ then $x <_p z$ by 8.3.9(2). If $k = \#(z)$ then $z = z_1 \,,_p z_2$ for some z_1, z_2 such that $Prf(z_1)$, $Prf(z_2)$ by 8.3.6(7) and $\#(z_1) + \#(z_2) = \#(1) + \#(w) = k \dot{-} 1$ by 8.3.6(2). For the proof of $1 \,,_p w = x \leq_p z_1 \,,_p z_2 = z$ we note that $1 \leq_p z_1$ by 8.3.9(4). We use 8.3.9(5) in the two cases when either $1 <_p z_1$ and then $x <_p z$ or else $1 = z_1$ and then, since $\#(w) = \#(z_2)$, we get $w \leq_p z_2$ by the minimality of w and so $a \leq_p x$.

The second subcase is when $v \neq 1$ and v is not the minimum with the count $\#(v)$. By similar reasoning as in the first case above we obtain by IH a v_1 s.t. $Prf(v_1)$, $\#(v_1) = \#(v)$, $v_1 <_p v$, and $s_p(v_1) = v$. We then obtain from 8.3.11(3) the maximum code b with the count $\#(w)$. We have $Prf(b)$, $\#(b) = \#(w)$, and we claim that $s_p(v_1 \,,_p b) = v \,,_p w$. Since $\#(v_1) + \#(b) = \#(v) + \#(w)$, we get $v_1 \,,_p b <_p v \,,_p w$ by 8.3.9(5). Now we take any z such that $v_1 \,,_p b <_p z$. We have $k = \#(v_1 \,,_p b) \leq \#(z)$ by 8.3.9(3). If $k < \#(z)$ then $x <_p z$ by 8.3.9(2). If $0 < k = \#(z)$ then $z = z_1 \,,_p z_2$ for some z_1, z_2 such that $Prf(z_1)$, $Prf(z_2)$ by 8.3.6(7) and $\#(z) = \#(z_1) + \#(z_2) + 1$ by 8.3.6(2). Since $v_1 \,,_p b <_p z_1 \,,_p z_2$ and $\#(v) + \#(w) = \#(v_1) + \#(b) = \#(z_1) + \#(z_2)$, we have either $v_1 <_p z_1$ or $v_1 = z_1$ and $b <_p z_2$ by 8.3.9(5). The latter case cannot obtain because it would contradict the maximality of b because we would have $\#(b) = \#(z_2)$. Hence we have $v_1 < z_1$ and so $v = s_p(v_1) \leq_p z_1$ by (5). If $v <_p z_1$ then $x = v \,,_p w <_p z_1 \,,_p z_2 = z$ by 8.3.9(5) If $v = z_1$ then $\#(w) = \#(z_2)$ and we have $w \leq z_2$ by the minimality of w. Thus $x = v \,,_p w \leq_p z_1 \,,_p z_2 = z$ by 8.3.9(5) again.

The third subcase is when $v \neq 1$ and v is the minimum code with the count $\#(v)$. We must have $\#(v) > 0$ by 8.3.5(4). We use 8.3.11(3) to get the maxima b_1 with the count $\#(v) \dot{-} 1$ and b_2 with the count $\#(w) + 1$. Thus $Prf(b_1)$, $\#(b_1) = \#(v) \dot{-} 1$, $Prf(b_2)$, $\#(b_2) = \#(w) + 1$, and $\#(b_1) + \#(b_2) = \#(v) + \#(w)$. We claim that $s_p(b_1 \,,_p b_2) = v \,,_p w$. First of all, we have $b_1 <_p v$ by 8.3.9(2) and so $b_1 \,,_p b_2 <_p v \,,_p w$ by 8.3.9(5). We now take any z s.t. $b_1 \,,_p b_2 <_p z$. We have $Prf(z)$ and $k = \#(b_1 \,,_p b_2) \leq \#(z)$ by 8.3.9(3). If $k < \#(z)$ we have $x <_p z$ by 8.3.9(2). If $0 < k = \#(z)$ then we have $z = z_1 \,,_p z_2$ for some z_1, z_2

such that $\mathit{Prf}(z_1)$, $\mathit{Prf}(z_2)$ by 8.3.6(7) and $\#(b_1) + \#(b_2) = \#(v) + \#(w) = \#(z_1) + \#(z_2)$ by 8.3.6(2). From $b_1 ,_p b_2 <_p z_1 ,_p z_2$ we get $b_1 <_p z_1$ or $b_1 = z_1$ and $b_2 <_p z_2$ by 8.3.9(5). The second case cannot happen because if $b_1 = z_1$ then $\#(b_2) = \#(z_2)$ and we get a contradiction $z_2 \leq_p b_2$ from the maximality of b_2. In the first case, when $b_1 <_p z_1$, we get $\#(b_1) \leq \#(z_1)$ by 8.3.9(3) and so $\#(b_1) < \#(z_1)$ by the maximality of b_1. Thus $\#(v) \leq \#(z_1)$. If $\#(v) < \#(z_1)$ then $x = v ,_p w <_p z_1 ,_p z_2 = z$ by 8.3.9(5). If $\#(v) = \#(z_1)$ then $v \leq_p z_1$ by the minimality of v and, since $\#(w) = \#(z_2)$, $w \leq_p z_2$ by the minimality of w. But then $x = v ,_p w \leq_p z_1 ,_p z_2 = z$ by 8.3.9(5).

Isomorphism of $\mathbb{N}$ and *Prf* and a Pairing Function over $\mathbb{N}$

We will now establish an isomorphism between natural numbers and prefix codes. The isomorphism preserves orders and endows $\mathbb{N}$ with pairing.

8.3.13 Enumeration of prefix codes. We define the unary function π by primitive recursion:

$$\vdash_{\mathrm{PAx}} \pi(0) = 1 \tag{1}$$
$$\vdash_{\mathrm{PAx}} \pi(x') = s_p\, \pi(x)\ . \tag{2}$$

The following properties of π assert that the function enumerates the prefix codes, i.e. it is an injection: (6), into *Prf*: (3), and onto *Prf*: (4). It is also an order isomorphism between $\mathbb{N}$ and *Prf*: (5).

$$\vdash_{\mathrm{PA}} \mathit{Prf}(\pi(x)) \tag{3}$$
$$\vdash_{\mathrm{PA}} \mathit{Prf}(y) \to \exists x\, \pi(x) = y \tag{4}$$
$$\vdash_{\mathrm{PA}} x < y \leftrightarrow \pi(y) <_p \pi(y) \tag{5}$$
$$\vdash_{\mathrm{PA}} \pi(x) = \pi(y) \to x = y\ . \tag{6}$$

(3): By induction on x. In the base case we have $\pi(0) = 1$ and $\mathit{Prf}(1)$ by 8.3.5(4). In the inductive case we obtain $\mathit{Prf}(\pi(x))$ from IH and $\pi(x) <_p s_p\, \pi(x) = \pi(x')$ by 8.3.12(5). But then $\mathit{Prf}(\pi(x'))$.

(4): Assume $\mathit{Prf}(y)$ and $\forall x\, \pi(x) \neq y$. The formula

$$\phi[y] \equiv \mathit{Prf}(y) \land \forall x\, \pi(x) \neq y$$

thus satisfies the antecedent of the principle of least prefix code 8.3.10(1) and there is a z such that $\phi[z]$, i.e. $\mathit{Prf}(z)$, $\forall x\, \pi(x) \neq z$, and for all $u <_p z$ we have $\neg\phi[u]$. Since $\pi(0) = 1$, we have $z \neq 1$ and so $\#(z) > 0$ by 8.3.5(4). But then $s_p(u) = z$ for some u s.t. $\mathit{Prf}(u)$ by 8.3.12(8) and $u <_p z$ by 8.3.12(5). Hence $\pi(x) = u$ for some x from $\neg\phi[u]$ and we contradict $\phi[z]$ because:

$$\pi(x') = s_p\, \pi(x) = s_p(u) = z\ .$$

(5): We prove $\forall y(5)$ by induction on x. In the base case we assume in the direction $(\to)$ $0 < y$. Then $z' = y$ for some z and $\pi(y) = s_p\,\pi(z)$. We have $\mathit{Prf}(\pi(z))$, $\mathit{Prf}(\pi(y))$ by (3) and $\pi(x) <_p \pi(y)$ by 8.3.12(5). Since $1 \leq_p \pi(x)$ by 8.3.9(4), we get $\pi(0) = 1 <_p \pi(y)$ by 8.3.8(5). In the direction $(\leftarrow)$ we assume $\pi(0) <_p \pi(y)$. Thus $\mathit{Prf}(\pi(0))$, $\mathit{Prf}(\pi(y))$ and then $\pi(y) \neq 1 = \pi(0)$ by 8.3.8(4). Hence $y \neq 0$, i.e. $0 < y$.

In the inductive case we have $x' < y$ iff $x' < z'$ for some z s.t. $z' = y$ iff $x < z$ for some z s.t. $z' = y$ iff, by IH, $\pi(x) <_p \pi(z)$ for some z s.t. $z' = y$, iff by 8.3.12(7), $s_p\,\pi(x) <_p s_p\,\pi(z)$ for some z s.t. $z' = y$, iff $\pi(x') <_p \pi(z')$ for some z s.t. $z' = y$ iff $\pi(x') <_p \pi(y)$.

(6): if $\pi(x) = \pi(y)$ then, since $\mathit{Prf}(\pi(x))$ by (3), we have $\pi(x) \not<_p \pi(y)$ and $\pi(y) \not<_p \pi(x)$ by 8.3.8(4) and so $x \not< y$ and $y \not< x$ by (5).

Property (4) is the existence condition for the inverse of π introduced into PA by minimalization:

$$\pi^{-1}(x) = \mu_y[\mathit{Prf}(x) \to \pi(y) = x] \tag{7}$$

Direct consequence of the defining axiom for π^{-1} is

$$\vdash_{\mathrm{PA}} \mathit{Prf}(x) \to \pi\,\pi^{-1}(x) = x\ . \tag{8}$$

8.3.14 Pairing function. We are now ready to introduce by explicit definition into PA the binary pairing function:

$$\vdash_{\mathrm{PAx}} x, y = \pi^{-1}(\pi(x)\,{,_p}\,\pi(y)) \tag{1}$$

The function extends the order isomorphism π between $\mathbb{N}$ and Prf also to pairing because we have:

$$\vdash_{\mathrm{PA}} \pi(x, y) = \pi(x)\,{,_p}\,\pi(y)\ . \tag{2}$$

Indeed, from the definition we obtain $\pi(x, y) = \pi\,\pi^{-1}(\pi(x)\,{,_p}\,\pi(y))$ and, since $\mathit{Prf}(\pi(x, y))$ by 8.3.13(3), the property follows by 8.3.13(8).

The basic properties of the pairing function are the pairing property 1.3.7(1) which is proved as (3) and the property 1.3.7(3) proved as (4) which assert that every positive number is in the range of the pairing function:

$$\vdash_{\mathrm{PA}} x, y = v, w \to x = v \land y = w \tag{3}$$

$$\vdash_{\mathrm{PA}} x = 0 \lor \exists v \exists w\, x = v, w\ . \tag{4}$$

(3): Assume $x, y = v, w$. From $\pi(x, y) = \pi(v, w)$ we obtain $\pi(x)\,{,_p}\,\pi(y) = \pi(v)\,{,_p}\,\pi(w)$ by (2). Since $\mathit{Prf}(\pi(x))$, $\mathit{Prf}(\pi(v))$, $\mathit{Prf}(\pi(y))$ by 8.3.13(3), we obtain $\pi(x) = \pi(v)$; $\pi(y) = \pi(w)$ by 8.3.6(3), and $x = \pi^{-1}\pi(x) = \pi^{-1}\pi(v) = v$; $y = \pi^{-1}\pi(y) = \pi^{-1}\pi(w) = w$ by 8.3.13(8).

(4): Assume $0 < x$ and obtain $1 = \pi(x) <_p \pi(x)$ by 8.3.13(5). We have $\mathit{Prf}(1)$ and $\mathit{Prf}(\pi(x))$. Since $1 \not<_p 1$ by 8.3.8(4), we have $1 \neq \pi(x)$ and so

$\#(\pi(x)) > 0$ by 8.3.5(4). Thus $\pi(x) = y \,{,_p}\, z$ for some y, z such that $\mathit{Prf}(y)$, $\mathit{Prf}(z)$ by 8.3.6(7). We have $\pi(v) = y$ and $\pi(w) = z$ for some v and w by 8.3.13(4) and so

$$x \overset{8.3.13(8)}{=} \pi^{-1}\pi(x) = \pi^{-1}(y \,{,_p}\, z) = \pi^{-1}(\pi(v) \,{,_p}\, \pi(w)) \overset{8.3.14(1)}{=} v, w \ .$$

8.3.15 Pair size function. The function $\#(x)$ measures the complexity of prefix codes x as the number of inner nodes of binary trees expressed by x. The isomorphic image of $\#(x)$ is the pair size function $|x|_p$ (see Par. 1.3.9) which is introduced into PA by an explicit definition:

$$\vdash_{\mathrm{PAx}} |x|_p = \#(\pi(x)) \tag{1}$$

The following are the basic properties of the pair size function

$$\vdash_{\mathrm{PA}} |0|_p = 0 \tag{2}$$

$$\vdash_{\mathrm{PA}} |x, y|_p = |x|_p + |y|_p + 1 \ . \tag{3}$$

(2): We have $\pi(0) = 1$ and $\#(1) = 0$ by 8.3.3(14).
(3): We have $\mathit{Prf}(\pi(x))$ and $\mathit{Prf}(\pi(y))$ by 8.3.13(3) and so

$$\begin{aligned} |x, y|_p = \#(\pi(x, y)) &\overset{8.3.14(2)}{=} \#(\pi(x) \,{,_p}\, \pi(y)) \overset{8.3.6(2)}{=} \\ &\#(\pi(x)) + \#(\pi(y)) + 1 = |x|_p + |y|_p + 1 \ . \end{aligned}$$

8.3.16 Ordering properties of pairs. The pairing property 8.3.14(3) and the property 8.3.14(4) which says that there is at most one atom 0 are concerned solely with the pairing function. We will now investigate properties connecting pairing to the order on $\mathbb{N}$. Property (1) says that 0 is an atom, (2) gives sufficent and necessary conditions for the comparison of two pairs, and (3) will be the basis for the induction principle on pairs:

$$\vdash_{\mathrm{PA}} 0 < x, y \tag{1}$$

$$\begin{aligned} \vdash_{\mathrm{PA}} x, y < v, w \leftrightarrow |x, y|_p < |v, w|_p \lor \\ |x, y|_p = |v, w|_p \land (x < v \lor x = v \land y < w) \end{aligned} \tag{2}$$

$$\vdash_{\mathrm{PA}} x < x, y \land y < x, y \ . \tag{3}$$

(1): We have $\mathit{Prf}(\pi(x))$, $\mathit{Prf}(\pi(y))$ by 8.3.13(3) and $\mathit{Prf}(\pi(x) \,{,_p}\, \pi(y))$, $\#(\pi(x) \,{,_p}\, \pi(y)) > 0$ by 8.3.6(2). For $\pi(0) = 1$ we have $\mathit{Prf}(\pi(0))$ and $\#(\pi(0)) = 0$ by 8.3.5(4). We get $\pi(0) <_p \pi(x) \,{,_p}\, \pi(y)$ by 8.3.9(2) and, since and $\pi(x, y) = \pi(x) \,{,_p}\, \pi(y)$ by 8.3.14(2), we obtain $0 < x, y$ by 8.3.13(5).

(2): We have $x, y < v, w$ iff, by 8.3.13(5), $\pi(x, y) <_p \pi(v, w)$ iff, by 8.3.14(2), $\pi(x) \,{,_p}\, \pi(y) <_p \pi(v) \,{,_p}\, \pi(w)$.

We have $\mathit{Prf}(\pi(x))$, $\mathit{Prf}(\pi(y))$, $\mathit{Prf}(\pi(v))$, $\mathit{Prf}(\pi(w))$ by 8.3.13(3) and $\mathit{Prf}(\pi(x) \,{,_p}\, \pi(y))$, $\mathit{Prf}(\pi(v) \,{,_p}\, \pi(w))$ by 8.3.6(2).

We also have $|x,y|_p < |v,w|_p$ iff $\#(\pi(x,y)) < \#(\pi(v,w))$ iff, by 8.3.14(2), $\#(\pi(x) \,,_p\, \pi(y)) < \#(\pi(v) \,,_p\, \pi(w))$ iff, by 8.3.6(2), $\#(\pi(x)) + \#(\pi(y)) < \#(\pi(v)) + \#(\pi(w))$.

We similarly have $|x,y|_p = |v,w|_p$ iff $\#(\pi(x)) + \#(\pi(y)) = \#(\pi(v)) + \#(\pi(w))$.

Now, in the direction ($\rightarrow$) assume $x,y < v,w$, get $\pi(x,y) <_p \pi(v,w)$ by 8.3.13(5), and then $\#(\pi(x,y)) \leq \#(\pi(v,w))$ by 8.3.9(3). Thus $|x,y|_p \leq |v,w|_p$. If $|x,y|_p < |v,w|_p$ there is nothing to prove. If $|x,y|_p = |v,w|_p$ then $\#(\pi(x)) + \#(\pi(y)) = \#(\pi(v)) + \#(\pi(w))$ and we have

$$\pi(x) <_p \pi(v) \vee \pi(x) = \pi(v) \wedge \pi(y) <_p \pi(w) \tag{4}$$

by 8.3.9(5). Thus

$$x < v \vee x = v \wedge y < w \tag{5}$$

by 8.3.13(5)(6).

In the direction ($\leftarrow$) consider first the case $|x,y|_p < |v,w|_p$. We get $\#(\pi(x) \,,_p\, \pi(y)) < \#(\pi(v) \,,_p\, \pi(w))$ by 8.3.14(2) and $\pi(x) \,,_p\, \pi(y) <_p \pi(v) \,,_p\, \pi(w)$ by 8.3.9(2). Hence $x,y < v,w$ by the above.

In the second case assume $|x,y|_p = |v,w|_p$, i.e. $\#(\pi(x)) + \#(\pi(y)) = \#(\pi(v)) + \#(\pi(w))$, and (5). We obtain (4) by 8.3.13(5) and $\pi(x) \,,_p\, \pi(y) <_p \pi(v) \,,_p\, \pi(w)$ by 8.3.9(5). Thus $x,y < v,w$ again.

(3): If $x = 0$ we have $x < x,y$ by (1). If $x > 0$ we have $x = v,w$ for some v, w by 8.3.14(4), and since $|x|_d < |x,y|$ by 8.3.15(3), we get $x < x,y$ by (2). The proof of $y < x,y$ is similar.

8.3.17 Projection functions. The unary projection functions H and T (see Par. 1.3.12) are introduced into PA by minimalization whose existence conditions are direct consequences of 8.3.14(4):

$$\vdash_{\mathrm{PAx}} H(x) = \mu_v[x > 0 \rightarrow \exists w\, v,w = x] \tag{1}$$

$$\vdash_{\mathrm{PAx}} T(x) = \mu_w[x > 0 \rightarrow \exists v\, v,w = x]\ . \tag{2}$$

The projection functions satisfy the following:

$$\vdash_{\mathrm{PA}} H(0) = 0 \tag{3}$$

$$\vdash_{\mathrm{PA}} H(v,w) = v \tag{4}$$

$$\vdash_{\mathrm{PA}} T(0) = 0 \tag{5}$$

$$\vdash_{\mathrm{PA}} T(v,w) = w\ . \tag{6}$$

(3): The defining axiom for H implies $0 < H(0) \rightarrow \neg(0 > 0 \rightarrow \exists w\, 0,w = 0)$ from which we get $0 < H(0) \rightarrow 0 > 0$ and then $H(0) = 0$.

(4): The defining axiom for H implies $v,w > 0 \rightarrow \exists w_1\, H(v,w),w_1 = v,w$. We then get $H(v,w),w_1 = v,w$ for some w_1 by 8.3.16(1) and $H(v,w) = v$ by 8.3.14(3).

(5): Similarly as (3).

(6): Similarly as (4).

8.3.18 List indexing. We wish to introduce into PA the list indexing function $(x)_i$. The function was defined in Par. 1.3.18 by a clausal definition to satisfy:

$$\vdash_{\mathrm{PA}} (0)_x = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} (v,w)_0 = v \tag{2}$$
$$\vdash_{\mathrm{PA}} (v,w)_{i+1} = (w)_i \ . \tag{3}$$

The reader will note that this is not a definition by primitive recursion because the paramater x changes in the recursive application. We can introduce the list indexing function into PA with the help of the binary function $T^i(x)$ called the *iteration* of T. The iteration function is introduced into PA by primitive recursion:

$$\vdash_{\mathrm{PAx}} T^0(x) = x \tag{4}$$
$$\vdash_{\mathrm{PAx}} T^{i'}(x) = T\,T^i(x) \ . \tag{5}$$

The iteration function satisfies

$$\vdash_{\mathrm{PA}} T^i(0) = 0 \tag{6}$$
$$\vdash_{\mathrm{PA}} \forall x\, T^{i+1}(x) = T^i T(x) \ . \tag{7}$$

(6): By induction on i. In the base case we have $T^0(0) = 0$. In the inductive case we have $T^{i'}(0) = T\,T^i(0) \overset{\mathrm{IH}}{=} T(0) \overset{8.3.17(5)}{=} 0$.

(7): By induction on i. In the base case we have $T^{0+1}(x) = T\,T^0(x) = T(x) = T^0T(x)$. In the inductive case we get

$$T^{i'+1}(x) = T\,T^{i'}(x) \overset{\mathrm{IH}}{=} T\,T^iT(x) = T^{i+1}T(x) \ .$$

We can now introduce the indexing function into PA by explicit definition:

$$\vdash_{\mathrm{PAx}} (x)_i = H\,T^i(x) \tag{8}$$

and we can prove the above properties:

(1): We have $(0)_i = H\,T^i(0) \overset{(6)}{=} H(0) \overset{8.3.17(3)}{=} 0$.

(2): We have $(v,w)_0 = H\,T^0(v,w) = H(v,w) \overset{8.3.17(4)}{=} v$.

(3): We have $(v,w)_{i+1} = H\,T^{i+1}(v,w) \overset{(7)}{=} H\,T^iT(v,w) \overset{8.3.17(6)}{=} H\,T^i(w) = (w)_i$.

8.4 Course of Values Recursion with Measure

The most general form of introducing functions into PA by recursion is the *course of values recursion with measure* where we introduce into PA an n-ary function f such that $\vdash_{\text{PA}} f(\vec{x}) = \tau[\vec{x}]$ for a term τ applying, in addition to the previously introduced functions, also the function symbol f provided a measure term $\mu[\vec{x}]$ 'goes down' in the recursion, i.e. we have $\mu[\vec{\rho}] < \mu[\vec{x}]$ for all recursive applications $f(\vec{\rho})$. There are no additional restrictions on the form of recursive applications $f(\vec{\rho})$ and the arguments $\vec{\rho}$ can again apply the function f in a *nested* form. The depth of nesting is not restricted.

The requirement that that the measure of arguments goes down is not met by all terms τ. Suitable terms must satisfy certain non-trivial contextual properties. We leave the specification of the properties until the third part **UNFINISHED** of this text where we introduce a *clausal language* for a 'comfortable' definition of functions such as is expected in computer programming.

In this section we introduce syntactical restrictions imposed on recursive applications in τ which will guarantee that the measure goes down regardless of the form of the term τ.

8.4.1 Case discrimination function D. We will need in PA the ternary *case discrimination* function D satisfying

$$\vdash_{\text{PA}} D(x', y, z) = y \tag{1}$$

$$\vdash_{\text{PA}} D(0, y, z) = z \ . \tag{2}$$

The function is introduced into PA by contextual definition:

$$\vdash_{\text{PAx}} D(x, y, z) = v \leftrightarrow x > 0 \land v = y \lor x = 0 \land v = z \tag{3}$$

whose existence abd uniqueness conditions are straigtforward to prove. Properties (1), (2) directly follow from the defining axiom.

8.4.2 Characteristic functions of predicates. Let P be an n-ary predicate which has been introduced into PA. We denote by P_* its *characteristic function* which is an n-ary function introduced into PA by minimalization:

$$\vdash_{\text{PAx}} P_*(\vec{x}) = \mu_y[P(\vec{x}) \to y = 1] \ . \tag{1}$$

This is legal because the existence condition $\vdash_{\text{PA}} \exists y(P(\vec{x}) \to y = 1)$ is trivially provable. We have

$$\vdash_{\text{PA}} P(\vec{x}) \to P_*(\vec{x}) = 1 \tag{2}$$

$$\vdash_{\text{PA}} P(\vec{x}) \leftrightarrow P_*(\vec{x}) > 0 \tag{3}$$

because (2) directly follows from the defining axiom for P_*. Property (3) in the direction ($\to$) follows from (2). In the direction ($\leftarrow$) we note that the minimality condition in the defining axiom for P_* is $\vdash_{\text{PA}} y < P_*(\vec{x}) \to \neg(P(\vec{x}) \to y = 1)$ from which we obtain ($\leftarrow$) of (3) by instantiation $y := 0$.

8.4.3 Numerals. We will need a notation for successor terms directly denoting natural numbers. The terms are called (monadic) *numerals* and they are defined in the meta-theory to satisfy the following recurrences:

$$\underline{0}_m \equiv 0 \tag{1}$$
$$\underline{n+1}_m \equiv \underline{n}'_m \ . \tag{2}$$

Note that for a number n the numeral term $\underline{n}_m$ is of the form

$$0\overbrace{{}'\ldots{}'}^{n}$$

and it denotes n in the standard model of PA.

8.4.4 Measure induction. Properties of functions introduced into PA by course of values recursion with measure μ are generally proved by induction with measure.

Let T be a proper extension of PA containing the predicate $<$, $\phi[\vec{x}]$ a formula, and $\mu[\vec{x}]$ a term of $\mathcal{L}_T$ with $n \geq 1$ indicated variables. Both ϕ and μ can have additional free variables as parameters. Furthermore, let the new variables $\vec{y}$ be pairwise distinct from the variables of $\vec{x}$. The formula of the *induction with measure* μ is

$$\forall\vec{x}(\forall\vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \phi[\vec{y}]) \to \phi[\vec{x}]) \to \phi[\vec{x}] \tag{1}$$

The reader will note that for $\vec{x} \equiv x$ and $\mu[x] \equiv x$ the schema of measure induction is the schema of complete induction (see Par. 7.3.7).

8.4.5 Theorem. *Every proper extension T of PA containing the predicate $<$ proves the schema of induction with measure 8.4.4(1).*

Proof. We prove 8.4.4(1) from an auxiliary property

$$T \vdash \forall\vec{x}(\forall\vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \phi[\vec{y}]) \to \phi[\vec{x}]) \to \forall\vec{v}(\mu[\vec{v}] < z \to \phi[\vec{v}])$$

with $\vec{v}$ and z new. We work in T, assume the formula expressing that ϕ *is μ-progressive*

$$\forall\vec{x}(\forall\vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \to \phi[\vec{y}]) \to \phi[\vec{x}]) \ , \tag{1}$$

and prove

$$\forall\vec{v}(\mu[\vec{v}] < z \to \phi[\vec{v}]) \tag{2}$$

by induction on z. In the base case there is nothing to prove. In the inductive case we take any $\vec{v}$ s.t. $\mu[\vec{v}] < z'$ and consider two cases by dichotomy. If $\mu[\vec{v}] < z$ we obtain $\phi[\vec{v}]$ from IH: (2), If $\mu[\vec{v}] \geq z$ then we have $\mu[\vec{v}] = z$ and we use a variant $\forall\vec{y}(\mu[\vec{y}] < \mu[\vec{v}] \to \phi[\vec{y}])$ of IH: (2) in (1) instantiated with $\vec{x} := \vec{v}$ to obtain $\phi[\vec{v}]$.

The formula for the measure induction 8.4.4(1) follows from the auxiliary property by instantiating its consequent with $z := \mu[\vec{x}] + 1$ and $\vec{v} := \vec{x}$. $\square$

8.4.6 Extension by course of values recursion with measure. Let T be a proper extension of PA. We assume that the pairing function (x, y), the case discrimination function $D(x, y, z)$, as well as the characteristic function $<_*$ of the predicate $<$ have been introduced into T.

We wish to extend T into a theory S whose language contains the n-ary function symbol f $(n \geq 1)$ in such a way that a *course of values* definition $f(\vec{x}) = \tau$ is a theorem of S. For that we assume that $\tau[f; \vec{x}]$ is a term of $\mathcal{L}_T + f$ with its free variables among the n indicated ones. Thus τ is built up from the variables among $\vec{x}$, numerals $\underline{n}_m$, and applications $g_1(\vec{\rho})$, ..., $g_k(\vec{\rho})$ of functions where for $1 \leq j \leq k$ the function g_j has the arity $n_j \geq 1$. The term τ can also *recursively* apply the n-ary function symbol f which we indicate as $\tau[f; \vec{x}]$. The recursive applications $f(\vec{\rho})$ can be arbitrary, even *nested* when f is applied in terms $\vec{\rho}$. There is no restriction on the depth of nesting. The only condition, which is a semantic one, is that the recursion 'goes down' in a measure term $\mu[\vec{x}]$ of $\mathcal{L}_T$ with its free variables among the n indicated ones.

We keep the notation introduced in this paragraph fixed until the end of the section.

For an n-tuple of terms $\vec{\rho}$ and an n-ary function symbol g we will denote by $\tau[g; \vec{\rho}]$ the term obtained from τ by replacing in it all occurrences of variables from among $\vec{x}$ by the corresponding terms from among $\vec{\rho}$ and by the replacement of all recursive applications $f(\vec{\sigma})$ by applications $g(\vec{\sigma})$. We will also use the notation $\tau[[f]^{\mu}_{\vec{x}}; \vec{x}]$ as an abbreviation for the term

$$\tau[\lambda\vec{y}.D((\mu[\vec{y}] <_* \mu[\vec{x}], f(\vec{y}), 0); \vec{x}] \ ,$$

i.e. the term where we have replaced every application of $f(\vec{\sigma})$ in τ by the *guarded* application

$$D((\mu[\vec{\sigma}] <_* \mu[\vec{x}]), f(\vec{\sigma}), 0) \ .$$

The reader will note that the substitution of terms $\vec{\rho}$ for the corresponding variables $\vec{x}$ in the guarded term $\tau[[f]^{\mu}_{\vec{x}}; \vec{x}]$ is written as $\tau[[f]^{\mu]}_{\vec{\rho}}; \vec{\rho}]$ and it is an abbreviation for the term

$$\tau[\lambda\vec{y}.D((\mu[\vec{y}] <_* \mu[\vec{\rho}], f(\vec{y}), 0); \vec{\rho}] \ ,$$

i.e. the term where we have replaced every application of $f(\vec{\sigma})$ in τ by the guarded application

$$D((\mu[\vec{\sigma}] <_* \mu[\vec{\rho}]), f(\vec{\sigma}), 0) \ .$$

We use the same notation $\rho[[f]^{\mu}_{\vec{x}}; \vec{x}]$ also for subterms ρ of τ.

The extension of T to S with the $(n+1)$-ary function symbol f and with the axioms universal closures of

$$f(\vec{x}) = \tau[[f]^{\mu}_{\vec{x}}; \vec{x}] \tag{1}$$

$$\forall \vec{v}(\mu[\vec{v}] < \mu[\vec{x}] \rightarrow \phi[\ulcorner\langle\tau\rangle\urcorner, \vec{v}, f(\vec{v})]) \rightarrow \phi[\ulcorner\langle\tau\rangle\urcorner, \vec{x}, f(\vec{x})] \ . \tag{2}$$

is called *extension by course of values recursion with measure.* The formula $\phi[c, \vec{x}, y]$, which is of $\mathcal{L}_T$ and it is used in the single induction (with measure) axiom of S containing the symbol f, will be determined in Par. 8.4.13.

We do not impose any semantic restrictions on the recursion in τ to guarantee that the measure goes down, We achieve the same effect by purely syntactic means where we surround recursive applications by *if-then-else* guards. Such a restriction is acceptable from the point of view of mathematics where it simplifies the proofs below but, by amounting to an additional test, it is not acceptable in computer programming. We will discuss the semantic conditions (which can be syntactically enforced by provability) in the part three **UNFINISHED** of this text.

8.4.7 Special terms. Pursuing our plan of introducing the function f into the theory S, we first extend the theory T to T_1 by introducing the list indexing function $(x)_i$ (see Par. 8.3.18) and, by explicit definitions, the functions h_j for every $1 \leq j \leq k$ as *special contractions* of functions g_j:

$$T_1 \vdash h_j(x) = g_j((x)_0, (x)_{\underline{1}_m}, \ldots, (x)_{\underline{n_j - 1}_m}) \ . \tag{1}$$

It should be clear that we have for all $1 \leq j \leq k$:

$$T_1 \vdash h_j(x_1, \ldots, x_{n_j}, 0) = g_j(x_1, \ldots, x_{n_j}) \ . \tag{2}$$

The reader will recall our convention that the single argument of h_j is obtained by pairing.

For every subterm ρ of τ we define its *contraction* term $\langle \rho \rangle$ by induction on the structure of ρ to satisfy:

$$\begin{aligned}
\langle x_i \rangle &\equiv (x)_{\underline{i-1}_m} \\
\langle \underline{n}_m \rangle &\equiv \underline{n}_m \\
\langle g_j(\rho_1, \ldots, \rho_n) \rangle &\equiv h_j(\langle \rho_1 \rangle, \ldots, \langle \rho_n \rangle, 0) \\
\langle f(\rho_1, \ldots, \rho_n) \rangle &\equiv r(\langle \rho_1 \rangle, \ldots, \langle \rho_n \rangle, 0)
\end{aligned}$$

where r is a new unary function symbol. The reader will note that the term $\langle \tau \rangle$ is built up from the single variable x used only in applications $(x)_{\underline{i-1}_m}$ where $1 \leq i \leq n$ and from numerals $\underline{m}_m$ by applications of unary function symbols r and h_j where $1 \leq j \leq k$ whose arguments may contain also applications of the pairing function. Until the end of this section we call such terms *special.*

We designate by $\mu_1[x]$ the term obtained from the measure term $\mu[\vec{x}]$ by replacing for every $1 \leq i \leq n$ the occurrences of variables x_i by $(x)_{\underline{i-1}_m}$. Since $T_1 \vdash (x_1, \ldots, x_n, 0)_{\underline{i-1}_m} = x_i$ for all $1 \leq i \leq n$, we van prove by a simple meta-theoretical induction on the structure of μ:

$$T_1 \vdash \mu_1[(x_1, \ldots, x_n, 0)] = \mu[x_1, \ldots, x_n] \ . \tag{3}$$

8.4.8 Computation trees. We will introduce the function f into S by the arithmetization of computations of terms $r(\underline{a}_m)$ using as *computation rule* the identity $r(x) = \langle\tau\rangle[[r]^{\mu_1}_x\,;x]$. Terms of the form $r(\underline{a}_m)$ are special cases of subterms of $\langle\tau\rangle[[r]^{\mu_1}_{\underline{a}_m}\,;\underline{a}_m]$ and we will need to record the computation of all subterms ρ of $\langle\tau\rangle$. The computation of such a special term ρ is recorded by a binary labelled tree with the label consisting of a triple $\langle\rho, a, v\rangle$ where a is the value assigned to the variable x which may occur in ρ and v is the computed value, i.e. the denotation of the term $\rho[[r]^{\mu_1}_{\underline{a}_m}\,;\underline{a}_m]$. The two sons t_1 and t_2 are the trees recording possible subcomputations:

$$\begin{array}{ccc} & \langle\rho, a, v\rangle & \\ t_1 & & t_2 \end{array}$$

The form of the term ρ determines the shape of the sons t_1 and t_2 as follows. If $\rho \equiv \rho_1, \rho_2$ then the computation tree looks as follows:

$$\begin{array}{cc} \multicolumn{2}{c}{\langle(\rho_1,\rho_2), a, (v_1, v_2)\rangle} \\ \langle\rho_1, a, v_1\rangle & \langle\rho_2, a, v_2\rangle \\ t_1 & t_2 \end{array}$$

where the denotation v_1 of $\rho_1[[r]^{\mu_1}_{\underline{a}_m}\,;\underline{a}_m]$ is computed in the left son and the denotation v_2 of $\rho_2[[r]^{\mu_1}_{\underline{a}_m}\,;\underline{a}_m]$ is computed in the right son. The denotation of $(\rho_1,\rho_2)[[r]^{\mu_1}_{\underline{a}_m}\,;\underline{a}_m]$ is then the pair (v_1, v_2).

If $\rho \equiv (x)_{\underline{i}_m}$ or $\rho \equiv \underline{n}_m$ then the respective computation trees are:

$$\langle(x)_{\underline{i}_m}, a, (a)_i\rangle \qquad\qquad \langle\underline{n}_m, a, n\rangle$$

where there are no subcomputations because the denotations of $(x)_{\underline{i}_m}[[r]^{\mu}_{\underline{a}_m}\,;\underline{a}_m]$ and $\underline{n}_m[[r]^{\mu}_{\underline{a}_m}\,;\underline{a}_m]$ can be determined directly as $(a)_i$ and n respectively.

If $\rho \equiv h_j(\rho_1)$ then the computation tree is

$$\begin{array}{c} \langle h_j(\rho_1), a, h_j(v)\rangle \\ \langle\rho_1, a, v\rangle \\ t \end{array}$$

where we record in the left son the computation of the argument ρ_1 into the value v and then the denotation of $h_j(\rho_1)[[r]^{\mu_1}_{\underline{a}_m}\,;\underline{a}_m]$ is $h_j(v)$. There is not need to record any computation in the right son.

Finally, if $\rho \equiv r(\rho_1)$ then there are two possible computation trees:

$$\begin{array}{cc} \multicolumn{2}{c}{\langle r(\rho_1), a, w\rangle} \\ \langle\rho_1, a, v\rangle & \langle\langle\tau\rangle, v, w\rangle \\ t_1 & t_2 \end{array} \qquad\qquad \begin{array}{c} \langle r(\rho_1), a, 0\rangle \\ \langle\rho_1, a, v\rangle \\ t_1 \end{array}$$

In both cases the denotation v of the argument ρ_1 is computed in the left son. The two cases are determined by the outcome of the test $\mathcal{N} \models \mu_1[\underline{v}_m] < \mu_1[\underline{a}_m]$. If the measure decreases, i.e. if the formula $\mu_1[\underline{v}_m] < \mu_1[\underline{a}_m]$ is true in the standard model, then the computation tree is shown above on the left. This is when the identity $r(x) = \langle\tau\rangle[[r]^{\mu_1}_x ; x]$ is used as the computation rule in the form $r(\underline{v}_m) \mapsto \langle\tau\rangle[[r]^{\mu_1}_{\underline{v}_m} ; \underline{v}_m]$. The denotation w of the term $\langle\tau\rangle[[r]^{\mu_1}_{\underline{v}_m} ; \underline{v}_m]$ is computed in the right son and the denotation of the recursive application $r(\underline{v}_m)$ is determined as w.

If the outcome of the test is negative then the computation tree is shown above on the right where the denotation of $r(\underline{v}_m)$ is 0. The reader will note that the computation of $r(\rho)$ thus evaluates the guard

$$r(\rho_1)[[r]^{\mu_1}_{\underline{a}_m} ; \underline{a}_m] \equiv D(\mu_1[\rho_1[[r]^{\mu_1}_{\underline{a}_m} ; \underline{a}_m]] <_* \mu_1[x[[r]^{\mu_1}_{\underline{a}_m} ; \underline{a}_m]], r(\rho_1[[r]^{\mu_1}_{\underline{a}_m} ; \underline{a}_m]), 0) \ .$$

It should be obvious that we can construct a computation tree for any subterm ρ of $\langle\tau\rangle$ and any assignment a of the value of the variable x because the terms in the labels of the tree are always smaller except in the right sons of recursive applications but then the measure decreases and the initial measure, which is the denotation of $\mu_1[\underline{a}_m]$, can decrease only finitely many times.

The property of t being a computation tree can be expressed as follows:

> for all non-empty subtrees s of t the label of s is of a form $\langle\rho, a, v\rangle$ where ρ is a subterm of $\langle\tau\rangle$ and the relation between this label and the labels of the two sons of s is as shown in the above diagrams.

We will arithmetize the computation trees by extending in Par. 8.4.9 the theory T_1 to T_3 with the arithmetized subtree predicate $a \trianglelefteq b$ where a codes a subtree of the tree coded by b We will then extend in Par. 8.4.11 the theory T_3 to T_4 with a predicate $Ct(c)$ holding in the standard model iff c codes a computation tree t. The predicate Ct will be introduced with the help of the he predicate $Nd(a)$ expressing the local *node* relation between the label of the non-empty tree coded by a and the labels of its two sons.

8.4.9 Subtree predicate. We will now extend the theory T_1 into a theory T_3 by introducing a binary predicate $u \trianglelefteq t$ intended to hold whenever u codes a subtree of a binary tree coded by t. The empty binary tree is coded by the number 0 and the binary tree with the label b and two sons t_1, t_2 by the triple n, a_1, a_2 where a_1 and a_2 are the codes of the respective sons.

We wish the subtree predicate to satisfy the following:

$$T_3 \vdash u \trianglelefteq t \leftrightarrow u = 0 \lor u = t \lor \exists b \exists t_1 \exists t_2 (t = b, t_1, t_2 \land (u \trianglelefteq t_1 \lor u \trianglelefteq t_2)) \ . \tag{1}$$

The reader will note that such a subtree predicate $u \trianglelefteq t$ does not fully express the relation that u codes a subtree of a binary tree coded by t. In particular, we have $0 \trianglelefteq t$ even if t is not a code. But if t codes a binary tree and $u \trianglelefteq t$ holds then u codes a subtree of the tree coded by t.

Property (1) is a recurrence where the subtree predicate is applied on the right to lesser second arguments $t_1 < t$ and $t_2 < t$ than on the left. Recursive predicates are usually defined from their characteristic functions. We cannot introduce $\trianglelefteq_*$ by primitive recursion because its natural recurrences

$$\begin{gathered}(0 \trianglelefteq_* t) = 1 \\ (u \trianglelefteq_* u) = 1 \\ (u \trianglelefteq_* t_1) = 1 \lor (u \trianglelefteq_* t_2) = 1 \to (u \trianglelefteq_* b, t_1, t_2) = 1\end{gathered}$$

are of the form of so called *course of values recursion* where the recursive argument (the second one) does not decrease in the recursion to its immediate predecessor. Course of values recursion can be reduced to primitive recursion with the help ot the *course of values function* h for $\trianglelefteq_*$ such that the following holds:

$$h(t,u) = (u \trianglelefteq_* t-1), (u \trianglelefteq_* t-2), \ldots, (u \trianglelefteq_* 1), (u \trianglelefteq_* 0), 0 \; .$$

We clearly have

$$(h(t+i',u))_i \to u \trianglelefteq_* t$$

and so the values of applications $u \trianglelefteq_* t_1$ and $u \trianglelefteq_* t_2$ in the recurrences for $\trianglelefteq_*$ can be recovered from the course of values function h as $(h(t,u))_i$ where $t_1 + i' = t$ or $t_2 + i' = t$ respectively.

Preparatory to the introduction of the function h we explicitly extend T_1 into T_2 with an auxiliary ternary predicate R:

$$\begin{aligned}T_2 \vdash R(u,t,a) \leftrightarrow{} & u = 0 \lor u = t \lor \\ & \exists b \exists t_1 \exists t_2 \exists i (t = b, t_1, t_2 \land (t_1 + i' = t \lor t_2 + i' = t) \land (a)_i > 0) \; ,\end{aligned} \tag{2}$$

we also introduce into T_1 its characteristic function R_* (see Par. 8.4.2), and finally the course of values function h which is defined by primitive recursion:

$$T_2 \vdash h(0,u) = 0 \tag{3}$$

$$T_2 \vdash h(t',u) = R_*(u,t,h(t,u)), h(t,u) \; . \tag{4}$$

The reader will note that the characteristic function $\trianglelefteq_*$ for $\trianglelefteq$ could be now introduced into T_2 (but we will not need to do this) by explicit definition $u \trianglelefteq_* t = R_*(u,t,h(t,u))$ because of the following property:

$$T_2 \vdash (h(s+i',u))_i = R_*(u,s,h(s,u)) \tag{5}$$

which is proved in T_2 by induction on i. In the base case we have

$$(h(s{+}0',u))_0 = (h(s',u))_0 = (R_*(u,s,h(s,u)), h(s,u))_0 \overset{8.3.18(2)}{=} R_*(u,s,h(s,u)) \; .$$

In the inductive case we have

$$
\begin{aligned}
(h(s+i'',u))_{i'} = {} & (h((s+i')',u))_{i'} = \\
& (R_*(u,s+i',h(s+i',u)),h(s+i',u))_{i'} \overset{8.3.18(3)}{=} \\
& (h(s+i',u))_i \overset{\mathrm{IH}}{=} R_*(u,s,h(s,u)) \ .
\end{aligned}
$$

We are now ready to extend T_2 into T_3 by introducing the subtree predicate by explicit definition:

$$
T_3 \vdash u \trianglelefteq t \leftrightarrow R(u,t,h(t,u)) \ . \tag{6}
$$

The predicate satisfies the following auxilary property:

$$
T_3 \vdash u \trianglelefteq s \land s < t \leftrightarrow \exists i(s+i' = t \land (h(t,u))_i > 0) \tag{7}
$$

for which we have $u \trianglelefteq s$ and $s < t$ iff $R(u,s,h(s,u))$ and $s < t$ iff, by 8.4.2(3), $R_*(u,s,h(s,u)) > 0$ and $s+i' = t$ for some i iff, by (5), $(h(t,u))_i > 0$ and $s+i' = t$ for some i.

We are now ready to prove in T_3 the basic recurrence (1) for the subtree predicate. We have $u \trianglelefteq t$ iff $R(u,t,h(t,u))$ iff, by (2), $(u = 0 \lor u = t)$ or $t = b,t_1,t_2$, $(t_1+i' = t \lor t_2+i' = t)$, and $(h(t,u))_i > 0$ for some b, t_1, t_2, and i iff $(u = 0 \lor u = t)$ or $t = b,t_1,t_2$ and

$$
\exists i(t_1+i' = t \land (h(t,u))_i > 0) \lor \exists i(t_2+i' = t \land (h(t,u))_i > 0)
$$

for some b, t_1, t_2 iff, by (7), $(u = 0 \lor u = t)$ or $t = b,t_1,t_2$ and

$$
t_1 < t \land u \trianglelefteq t_1 \lor t_2 < t \land u \trianglelefteq t_2
$$

for some b, t_1, t_2 iff, by 8.3.16(3), $(u = 0 \lor u = t)$ or $t = b,t_1,t_2$ and $(u \trianglelefteq t_1 \lor u \trianglelefteq t_2)$ for some b, t_1, t_2.

8.4.10 Codes of special terms. Special terms are arithmetized by encoding into numbers. To that end we introduce the following *constructor* functions operating on terms:

$$
\begin{aligned}
\boldsymbol{X}_\rho &\equiv 0,\rho \qquad (1)\\
\boldsymbol{N}(\rho) &\equiv 1,\rho \qquad (2)\\
\boldsymbol{P}(\rho_1,\rho_2) &\equiv 2,\rho_1,\rho_2 \qquad (3)\\
\boldsymbol{H}_{\rho_1}(\rho_2) &\equiv 3,\rho_1,\rho_2 \qquad (4)\\
\boldsymbol{R}(\rho) &\equiv 4,\rho \ . \qquad (5)
\end{aligned}
$$

Constructor meta-functions are used to assign codes $\ulcorner \rho \urcorner$ (Gödel numbers) to special terms ρ to satisfy:

$$\begin{aligned}
\ulcorner (x)_{\underline{i}_m} \urcorner &\equiv \boldsymbol{X}_{\underline{i}_m} && (6)\\
\ulcorner \underline{m}_m \urcorner &\equiv \boldsymbol{N}(\underline{m}_m) && (7)\\
\ulcorner \tau_1, \tau_2 \urcorner &\equiv \boldsymbol{P}(\ulcorner \tau_1 \urcorner, \ulcorner \tau_2 \urcorner) && (8)\\
\ulcorner h_j(\tau) \urcorner &\equiv \boldsymbol{H}_{\underline{j}_m}(\ulcorner \tau \urcorner) && (9)\\
\ulcorner r(\tau) \urcorner &\equiv \boldsymbol{R}(\ulcorner \tau \urcorner)\ . && (10)
\end{aligned}$$

The reader will note that $\ulcorner \rho \urcorner$ stands for a closed term of $\mathcal{L}_{T_2}$ whose interpretation in the standard model of PA denotes the code of the special term ρ. Specifically, $\ulcorner \underline{3}_m \urcorner$ stands for the term $\boldsymbol{N}(0''')$ which denotes the same number as the term $1, 3$, i.e. the number 15.

The reader may ask why we have defined the constructor function as meta-functions yielding terms rather than as functions in PA? The reason for that will be seen in Par. 8.4.13 where it will be essential that the terms constructed with the help of constructors are of $\mathcal{L}_T$.

8.4.11 The predicate $\boldsymbol{Ct}$**.** We will now extend the theory T_3 to T_4 by introducing the predicate $Ct(t)$ holding of codes t of computation trees. We arithmetize (encode) the empty computation tree as the number 0 and the tree

$$\begin{array}{ccc} & \langle \rho, a, v \rangle & \\ \diagup & & \diagdown \\ \cdots t_1 \cdots & & \cdots t_2 \cdots \end{array}$$

by the number denoted by the term

$$(\ulcorner \rho \urcorner, \underline{a}_m, \underline{v}_m), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner$$

where $\ulcorner t_1 \urcorner$ and $\ulcorner t_2 \urcorner$ encode the two sons respectively. The predicate is defined with the help of an auxiliary unary predicate $Nd(t)$ holding iff the labels of t and of its sons satisfy the local *node* conditions discussed in Par. 8.4.8.

Both predicates are introduced by explicit definitions:

$$\begin{aligned}
&T_4 \vdash Nd(t) \leftrightarrow \exists c \exists a \exists v \exists t_1 \exists t_2 (t = (c, a, v), t_1, t_2 \land (\\
&\qquad \exists i (c = \boldsymbol{X}_i \land i < n \land v = (a)_i \land t_1 = 0 \land t_2 = 0) \lor\\
&\qquad \exists m (c = \boldsymbol{N}(m) \land v = n \land t_1 = 0 \land t_2 = 0) \lor\\
&\qquad \exists c_1 \exists c_2 \exists v_1 \exists v_2 \exists s_1 \exists s_2 (c = \boldsymbol{P}(c_1, c_2) \land v = v_1, v_2 \land\\
&\qquad\quad t_1 = (c_1, a, v_1), s_1 \land t_2 = (c_2, a, v_2), s_2) \lor\\
&\qquad \exists c_1 \exists j \exists w \exists s_1 (c = \boldsymbol{H}_j(c_1) \land t_1 = (c_1, a, w), s_1 \land t_2 = 0 \land\\
&\qquad\quad (j = \underline{1}_m \land v = h_1(w) \lor \ldots \lor j = \underline{k}_m \land v = h_k(w))) \lor\\
&\qquad \exists c_1 \exists w \exists s_1 \exists s_2 (c = \boldsymbol{R}(c_1) \land t_1 = (c_1, a, w), s_1 \land\\
&\qquad\quad (\mu_1[w] < \mu_1[a] \land t_2 = (\ulcorner \tau \urcorner, w, v), s_2 \lor\\
&\qquad\quad \mu_1[w] \geq \mu[a] \land v = 0 \land t_2 = 0))) && (1)\\
&T_4 \vdash Ct(t) \leftrightarrow \forall u (u \trianglelefteq t \land u > 0 \rightarrow Nd(u))\ . && (2)
\end{aligned}$$

and Ct satisfies the following:

$$T_4 \vdash Ct(0) \tag{3}$$
$$T_4 \vdash i < n \to Ct((\boldsymbol{X}_i, a, (a)_i), 0, 0) \tag{4}$$
$$T_4 \vdash Ct((\boldsymbol{N}(m), a, m), 0, 0) \tag{5}$$
$$\begin{aligned} T_4 \vdash\ & Ct((c_1, a, v_1), s_1) \wedge Ct((c_2, a, v_2), s_2) \to \\ & \quad Ct((\boldsymbol{P}(c_1, c_2), a, v_1, v_2), ((c_1, a, v_1), s_1), ((c_2, a, v_2), s_2)) \end{aligned} \tag{6}$$
$$T_4 \vdash Ct((c, a, v), s) \to Ct((\boldsymbol{H}_{\underline{j}_m}(c), a, h_j(v)), ((c, a, v), s), 0) \tag{7}$$
$$\begin{aligned} T_4 \vdash\ & Ct((c, a, v), s_1) \wedge \mu_1[v] < \mu_1[a] \wedge Ct((\ulcorner\langle\tau\rangle\urcorner, v, w), s_2) \to \\ & \quad Ct((\boldsymbol{R}(c), a, w), ((c, a, v), s_1), ((\ulcorner\langle\tau\rangle\urcorner, v, w), s_2)) \end{aligned} \tag{8}$$
$$T_4 \vdash Ct((c, a, v), s_1) \wedge \mu_1[v] \geq \mu_1[a] \to Ct((\boldsymbol{R}(c), a, 0), ((c, a, v), s_1), 0) \tag{9}$$
$$T_4 \vdash Ct(b, t_1, t_2) \to Ct(t_1) \wedge Ct(t_2)\ . \tag{10}$$

Property (7) is a schema of k theorems one for each $1 \leq j \leq k$. Properties (3) through (9) can be called *sufficient* conditions for computation trees to be constructed out of smaller trees. The property (10) can be seen as stating a *necessary* condition for a triple b, t_1, t_2 to be a computation tree.

(3): This holds trivially.

(4): Assume $i < n$ and take any $u > 0$ such that $u \trianglelefteq (\boldsymbol{X}_i, a, (a)_i), 0, 0$. Since $u \trianglelefteq 0$ leads to contradiction $u = 0$, it must be the case that $u = (\boldsymbol{X}_i, a, (a)_i)), 0, 0$ by 8.4.9(1) and thus $Nd(u)$. This proves the consequent.

(5): Take any $u > 0$ such that $u \trianglelefteq (\boldsymbol{N}(m), a, m), 0, 0$. Since $u \trianglelefteq 0$ leads to contradiction $u = 0$, it must be the case that $u = (\boldsymbol{N}(m), a, m), 0, 0$ by 8.4.9(1) and thus $Nd(u)$. This proves the consequent.

(6): Assume $Ct((c_1, a, v_1), s_1)$, $Ct((c_2, a, v_2), s_2)$. For

$$t := (\boldsymbol{P}(c_1, c_2), a, v_1, v_2), ((c_1, a, v_1), s_1), ((c_2, a, v_2), s_2)$$

we wish to prove $Ct(t)$. We thus take any $u > 0$ such that $u \trianglelefteq t$. We consider the three cases implied by 8.4.9(1). If $u = t$ then we can see that $Nd(u)$ and hence $Ct(t)$ hold. If $u \trianglelefteq (c_1, a, v_1), s_1$ then we obtain $Nd(u)$ and hence $Ct(t)$ from the assumption $Ct((c_1, a, v_1), s_1)$. If $u \trianglelefteq (c_2, a, v_2), s_2$ then we obtain $Nd(u)$ and hence $Ct(t)$ from the assumption $Ct((c_2, a, v_2), s_2)$.

(7): Take any $1 \leq j \leq k$ and assume $Ct((c, a, v), s)$. For

$$t := (\boldsymbol{H}_{\underline{j}_m}(c), a, h_j(v)), ((c, a, v), s), 0$$

we wish to prove $Ct(t)$. We thus take any $u > 0$ such that $u \trianglelefteq t$. Since $u \trianglelefteq 0$ leads to contradiction $u = 0$, we consider the two cases implied by 8.4.9(1). If $u = t$ then we can see that $Nd(u)$ and hence $Ct(t)$ hold. If $u \trianglelefteq (c, a, v), s$ we obtain $Nd(u)$, and hence $Ct(t)$, from the assumption $Ct((c, a, v), s)$.

(8): Assume $Ct((c, a, v), s_1)$, $\mu_1[v] < \mu_1[a]$, $Ct((\ulcorner\langle\tau\rangle\urcorner, v, w), s_2)$, and for

$$t := (\boldsymbol{R}(c), a, w), ((c, a, v), s_1), ((\ulcorner\langle\tau\rangle\urcorner, v, w), s_2)$$

we wish to prove $Ct(t)$. We thus take any $u > 0$ such that $u \trianglelefteq t$. We consider the three cases implied by 8.4.9(1). If $u = t$ then we can see that $Nd(u)$ and hence $Ct(t)$ hold. If $u \trianglelefteq (c, a, v), s_1$ or $u \trianglelefteq (\ulcorner\langle\tau\rangle\urcorner, v, w), s_2$ then we obtain $Nd(u)$, and hence $Ct(t)$ from the corresponding assumptions on Ct.

(9): Assume $Ct((c, a, v), s_1)$, $\mu_1[v] \geq \mu_1[a]$, and for

$$t := (\boldsymbol{R}(c), a, 0), ((c, a, v), s_1), 0$$

we wish to prove $Ct(t)$. We thus take any $u > 0$ such that $u \trianglelefteq t$. Since $u \trianglelefteq 0$ leads to contradiction $u = 0$, we consider the two cases implied by 8.4.9(1). If $u = t$ then we can see that $Nd(u)$ and hence $Ct(t)$ hold. If $u \trianglelefteq (c, a, v), s_1$ then we obtain $Nd(u)$, and hence $Ct(t)$, from the assumption $Ct((c, a, v), s_1)$.

(10): Assume $Ct(b, t_1, t_2)$ and for the proof of $Ct(t_1)$ take any $u > 0$ such that $u \trianglelefteq t_1$. We have $u \trianglelefteq b, t_1, t_2$ by 8.4.9(1), $Nd(u)$ from the assumption by (2), and hence $Ct(t_1)$ by (2). We prove $Ct(t_2)$ similarly.

8.4.12 Existence and uniqueness properties for r. We could now introduce the function r by the implicit definition $\exists s\, Ct((\ulcorner\langle\tau\rangle\urcorner, x, r(x)), s)$ and prove that it solves the identity $r(x) = \langle\tau\rangle[[r]^{\mu_1}_x; x]$. In the proof of Theorem 8.4.14 we will introduce instead the n-ary function f directly by an implicit axiom equivalent to

$$\exists s\, Ct((\ulcorner\langle\tau\rangle\urcorner, (x_1, \ldots, x_n, 0), f(x_1, \ldots, x_n)), s)$$

and then solve the identity $f(\vec{x}) = \tau[[f]^{\mu}_{\vec{x}}; \vec{x}]$.

In any case we will need the following properties from which the existence uniqueness conditions for r and f will follow:

$$T_4 \vdash \exists y \exists s\, Ct((\ulcorner\langle\tau\rangle\urcorner, x, y), s) \tag{1}$$

$$T_4 \vdash Ct((c, x, y_1), s_1) \wedge Ct((c, x, y_2), s_2) \rightarrow y_1 = y_2 \wedge s_1 = s_2\ . \tag{2}$$

(1): We first prove the following auxiliary properties:

$$T_4 \vdash \forall v(\mu_1[v] < \mu_1[x] \rightarrow \exists y \exists s\, Ct((\ulcorner\langle\tau\rangle\urcorner, v, y), s)) \rightarrow \exists y \exists s\, Ct((\ulcorner\rho\urcorner, x, y), s)\ . \tag{3}$$

for the finitely many subterms ρ of $\langle\tau\rangle$ in the order of their construction, i.e. by the meta-theoretical induction on the construction of the special term ρ. So assume the antecedent

$$\forall v(\mu_1[v] < \mu_1[x] \rightarrow \exists y \exists s\, Ct((\ulcorner\langle\tau\rangle\urcorner, v, y), s) \tag{4}$$

and continue by the case analysis of the special term ρ where we wish to find a y and s such that $Ct((\ulcorner\rho\urcorner, x, y), s)$.

If $\rho \equiv (x)_{\underline{i}_m}$ where $i < n = \underline{n}_m$ then $\ulcorner\rho\urcorner \equiv \boldsymbol{X}_i$, we use 8.4.11(4), and set $y := (x)_i$, $s := 0, 0$.

If $\rho \equiv \underline{m}_m$ then $\ulcorner\rho\urcorner \equiv \boldsymbol{N}(\underline{m}_m)$, we use 8.4.11(5), and set $y := \underline{m}_m$, $s := 0, 0$.

If $\rho \equiv \rho_1, \rho_2$ then $\ulcorner\rho\urcorner \equiv \boldsymbol{P}(\ulcorner\rho_1\urcorner, \ulcorner\rho_2\urcorner)$ and we have

$$T_4 \vdash (4) \rightarrow \exists y \exists s\, Ct((\ulcorner\rho_1\urcorner, x, y), s)$$
$$T_4 \vdash (4) \rightarrow \exists y \exists s\, Ct((\ulcorner\rho_2\urcorner, x, y), s)$$

by two inductive meta-hypotheses. We use the assumption (4) and obtain $Ct((\ulcorner\rho_1\urcorner, x, y_1), s_1)$, $Ct((\ulcorner\rho_2\urcorner, x, y_2), s_2)$ for some y_1, y_2, s_1, and s_2. We now use 8.4.11(6) and set $y := y_1, y_2$, $s := ((\ulcorner\rho_1\urcorner, x, y_1), s_1), ((\ulcorner\rho_2\urcorner, x, y_2), s_2)$.

If $\rho \equiv h_j(\rho_1)$ where $1 \leq j \leq k$ then $\ulcorner\rho\urcorner \equiv \boldsymbol{H}_{\underline{j}_m}(\ulcorner\rho_1\urcorner)$ and we have $Ct((\ulcorner\rho_1\urcorner, x, v), s_1)$ for some v and s_1 from the inductive meta-hypothesis. We now use 8.4.11(7) and set $y := h_j(v)$, $s := ((\ulcorner\rho_1\urcorner, x, v), s_1), 0$.

If $\rho \equiv r(\rho_1)$ then $\ulcorner\rho\urcorner \equiv \boldsymbol{R}(\ulcorner\rho_1\urcorner)$ and we have $Ct((\ulcorner\rho_1\urcorner, x, v), s_1)$ for some v and s_1 from the inductive meta-hypothesis. We now consider two cases. If $\mu_1[v] < \mu_1[x]$ we have $Ct((\ulcorner\langle\tau\rangle\urcorner, v, z), s_2)$ for some w and s_2 from (4) and it suffices now to use 8.4.11(8) and set $y := w$, $s := ((\ulcorner\rho_1\urcorner, x, v), s_1), ((\ulcorner\langle\tau\rangle\urcorner, v, w), s_2)$. If $\mu_1[v] \geq \mu_1[x]$ then it suffices to use 8.4.11(9) and set $y := 0$, $s := ((\ulcorner\rho_1\urcorner, x, v), s_1), 0$. This ends the proof of the auxiliary properties (3).

We now prove (1) by measure induction with $\mu_1[x]$. The induction hypothesis is (4) and the property follows from it by (3) with $\rho := \langle\tau\rangle$.

(2): We prove

$$T_4 \vdash \forall c \forall x \forall y_1 \forall y_2 \forall s_2 (Ct((c, x, y_1), s_1) \land Ct((c, x, y_2), s_2) \rightarrow y_1 = y_2 \land s_1 = s_2) \tag{5}$$

by complete induction on s_1. So we take any c, x, y_1, y_2, s_2, and assume $Ct((c, x, y_1), s_1)$, $Ct((c, x, y_2), s_2)$. We have $(c, x, y_1), s_1 \trianglelefteq (c, x, y_1), s_1$ by 8.4.9(1),

$$Nd((c, x, y_1), s_1) \tag{6}$$

by 8.4.11(2), $s_1 = t_1, t_2$ for some t_1 and t_2 by 8.4.11(1), and $Ct(t_1)$, $Ct(t_2)$ by 8.4.11(10). We similarly obtain

$$Nd((c, x, y_2), s_2)\ , \tag{7}$$

$s_2 = u_1, u_2$, $Ct(u_1)$, and $Ct(u_2)$ for some u_1 and u_2.

We now consider the cases implied by (6) and (7) where we wish to prove $y_1 = y_2$, $t_1 = u_1$, and $t_2 = u_2$.

If $c = \boldsymbol{X}_i$ for some i then we have $i < n$, $y_1 = (x)_i = y_2$, $t_1 = 0 = u_1$, and $t_2 = 0 = u_2$.

If $c = \boldsymbol{N}(m)$ for some m then we have $y_1 = m = y_2$, $t_1 = 0 = u_1$, and $t_2 = 0 = u_2$.

If $c = \boldsymbol{P}(c_1, c_2)$ for some c_1, c_2 then we have $y_1 = w_1, w_2$, $t_1 = (c_1, x, w_1), s_3$; $t_2 = (c_2, x, w_2), s_4$ for some w_1, w_2, s_3, s_4 by (6) and $y_2 =$

z_1, z_2; $u_1 = (c_1, x, z_1), s_5$; $u_2 = (c_2, x, z_2), s_6$ for some z_1, z_2, s_5, s_6 by (7). Since $s_3 < t_1 < s_1$, we get $w_1 = z_1$; $s_3 = s_5$ from $Ct(t_1)$, $Ct(u_1)$ by IH. Similarly, since $s_4 < t_2 < s_1$, we get $w_2 = z_2$; $s_4 = s_6$ from $Ct(t_2)$, $Ct(u_2)$ by IH. Hence $y_1 = y_2$; $t_1 = u_1$; and $t_2 = u_2$.

If $c = \boldsymbol{H}_i(c_1)$ for some i, c_1 then we have

$$i = \underline{1}_m \wedge y_1 = h_1(w) \vee \ldots \vee i = \underline{k}_m \wedge y_1 = h_k(w) \ ,$$

$t_1 = (c_1, x, w), s_3$; $t_2 = 0$ for some w and s_3 by (6) and

$$i = \underline{1}_m \wedge y_2 = h_1(z) \vee \ldots \vee i = \underline{k}_m \wedge y_2 = h_k(z) \ ,$$

$u_1 = (c_1, x, z), s_4$; $u_2 = 0$ for some z and s_4 by (7). Since $s_3 < t_1 < s_1$, we get $w = z$; $s_3 = s_4$ by IH from $Ct(t_1)$, $Ct(u_1)$. Hence $y_1 = y_2$; $t_1 = u_1$; and $t_2 = u_2$.

If $c = \boldsymbol{R}(c_1)$ for some c_1 then we have $t_1 = (c_1, x, w), s_3$ for some w and s_3 by (6) and $u_1 = (c_1, x, z), s_4$ for some z and s_4 by (7). Since $s_3 < t_1 < s_1$, we get $w = z$, $s_3 = s_4$ by IH from $Ct(t_1)$, $Ct(u_1)$. Hence $t_1 = u_1$. We now consider two cases. If $\mu_1[w] < \mu_1[x]$ then we have $t_2 = \ulcorner\tau\urcorner, w, y_1, s_5$ for some s_5 by (6) and $u_2 = \ulcorner\tau\urcorner, z, y_2, s_6$ for some s_6 by (7). Since $s_5 < t_2 < s_1$, $w = z$, we get $y_1 = y_2$, $s_5 = s_6$ by IH from $Ct(t_2)$, $Ct(u_2)$. Hence $t_2 = u_2$. If $\mu_1[w] \geq \mu_1[x]$ then we have $y_1 = 0 = y_2$ and $t_2 = 0 = u_2$ by (6), (7).

8.4.13 Graph of the arithmetized denotation function for subterms of τ. We will now effectively determine an $(n+2)$-ary formula $\phi[c, \vec{x}, y]$ of $\mathcal{L}_T$ with the free variables among the indicated ones, which is used in the induction axiom 8.4.6(2) of S. The formula can be viewed as the graph of the arithmetized denotation function for the subterms ρ of τ because we will have $\mathbb{N} \models \phi[\ulcorner\langle\rho\rangle\urcorner, \vec{x}, y]$ in the standard model of S iff y is the denotation of the term $\rho[[f]^{\mu}_{\vec{x}}, \vec{x}]$ in the assignment $\vec{x}$.

Since T_4 is an extension by definitions of T, the formula $\phi[c, x_1, \ldots, x_n, y]$ is effectively obtained from the formula

$$\exists s\, Ct((c, (x_1, \ldots, x_n, 0), y), s)$$

of $\mathcal{L}_{T_4}$ by translation and in such a way that we have

$$T_4 \vdash \phi[c, x_1, \ldots, x_n, y] \leftrightarrow \exists s\, Ct((c, (x_1, \ldots, x_n, 0), y), s) \qquad (1)$$

by the Theorem on Extensions by definition 6.6.2. We will need the following properties of the formula ϕ:

$$T \vdash \exists y \phi[\ulcorner\langle\tau\rangle\urcorner, \vec{x}, y] \tag{2}$$
$$T \vdash \phi[c, \vec{x}, y_1] \wedge \phi[c, \vec{x}, y_2] \to y_1 = y_2 \tag{3}$$
$$T \vdash \phi[\boldsymbol{X}_{\underline{i-1}_m}, \vec{x}, x_i] \tag{4}$$
$$T \vdash \phi[\boldsymbol{N}(m), \vec{x}, m] \tag{5}$$
$$T \vdash \phi[c_1, \vec{x}, v_1] \wedge \phi[c_2, \vec{x}, v_2] \to \phi[\boldsymbol{P}(c_1, c_2), \vec{x}, (v_1, v_2)] \tag{6}$$
$$T \vdash \phi[c, \vec{x}, (v_1, \ldots, v_{n_j}, 0)] \to \phi[\boldsymbol{H}_{\underline{j}_m}(c), \vec{x}, g_j(v_1, \ldots, v_{n_j})] \tag{7}$$
$$T \vdash \phi[c, \vec{x}, (v_1, \ldots, v_n, 0)] \wedge \mu[v_1, \ldots, v_n] < \mu[\vec{x}] \wedge$$
$$\phi[\ulcorner\langle\tau\rangle\urcorner, v_1, \ldots, v_n, w] \to \phi[\boldsymbol{R}(c), \vec{x}, w] \tag{8}$$
$$T \vdash \phi[c, \vec{x}, (v_1, \ldots, v_n, 0)] \wedge \mu[v_1, \ldots, v_n] \geq \mu[\vec{x}] \to$$
$$\phi[\boldsymbol{R}(c), \vec{x}, 0] \ . \tag{9}$$

for every $1 \leq i \leq n$ and $1 \leq j \leq k$. In the following proofs we work in T_4 and use the equivalence (1) without explicitly referring to it. Properties (2) through (9) are thus derived in T_4 but, since they all are in the language $\mathcal{L}_T$, they are also theorems of T because T_4 is conservative over T.

(2): A direct consequence of 8.4.12(1).

(3): A direct consequence of 8.4.12(2).

(4): Take an i s.t. $1 \leq i \leq n$. Since T_4 proves $\underline{i-1}_m < n$ and

$$(x_1, \ldots, x_n, 0)_{\underline{i-1}_m} = x_i \ ,$$

we get $Ct((\boldsymbol{X}_{\underline{i-1}_m}, (x_1, \ldots, x_n, 0), x_i), 0, 0)$ by 8.4.11(4) and then

$$\exists s \, Ct((\boldsymbol{X}_{\underline{i-1}_m}, (x_1, \ldots, x_n, 0), x_i), s) \ .$$

(5): A direct consequence of 8.4.11(5).

(6): A direct consequence of 8.4.11(6).

(7): Take any j s.t. $1 \leq j \leq k$ and assume the antecedent. Then $Ct((c, (x_1, \ldots, x_n, 0), (v_1, \ldots, v_{n_j}, 0)), s_1)$ for some s_1 and we get

$$\exists s \, Ct((\boldsymbol{H}_{\underline{j}_m}(c), (x_1, \ldots, x_n, 0), h_j(v_1, \ldots, v_{n_j}, 0)), s)$$

by 8.4.11(7). We now use 8.4.7(2) to get

$$\exists s \, Ct((\boldsymbol{H}_{\underline{j}_m}(c), (x_1, \ldots, x_n, 0), g_j(v_1, \ldots, v_{n_j})), s) \ .$$

(8): Assume the antecedent. Then $Ct((c, (x_1, \ldots, x_n, 0), (v_1, \ldots, v_n, 0)), s_1)$, $\mu[v_1, \ldots, v_n] < \mu[x_1, \ldots, x_n]$, and $Ct((\ulcorner\langle c\rangle\urcorner, (v_1, \ldots, v_n, 0), w), s_2)$, for some s_1, s_2. We have $\mu_1[(v_1, \ldots, v_n, 0)] < \mu_1[(x_1, \ldots, x_n, 0)]$ by 8.4.7(3) and $\exists s \, Ct((\boldsymbol{R}(c), (x_1, \ldots, x_n, 0), w), s)$ by 8.4.11(8).

(9): This is similar to and somewhat simpler than (8).

8.4.14 Theorem. *If T is a proper extension of PA containing the pairing function (x,y), the case discrimination function $D(x,y,z)$, as well as the characteristic function $<_*$ of the predicate $<$ then an extension of T by course of values recursion with measure is an extension by definition.*

Proof. Let T be as in the theorem, S an extension of T by course of values recursion with measure as in Par. 8.4.6, and S_1 an extension of T by implicit definition with the defining axiom an universal closure of $\phi[\ulcorner\langle\tau\rangle\urcorner,\vec{x},f(\vec{x})]$. We have $\mathcal{L}_{S_1}=\mathcal{L}_S$ and S_1 is an extension by definition of T by Thm. 6.6.3 because T proves the existence 8.4.13(2) and uniqueness 8.4.13(3) conditions for f. Clearly

$$S_1 \vdash \phi[\ulcorner\langle\tau\rangle\urcorner,\vec{x},f(\vec{x})] \ . \tag{1}$$

In order to prove the theorem it suffices to prove that the theories S and S_1 are equivalent.

For the proof $S_1 \vdash S$ we derive auxiliary properties

$$S_1 \vdash \phi[\ulcorner\langle\rho\rangle\urcorner,\vec{x},\rho[[f]^{\mu}_{\vec{x}};\vec{x}]] \tag{2}$$

for the finitely many subterms ρ of τ by the meta-induction on the construction of ρ.

If $\rho\equiv x_i$ where $1\le i\le n$ then, since $\ulcorner\langle x_i\rangle\urcorner\equiv\ulcorner(x)_{\underline{i-1}_m}\urcorner\equiv\boldsymbol{X}_{\underline{i-1}_m}$, we have $\phi[\boldsymbol{X}_{\underline{i-1}_m},\vec{x},x_i]$ by 8.4.13(4) and we note that $x_i[[f]^{\mu}_{\vec{x}};\vec{x}]\equiv x_i$.

If $\rho\equiv\underline{m}_m$ then, since $\ulcorner\langle\underline{m}_m\rangle\urcorner\equiv\ulcorner\underline{m}_m\urcorner\equiv\boldsymbol{N}(\underline{m}_m)$, we have $\phi[\boldsymbol{N}(\underline{m}_m),\vec{x},\underline{m}_m]$ by 8.4.13(5) and we note that $\underline{m}_m[[f]^{\mu}_{\vec{x}};\vec{x}]\equiv\underline{m}_m$.

If $\rho\equiv g_j(\rho_1,\ldots,\rho_{n_j})$ where $1\le j\le k$ we obtain $\phi[\ulcorner\langle\rho_1\rangle\urcorner,\vec{x},\rho_1[[f]^{\mu}_{\vec{x}};\vec{x}]]$, $\ldots$, $\phi[\ulcorner\langle\rho_{n_j}\rangle\urcorner,\vec{x},\rho_n[[f]^{\mu}_{\vec{x}};\vec{x}]]$ by n_j inductive meta-hypotheses. Since for

$$c=\boldsymbol{P}(\ulcorner\langle\rho_1\rangle\urcorner,\ldots,\boldsymbol{P}(\ulcorner\langle\rho_{n_j}\rangle\urcorner,\boldsymbol{N}(0))\ldots)\equiv\ulcorner\langle\rho_1\rangle,\ldots,\langle\rho_{n_j}\rangle,0\urcorner$$

we have

$$\ulcorner\langle g_j(\rho_1,\ldots,\rho_{n_j})\rangle\urcorner\equiv\ulcorner h_j(\langle\rho_1\rangle,\ldots,\langle\rho_{n_j}\rangle,0)\urcorner\equiv\boldsymbol{H}_{\underline{j}_m}(c)\ ,$$

we get

$$\phi[c,\vec{x},(\rho_1[[f]^{\mu}_{\vec{x}};\vec{x}],\ldots,\rho_{n_j}[[f]^{\mu}_{\vec{x}};\vec{x}],0)]$$

by n_j applications of 8.4.13(6) and then

$$\phi[\boldsymbol{H}_{\underline{j}_m}(c),\vec{x},g_j(\rho_1[[f]^{\mu}_{\vec{x}};\vec{x}],\ldots,\rho_{n_j}[[f]^{\mu}_{\vec{x}};\vec{x}])]$$

by 8.4.13(7). We are done since

$$g_j(\rho_1,\ldots,\rho_{n_j})[[f]^{\mu}_{\vec{x}};\vec{x}]\equiv g_j(\rho_1[[f]^{\mu}_{\vec{x}};\vec{x}],\ldots,\rho_{n_j}[[f]^{\mu}_{\vec{x}};\vec{x}])\ .$$

If $\rho\equiv f(\rho_1,\ldots,\rho_n)$ we obtain $\phi[\ulcorner\langle\rho_1\rangle\urcorner,\vec{x},\rho_1[[f]^{\mu}_{\vec{x}};\vec{x}]],\ldots,\phi[\ulcorner\langle\rho_n\rangle\urcorner,\vec{x},\rho_n[[f]^{\mu}_{\vec{x}};\vec{x}]]$ by n inductive meta-hypotheses. Since for

$$c = \boldsymbol{P}(\ulcorner\langle\rho_1\rangle\urcorner,\ldots,\boldsymbol{P}(\ulcorner\langle\rho_n\rangle\urcorner,\boldsymbol{N}(0))\ldots) \equiv \ulcorner\langle\rho_1\rangle,\ldots,\langle\rho_n\rangle,0\urcorner$$

we have

$$\ulcorner\langle f(\rho_1,\ldots,\rho_n)\rangle\urcorner \equiv \ulcorner r(\langle\rho_1\rangle,\ldots,\langle\rho_n\rangle,0)\urcorner \equiv \boldsymbol{R}(c)\ ,$$

we get

$$\phi[c,\vec{x},(\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}],0)]$$

by n applications of 8.4.13(6). We now consider two cases. If

$$\mu[\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}]] < \mu[\vec{x}] \tag{3}$$

then from (1) we obtain

$$\phi[\ulcorner\langle\tau\rangle\urcorner,\vec{x},f(\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}])] \tag{4}$$

and from 8.4.13(8) $\phi[\boldsymbol{R}(c),\vec{x},f(\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}])]$. We are done because

$$\begin{aligned} f(\rho_1,\ldots,\rho_n)[[f]^\mu_{\vec{x}};\vec{x}] \equiv D((&\mu[\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}]] <_* \mu[\vec{x}]),\\ &f(\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}]),0) =\\ &f(\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}])\ . \end{aligned}$$

If not (3) then we get $\phi[\boldsymbol{R}(c),\vec{x},0]$ by 8.4.13(9) and we are done because

$$\begin{aligned} f(\rho_1,\ldots,\rho_n)[[f]^\mu_{\vec{x}};\vec{x}] \equiv D((&\mu[\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}]] <_* \mu[\vec{x}]),\\ &f(\rho_1[[f]^\mu_{\vec{x}};\vec{x}],\ldots,\rho_n[[f]^\mu_{\vec{x}};\vec{x}]),0) = 0\ . \end{aligned}$$

With (2) proved, we derive the defining axiom 8.4.6(1) of S for f: $S_1 \vdash f(\vec{x}) = \tau[[f]^\mu_{\vec{x}};\vec{x}]$ by 8.4.13(3) from (1) and from (2) where we take the subterm τ of τ for ρ. Since S_1 is proper, it also proves the induction axiom 8.4.6(2) of S by Thm. 8.4.5.

Vice versa, for the proof $S \vdash S_1$ we derive auxiliary properties

$$S \vdash \forall\vec{v}(\mu[\vec{v}] < \mu[\vec{x}] \to \phi[\ulcorner\langle\tau\rangle\urcorner,\vec{v},f(\vec{y})]) \to \phi[\ulcorner\langle\rho\rangle\urcorner,\vec{x},\rho[[f]^\mu_{\vec{x}};\vec{x}]] \tag{5}$$

for the finitely many subterms ρ of τ by the meta-induction on the construction of ρ. So we assume

$$\forall\vec{v}(\mu[\vec{v}] < \mu[\vec{x}] \to \phi[\ulcorner\langle\tau\rangle\urcorner,\vec{v},f(\vec{y})]) \tag{6}$$

and continue by the case analysis of ρ exactly as in the proof of (2) where the only difference is in the case when $\rho \equiv f(\rho_1,\ldots,\rho_n)$ and (3) holds. We obtain (4) from the assumption (6) rather than from (1) as was the case above.

With (5) proved, we derive the defining axiom (1) for f in S_1: $S \vdash \phi[\ulcorner\langle\tau\rangle\urcorner,\vec{x},f(\vec{x})]$ by the induction axiom with measure 8.4.6(2) where we assume (6) and use (5) with the subterm τ of τ for ρ to get $\phi[\ulcorner\langle\tau\rangle\urcorner,\vec{x},\tau[[f]^\mu_{\vec{x}};\vec{x}]]$. We now get (1) from the defining axiom 8.4.6(1) for f in S. □

9. Proof Theory of PA

UNFINISHED Gentzen was first. but we need the strength of induction schemas for the characterization purposes by means of provably recursive functions.

Miscellaneous

9.0.15 Theorem. *We have*

$$\vdash_{PA} \exists q \exists r(x = q \cdot y + r \wedge r < y \wedge \phi[q,r]) \leftrightarrow y \neq 0 \wedge \phi[x \div y, x \bmod y] \tag{1}$$
$$\vdash_{PA} \forall q \forall r(x = q \cdot y + r \wedge r < y \rightarrow \phi[q,r]) \leftrightarrow (y \neq 0 \rightarrow \phi[x \div y, x \bmod y]). \tag{2}$$

9.0.16 Theorem. *We have*

$$\vdash_{PA} \exists y \exists z(x = y, z \wedge \phi[y,z]) \leftrightarrow x \neq 0 \wedge \phi[H(x), T(x)] \tag{1}$$
$$\vdash_{PA} \forall y \forall z(x = y, z \rightarrow \phi[y,z]) \leftrightarrow (x \neq 0 \rightarrow \phi[H(x), T(x)])\ . \tag{2}$$

9.0.17. In the sequel we will need the following additional properties of the basic functions and predicates of PA:

$$\vdash_{\mathrm{PA}} x > 0 \rightarrow x \cdot y \leq x \cdot z \leftrightarrow y \leq z \tag{1}$$
$$\vdash_{\mathrm{PA}} r_1 < y \wedge r_2 < y \rightarrow q_1 \cdot y + r_1 = q_2 \cdot y + r_2 \leftrightarrow q_1 = q_2 \wedge r_1 = r_2 \tag{2}$$
$$\vdash_{\mathrm{PA}} r_1 < y \wedge r_2 < y \rightarrow q_1 \cdot y + r_1 \leq q_2 \cdot y + r_2 \leftrightarrow q_1 < q_2 \vee q_1 = q_2 \wedge r_1 \leq r_2 \tag{3}$$
$$\vdash_{\mathrm{PA}} r_1 < y \wedge r_2 < y \rightarrow q_1 \cdot y + r_1 < q_2 \cdot y + r_2 \leftrightarrow q_1 < q_2 \vee q_1 = q_2 \wedge r_1 < r_2 \tag{4}$$
$$\vdash_{\mathrm{PA}} x > 0 \rightarrow x \cdot y \div (x \cdot z) = y \div z \tag{5}$$
$$\vdash_{\mathrm{PA}} x \mid y \rightarrow (y + z) \div x = y \div x + z \div x \tag{6}$$
$$\vdash_{\mathrm{PA}} x \mid y \wedge x \mid z \rightarrow x \mid y + z \tag{7}$$
$$\vdash_{\mathrm{PA}} x \mid y \rightarrow x \mid y \cdot z \tag{8}$$

Part II

Computer Programming

10. Clausal Language

10.1 Generalized Terms

10.1.1 Introduction. Generalized terms extend the language of (an extension of) PA with new constructs which will be used purely in the meta-theory to describe the introduction of functions and predicates into PA by clausal definitions. Generalized terms will also be used in the description of computation of such functions and predicates.

Characteristic Terms

10.1.2 Characteristic terms of formulas. For a formula ϕ we call a term ρ such that

$$\vdash_{\mathrm{PA}} (\phi \leftrightarrow \rho = 1) \wedge (\neg\phi \leftrightarrow \rho = 0)$$

the *characteristic term* of ϕ.

10.1.3 Characteristic functions. *Characteristic function* of an n-ary predicate $P(\vec{x})$ is the n-ary predicate $P_*(\vec{x})$ such that:

$$P_*(\vec{x}) = \begin{cases} 1 & \text{if } P(\vec{x}) \\ 0 & \text{otherwise.} \end{cases}$$

The characteristic function $P_*(\vec{x})$ of the predicate $P(\vec{x})$ can be introduced into PA by the following contextual definition:

$$\vdash_{\mathrm{PAx}} P_*(\vec{x}) = y \leftrightarrow P(\vec{x}) \wedge y = 1 \vee \neg P(\vec{x}) \wedge y = 0. \tag{1}$$

As a special case is the characterstic function $x_1 =_* x_2$ of the binary equality predicate $x_1 = x_2$ which can be introduced into PA by:

$$\vdash_{\mathrm{PAx}} (x_1 =_* x_2) = y \leftrightarrow x_1 = x_2 \wedge y = 1 \vee x_1 \neq x_2 \wedge y = 0. \tag{2}$$

The *boolean* functions are introduced into PA by the following explicit definitions:

$$\vdash_{\mathrm{PAx}} \neg_* x = D(x,0,1) \tag{3}$$
$$\vdash_{\mathrm{PAx}} x \wedge_* y = D(x, D(y,1,0),0) \tag{4}$$
$$\vdash_{\mathrm{PAx}} x \vee_* y = \neg_*(\neg_* x \wedge_* \neg_* y) \tag{5}$$
$$\vdash_{\mathrm{PAx}} x \to_* y = \neg_* x \vee_* y \tag{6}$$
$$\vdash_{\mathrm{PAx}} x \leftrightarrow_* y = (x \to_* y) \wedge_* (y \to_* x). \tag{7}$$

For an existential formula $\exists y\, \phi[\vec{x}, y]$ with all its free variables $\vec{x}$ indicated its *witnessing* function $w_{\exists y \phi}(\vec{x})$ is introduced into PA by minimalization:

$$\vdash_{\mathrm{PAx}} w_{\exists y \phi}(\vec{x}) = \mu_y[\phi[\vec{x}, y] \vee \neg\exists y\, \phi[\vec{x}, y] \wedge y = 0]. \tag{8}$$

For a universal formula $\forall y\, \phi[\vec{x}, y]$ with all its free variables $\vec{x}$ indicated its *counterexample* function $w_{\exists y \phi}(\vec{x})$ is introduced into PA by minimalization:

$$\vdash_{\mathrm{PAx}} c_{\forall y \phi}(\vec{x}) = \mu_y[\neg\phi[\vec{x}, y] \vee \forall y\, \phi[\vec{x}, y] \wedge y = 0]. \tag{9}$$

10.1.4 Assignment of characteristic terms. The assignment ϕ_* of a characteristic term to a formula is defined inductively on the construction of the formula as follows:

$$\top_* \equiv 1 \tag{1}$$
$$\bot_* \equiv 0 \tag{2}$$
$$(P(\vec{\tau}))_* \equiv P_*(\vec{\tau}) \tag{3}$$
$$(\tau_1 = \tau_2)_* \equiv (\tau_1 =_* \tau_2) \tag{4}$$
$$(\neg\phi)_* \equiv (\neg_* \phi_*) \tag{5}$$
$$(\phi_1 \wedge \phi_2)_* \equiv (\phi_{1*} \wedge_* \phi_{2*}) \tag{6}$$
$$(\phi_1 \vee \phi_2)_* \equiv (\phi_{1*} \vee_* \phi_{2*}) \tag{7}$$
$$(\phi_1 \to \phi_2)_* \equiv (\phi_{1*} \to_* \phi_{2*}) \tag{8}$$
$$(\phi_1 \leftrightarrow \phi_2)_* \equiv (\phi_{1*} \leftrightarrow_* \phi_{2*}) \tag{9}$$
$$(\exists y\, \phi[\vec{x}, y])_* \equiv \phi_*[\vec{x}, w_{\exists y \phi}(\vec{x})] \tag{10}$$
$$(\forall y\, \phi[\vec{x}, y])_* \equiv \phi_*[\vec{x}, c_{\forall y \phi}(\vec{x})]. \tag{11}$$

10.1.5 Theorem. *We have*

$$\vdash_{PA} (\phi \leftrightarrow \phi_* = 1) \wedge (\neg\phi \leftrightarrow \phi_* = 0). \tag{1}$$

Proof. Property (1) is proved by induction on the construction of ϕ. □

Patterns

10.1.6 Guarded patterns. guard $\Gamma[\vec{x}, \vec{a}]$, pattern $\phi[\vec{x}; \vec{y}]$ with input variables $\vec{x}$ and output variables $\vec{y}$, pattern's uniqueness condition

$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \phi[\vec{x}; \vec{y}] \wedge \phi[\vec{x}; \vec{z}] \rightarrow \bigwedge y_i = z_i. \tag{1}$$

recogniser $\rho[\vec{x}]$

$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \rho[\vec{x}] = 0 \vee \rho[\vec{x}] = 1 \tag{2}$$
$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \exists \vec{y}\, \phi[\vec{x}; \vec{y}] \leftrightarrow \rho[\vec{x}] = 1. \tag{3}$$

destructors $\vec{\delta}[\vec{x}]$

$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \exists \vec{y}\, \phi[\vec{x}; \vec{y}] \leftrightarrow \phi[\vec{x}; \vec{\delta}[\vec{x}]]. \tag{4}$$

We have

$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \exists \vec{y}(\phi[\vec{x}; \vec{y}] \wedge \psi[\vec{y}]) \leftrightarrow \rho[\vec{x}] = 1 \wedge \psi[\vec{\delta}] \tag{5}$$
$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \forall \vec{y}(\phi[\vec{x}; \vec{y}] \rightarrow \psi[\vec{y}]) \leftrightarrow \rho[\vec{x}] = 1 \rightarrow \psi[\vec{\delta}]. \tag{6}$$

Generalized Terms

10.1.7 Generalized terms. For a given tuple of variables $\vec{x}$ and a guard $\Gamma[\vec{x}, \vec{a}]$ we define the set of *generalized terms in $\vec{x}$ guarded by $\Gamma[\vec{x}, \vec{a}]$* as the smallest set of expressions satisfying the following:

- The variables $\vec{x}$ are generalized terms in $\vec{x}$ guarded by $\Gamma[\vec{x}, \vec{a}]$.
- If f is a n-ary function symbol of T and $\vec{\alpha}$ is an n-tuple of generalized terms in $\vec{x}$ guarded by $\Gamma[\vec{x}, \vec{a}]$ then so is the expression $f(\vec{\alpha})$.
- The expression of the form $(m \geq 1)$:

$$\mathcal{D}^{\vec{\delta}_1, \ldots, \vec{\delta}_m}_{\rho_1, \ldots, \rho_m}(\phi_1[\vec{x}; \vec{y}_1], \alpha_1[\vec{x}, \vec{y}_1], \ldots, \phi_m[\vec{x}; \vec{y}_m], \alpha_m[\vec{x}, \vec{y}_m]) \tag{1}$$

  is a generalized term in $\vec{x}$ guarded by $\Gamma[\vec{x}, \vec{a}]$ if for every $i = 1, \ldots, m$:
  - $\phi_i[\vec{x}; \vec{y}_i]$ is a pattern guarded by $\Gamma[\vec{x}, \vec{a}]$ with the recogniser ρ_i and the destructors $\vec{\delta}_i$,
  - $\alpha_i[\vec{x}, \vec{y}_i]$ is a generalized term in $\vec{x}, \vec{y}_i$ guarded by $\Gamma[\vec{x}, \vec{a}] \wedge \phi_i[\vec{x}; \vec{y}_i]$.

  Moreover, the patterns satisfies the following *disjointness* and *completeness* conditions:

$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{m} \neg(\exists \vec{y}_i\, \phi_i[\vec{x}; \vec{y}_i] \wedge \exists \vec{y}_j\, \phi_j[\vec{x}; \vec{y}_j]) \tag{2}$$
$$T \vdash \Gamma[\vec{x}, \vec{a}] \rightarrow \bigvee_{i=1}^{m} \exists \vec{y}_i\, \phi_i[\vec{x}; \vec{y}_i]. \tag{3}$$

Generalized terms of form $f(\vec{\alpha})$ are called *applications*. Generalized terms of a form (1) are called *case discrimination* terms.

As a simple consequence of the conditions (2),(3) and the properties of pattern's recognisers we get

$$T \vdash \Gamma[\vec{x},\vec{a}] \to \bigwedge_{\substack{i,j=1\\ i\neq j}}^{m} \neg(\rho_i = 1 \wedge \rho_j = 1) \tag{4}$$

$$T \vdash \Gamma[\vec{x},\vec{a}] \to \bigvee_{i=1}^{m} \rho_i = 1. \tag{5}$$

10.1.8 Translation of generalized terms. It would not be too difficult to assign denotations in the standard model of PA to the generalized terms but, since they will play role only in the meta-theory, we will not do it. We will instead translate the generalized terms to the terms of PA by defining a meta-theoretic function $\alpha^\star$ yielding a term of PA whose interpretation can be understood as the intended interpretation of α. The translation function is defined by induction on the construction of generalized terms as follows:

$$x^\star \equiv x \tag{1}$$

$$f(\alpha_1,\dots,\alpha_n)^\star \equiv f(\alpha_1^\star,\dots,\alpha_n^\star) \tag{2}$$

$$\begin{aligned}&\mathcal{D}^{\vec{\delta}_1,\dots,\vec{\delta}_m}_{\rho_1,\dots,\rho_m}(\phi_1,\alpha_1[\vec{y}_1],\dots,\phi_m,\alpha_m[\vec{y}_m])^\star \equiv\\ &\quad\equiv \overbrace{D(\rho_1,\alpha_1^\star[\vec{\delta}_1],\dots D}^{(m-1)\text{-times}}(\rho_{m-1},\alpha_{m-1}^\star[\vec{\delta}_{m-1}],\alpha_m^\star[\vec{\delta}_m])\dots).\end{aligned} \tag{3}$$

Generalized terms are never used in the formulas of theorems and proofs of PA except in the translated form $\alpha^\star$ which stands for a term of PA.

10.1.9 Graphs of generalized terms. Graphs of generalized terms are defined by induction on the construction of generalized terms as follows:

$$x \asymp v \equiv x = v \tag{1}$$

$$f(\alpha_1,\dots,\alpha_n) \asymp v \equiv \exists v_1 \cdots \exists v_n (\bigwedge_{i=1}^{n} \alpha_i \asymp v_i \wedge f(v_1,\dots,v_n) = v) \tag{2}$$

$$\mathcal{D}^{\vec{\delta}_1,\dots,\vec{\delta}_m}_{\rho_1,\dots,\rho_m}(\phi_1,\alpha_1[\vec{y}_1],\dots,\phi_m,\alpha_m[\vec{y}_m]) \asymp v \equiv \bigvee_{i=1}^{m} \exists \vec{y}_i \big(\phi_i \wedge \alpha_i[\vec{y}_i] \asymp v\big). \tag{3}$$

We have

$$T \vdash \tau \asymp v \leftrightarrow \tau = v \tag{4}$$

$$\begin{aligned}T \vdash &\bigwedge_{i=1}^{n} \forall v(\alpha_i \asymp v \leftrightarrow \beta_i \asymp v) \to\\ &\quad f(\alpha_1,\dots,\alpha_n) \asymp v \leftrightarrow f(\beta_1,\dots,\beta_n) \asymp v.\end{aligned} \tag{5}$$

In the sequel we will not explicitly indicate the uses of these two properties.

10.1.10 Theorem. *For every generalized term α guarded by Γ we have*

$$T \vdash \Gamma \to \forall v(\alpha \asymp v \leftrightarrow \alpha^\star = v). \tag{1}$$

Proof. Property (1) is proved induction on the construction of the generalized term α. So assume Γ, take any v, and continue by case analysis on α. If α is a variable then (1) holds trivially. If $\alpha \equiv f(\alpha_1, \ldots, \alpha_n)$ then the generalized terms α_i are guarded by Γ and we have

$$f(\alpha_1, \ldots, \alpha_n) \asymp v \overset{\mathrm{IH}}{\Leftrightarrow} f(\alpha_1^\star, \ldots, \alpha_n^\star) = v \overset{\mathrm{def}}{\Leftrightarrow} f(\alpha_1, \ldots, \alpha_n)^\star = v.$$

If $\alpha \equiv \mathcal{D}^{\vec{\delta}_1,\ldots,\vec{\delta}_m}_{\rho_1,\ldots,\rho_m}(\phi_1, \alpha_1[\vec{y}_1], \ldots, \phi_m, \alpha_m[\vec{y}_m])$ then the generalized terms $\alpha_i[\vec{y}_i]$ are guarded by $\Gamma \wedge \phi_i$ and we have

$$\begin{aligned}
&\mathcal{D}^{\vec{\delta}_1,\ldots,\vec{\delta}_m}_{\rho_1,\ldots,\rho_m}(\phi_1, \alpha_1[\vec{y}_1], \ldots, \phi_m, \alpha_m[\vec{y}_m]) \asymp v \overset{\mathrm{def}}{\Leftrightarrow} \bigvee_{i=1}^m \exists \vec{y}_i \big(\phi_i \wedge \alpha_i[\vec{y}_i] \asymp v\big) \overset{\mathrm{IH}}{\Leftrightarrow} \\
&\bigvee_{i=1}^m \exists \vec{y}_i \big(\phi_i \wedge \alpha_i^\star[\vec{y}_i] = v\big) \overset{10.1.6(5)}{\Leftrightarrow} \bigvee_{i=1}^m \big(\rho_i = \top_* \wedge \alpha_i^\star[\vec{\delta}_i] = v\big) \overset{(*)}{\Leftrightarrow} \\
&D(\rho_1, \alpha_1^\star[\vec{\delta}_1], \ldots D(\rho_{m-1}, \alpha_{m-1}^\star[\vec{\delta}_{m-1}], \alpha_m^\star[\vec{\delta}_m]) \ldots) = v \overset{\mathrm{def}}{\Leftrightarrow} \\
&\mathcal{D}^{\vec{\delta}_1,\ldots,\vec{\delta}_m}_{\rho_1,\ldots,\rho_m}(\phi_1, \alpha_1[\vec{y}_1], \ldots, \phi_m, \alpha_m[\vec{y}_m])^\star = v.
\end{aligned}$$

The step marked by $(*)$ follows from 10.1.6(2) and 10.1.7(4)(5). □

Regular Course of Values Recursion with Measure

10.1.11 Fixing notation. Let T be a proper extension of PA. Let us denote by $T[f]$ the theory obtained from T by adding a new n-ary function symbol f. Let further $\alpha[f; \vec{x}]$ be a generalized term of $T[f]$ guarded by $\Gamma[\vec{x}, \vec{a}]$ and $\mu[\vec{x}, \vec{a}]$ be a term of T.

$$w_i \equiv w_{\exists a_i \cdots \exists a_k \Gamma[\vec{x}, w_1[\vec{x}], \ldots, w_{i-1}[\vec{x}], a_i, \ldots, a_k]}$$

We have

$$T[f] \vdash \exists \vec{a}\, \Gamma[\vec{x}, \vec{a}] \leftrightarrow \Gamma[\vec{x}, \vec{w}[\vec{x}]]. \tag{1}$$

10.1.12 Governing conditions. To every (generalized) term α and an occurrence in α of a subterm β we define inductively on $\|\alpha\| - \|\beta\|$ the *governing condition* Γ^α_β *of* β *in* α. Here we denote by $\|\alpha\|$ the *size*, i.e. the number of operations, of the term α. If $\beta \equiv \alpha$ or β is a term of PA then $\Gamma^\alpha_\beta \equiv \top$. If $\beta \equiv \mathcal{D}^{\vec{\delta}_1,\ldots,\vec{\delta}_m}_{\rho_1,\ldots,\rho_m}(\phi_1, \alpha_1, \ldots, \phi_m, \alpha_m)$ then

$$\Gamma^\alpha_{\rho_i} \equiv \Gamma^\alpha_\beta \qquad \Gamma^\alpha_{\beta_i} \equiv \Gamma^\alpha_\beta \wedge \phi_i. \tag{1}$$

10.1.13 Conditions of regularity. We assign to each recursive occurrence $f(\vec{\beta})$ in α with governing condition $\Gamma^{\phi}_{f(\vec{\beta})}[f;\vec{x},\vec{a}]$ the following *condition of regularity*:

$$\Gamma^{\phi}_{f(\vec{\beta})}[f;\vec{x},\vec{a}] \wedge \bigwedge_{i=1}^{n} \beta_i \asymp v_i \rightarrow \mu[\vec{v},\vec{a}] < \mu[\vec{x},\vec{a}]. \tag{1}$$

We denote by $Reg^{\Gamma,\mu}_{\alpha}[f;\vec{x},\vec{a}]$ the conjunction of all conditions of regularity.

10.1.14 Lemma. *Let S be the extension of T by the following course of values recursion with measure:*

$$f(\vec{x}) = D(\Gamma_*[\vec{x},\vec{w}[\vec{x}]], \alpha^\star[[f]^{\mu[\vec{x},\vec{w}[\vec{x}]]}_{\vec{x}};\vec{x}],0). \tag{1}$$

If $S \vdash Reg^{\Gamma,\mu}_{\alpha}[f;\vec{x},\vec{a}]$ then

$$S \vdash \exists\vec{a}\,\Gamma[\vec{x},\vec{a}] \rightarrow f(\vec{x}) = \alpha^\star[f;\vec{x}] \tag{2}$$

$$S \vdash \neg\exists\vec{a}\,\Gamma[\vec{x},\vec{a}] \rightarrow f(\vec{x}) = 0. \tag{3}$$

Proof. We prove an auxiliary property by induction on the structure of β:

> for any occurrence of a subterm $\beta[f;\vec{x}]$ of $\alpha[f;\vec{x}]$ governed in α by $\Gamma^{\alpha}_{\beta}[f;\vec{x},\vec{a}]$ we have
>
> $$S \vdash \Gamma^{\alpha}_{\beta}[f;\vec{x},\vec{a}] \rightarrow \forall v\big(\beta[[f]^{\mu}_{\vec{x}};\vec{x}] \asymp v \leftrightarrow \beta[f;\vec{x}] \asymp v\big). \tag{4}$$

So assume $\Gamma^{\alpha}_{\beta}[f;\vec{x},\vec{a}]$, take any v, and continue by the case analysis of β. If β is a variable then the property holds trivially. If $\beta \equiv g(\vec{\gamma})$ then the terms $\vec{\gamma}$ are governed in α by Γ^{α}_{β} and we have

$$g(\vec{\gamma}[[f]^{\mu}_{\vec{x}};\vec{x}]) \asymp v \overset{\text{IH}}{\Leftrightarrow} g(\vec{\gamma}[f;\vec{x}]) \asymp v.$$

If $\beta \equiv f(\vec{\gamma})$ then the terms $\vec{\gamma}$ are governed in α by Γ^{α}_{β}. By regularity

$$\mu[\vec{\gamma}[f;\vec{x}],\vec{a}] < \mu[\vec{x},\vec{a}] \tag{5}$$

and thus we have

$$\begin{aligned}
&D(\mu[\vec{\gamma}[[f]^{\mu}_{\vec{x}};\vec{x}],\vec{a}] <_* \mu[\vec{x},\vec{a}], f(\vec{\gamma}[[f]^{\mu}_{\vec{x}};\vec{x}]),0) \asymp v \overset{\text{IH}}{\Leftrightarrow}\\
&D(\mu[\vec{\gamma}[f;\vec{x}],\vec{a}] <_* \mu[\vec{x},\vec{a}], f(\vec{\gamma}[f;\vec{x}]),0) \asymp v \overset{(5)}{\Leftrightarrow}\\
&D(1, f(\vec{\gamma}[f;\vec{x}]),0) \asymp v \Leftrightarrow f(\vec{\gamma}[f;\vec{x}]) \asymp v.
\end{aligned}$$

If $\beta \equiv \mathcal{D}^{\vec{\delta}_1,\ldots,\vec{\delta}_m}_{\rho_1,\ldots,\rho_m}(\phi_1,\gamma_1,\ldots,\phi_m,\gamma_m)$ then the terms ρ_i are governed in α by Γ^{α}_{β} and the terms γ_i by $\Gamma^{\alpha}_{\beta} \wedge \phi_i$. We have

$$\bigwedge_{i=1}^{m} \rho_i[[f]^\mu_{\vec{x}};\vec{x}] = \rho_i[f;\vec{x}] \tag{6}$$

$$\bigwedge_{i=1}^{m} \forall\vec{y}_i\bigl(\phi_i[f;\vec{x};\vec{y}_i] \to \forall v(\gamma_i[[f]^\mu_{\vec{x}};\vec{x};\vec{y}_i] \asymp v \leftrightarrow \gamma_i[f;\vec{x};\vec{y}_i] \asymp v)\bigr) \tag{7}$$

by IH and thus by the properties of pattern recognisers and (6):

$$\bigwedge_{i=1}^{m} \forall\vec{y}_i\bigl(\phi_i[[f]^\mu_{\vec{x}};\vec{x};\vec{y}_i] \leftrightarrow \phi_i[f;\vec{x};\vec{y}_i]\bigr). \tag{8}$$

We have

$$\begin{aligned}
&\mathcal{D}^{\vec{\vec{\delta}}[[f]^\mu_{\vec{x}};\vec{x}]}_{\vec{\rho}[[f]^\mu_{\vec{x}};\vec{x}]}\bigl(\dots,\phi_i[[f]^\mu_{\vec{x}};\vec{x};\vec{y}_i],\gamma_i[[f]^\mu_{\vec{x}};\vec{x},\vec{y}_i],\dots\bigr) \asymp v \overset{\mathrm{def}}{\Leftrightarrow}\\
&\bigvee_{i=1}^{m} \exists\vec{y}_i\bigl(\phi_i[[f]^\mu_{\vec{x}};\vec{x};\vec{y}_i] \wedge \gamma_i[[f]^\mu_{\vec{x}};\vec{x},\vec{y}_i] \asymp v\bigr) \overset{(8)}{\Leftrightarrow}\\
&\bigvee_{i=1}^{m} \exists\vec{y}_i\bigl(\phi_i[f;\vec{x};\vec{y}_i] \wedge \gamma_i[[f]^\mu_{\vec{x}};\vec{x},\vec{y}_i] \asymp v\bigr) \overset{(7)}{\Leftrightarrow}\\
&\bigvee_{i=1}^{m} \exists\vec{y}_i\bigl(\phi_i[f;\vec{x};\vec{y}_i] \wedge \gamma_i[f;\vec{x},\vec{y}_i] \asymp v\bigr) \overset{\mathrm{def}}{\Leftrightarrow}\\
&\mathcal{D}^{\vec{\vec{\delta}}[f;\vec{x}]}_{\vec{\rho}[f;\vec{x}]}\bigl(\dots,\phi_i[f;\vec{x};\vec{y}_i],\gamma_i[f;\vec{x},\vec{y}_i],\dots\bigr) \asymp v.
\end{aligned}$$

With the auxiliary property proved, we prove (2) as follows. Assume $\exists\vec{a}\,\Gamma[\vec{x},\vec{a}]$. Then $\Gamma[\vec{x},\vec{w}[\vec{x}]]$ by 10.1.11(1). We take in (4) the term α as its subterm and substitute $\vec{w}[\vec{x}]$ for $\vec{a}$. We have

$$\begin{aligned}
f(\vec{x}) &\overset{(1)}{=} D(\Gamma_*[\vec{x},\vec{w}[\vec{x}]],\alpha^\star[[f]^{\mu[\vec{x},\vec{w}[\vec{x}]]}_{\vec{x}};\vec{x}],0) \overset{10.1.5(1)}{=} D(1,\alpha^\star[[f]^{\mu[\vec{x},\vec{w}[\vec{x}]]}_{\vec{x}};\vec{x}],0) =\\
&= \alpha^\star[[f]^{\mu[\vec{x},\vec{w}[\vec{x}]]}_{\vec{x}};\vec{x}] \overset{(4),10.1.10(1)}{=} \alpha^\star[f;\vec{x}].
\end{aligned}$$

Property (3) follows from 10.1.11(1) by 10.1.5(1) □

10.1.15 Extensions by regular course of values recursion with measure. Suppose that in the extension S_1 of T by the following course of values recursion with measure:

$$f(\vec{x}) = D(\Gamma_*[\vec{x},\vec{w}[\vec{x}]],\alpha^\star[[f]^{\mu[\vec{x},\vec{w}[\vec{x}]]}_{\vec{x}};\vec{x}],0)$$

we have

$$S_1 \vdash \mathit{Reg}^{\Gamma,\mu}_{\alpha}[f;\vec{x},\vec{a}].$$

The extension of the theory T into S with the language $\mathcal{L}_T + f$ with the axioms universal closures of

$$\exists \vec{a}\, \Gamma[\vec{x}, \vec{a}] \rightarrow f(\vec{x}) = \alpha^\star[f; \vec{x}] \tag{1}$$

$$\neg \exists \vec{a}\, \Gamma[\vec{x}, \vec{a}] \rightarrow f(\vec{x}) = 0 \tag{2}$$

$$Reg_\alpha^{\Gamma,\mu}[f; \vec{x}, \vec{a}] \tag{3}$$

is called *extension by regular course of values recursion with measure*.

10.2 Clausal Definitions

10.3 The Strength of Clausal Definitions

11. Numeric Programs

11.1 Explicit Definitions

11.1.1 Explicit clausal definitions. Recall that explicit clausal definitions are obtained by unfolding of initial clauses of a form (see Par. **??**)

$$f(\vec{x}) = \alpha[\vec{x}],$$

where the generalised term α does not contain recursive applications of f. By Thm. **??** explicit clausal definitions are definitional extensions of PA. Recall also that primitive recursive functions are closed under explicit clausal definitions.

11.1.2 Minimum. The *minumum* function $\min(x, y)$ with its basic properties:

$$\vdash_{\mathrm{PA}} \min(x, y) \leq x \tag{1}$$
$$\vdash_{\mathrm{PA}} \min(x, y) \leq y \tag{2}$$
$$\vdash_{\mathrm{PA}} \min(x, y) = x \lor \min(x, y) = y \tag{3}$$

can be introduced into PA by the following explicit clausal definition as a primitive recursive function:

$\min(x, y) = x \leftarrow x \leq y$
$\min(x, y) = y \leftarrow x > y.$

The definition uses the dichotomic discrimination on $x \leq y$ and $x > y$. Properties (1)–(3) are proved by the corresponding case analysis. For instance, (1) follows from:

$$x \leq y \Rightarrow \min(x, y) \stackrel{\text{def}}{=} x \leq x$$
$$x > y \Rightarrow \min(x, y) \stackrel{\text{def}}{=} y \leq x.$$

11.1.3 Signum function. The *signum* function $\mathrm{sgn}(x)$ with its basic property:

$$\vdash_{\mathrm{PA}} x = 0 \land \mathrm{sgn}(x) = 0 \lor x > 0 \land \mathrm{sgn}(x) = 1 \tag{1}$$

can be introduced into PA by the following explicit clausal definition as a primitive recursive function:

$$\begin{aligned}&\mathrm{sgn}(0) = 0\\&\mathrm{sgn}(x+1) = 1.\end{aligned}$$

The definition uses monadic discrimination. Property (1) is proved by the corresponding case analysis.

11.2 Primitive Recursion

11.2.1 Primitive recursive clausal definitions. *Primitive recursive* clausal definition S of a function $f(\vec{y}, x, \vec{z})$ is a regular clausal definition for f which can be obtained by unfolding the clauses of a form

$$f(\vec{y}, x, \vec{z}) = \alpha_1[\vec{y}, \vec{z}] \leftarrow x = 0 \tag{1}$$
$$f(\vec{y}, x, \vec{z}) = \alpha_2[\dot{\lambda}\vec{w}.f(\vec{y}, x_1, \vec{z}); \vec{y}, x_1, \vec{z}] \leftarrow x = x_1 + 1, \tag{2}$$

where the generalised term α_1 does not apply f and each recursive application of f in the generalized term α_2 has the form $f(\vec{y}, x_1, \vec{z})$.

That the clausal definition S is a regular clausal definition can be seen from the following. Consider the (initial) clause of the form

$$f(\vec{y}, x, \vec{z}) = Num^{1,1}_{x_1,u}(x, Const_0(x, \alpha_1[\vec{y}, \vec{z}], 0), \alpha_2[\dot{\lambda}\vec{w}.f(\vec{y}, x_1, \vec{z}); \vec{y}, x_1, \vec{z}]).$$

Since $\vdash_{\mathrm{PA}} x = x_1 + 1 \rightarrow x_1 < x$ the clause is regular in the argument x. One unfolding step with numeric discrimination yields

$$\begin{aligned}&f(\vec{y}, x, \vec{z}) = Const_0(x, \alpha_1[\vec{y}, \vec{z}], 0) \leftarrow x < 1\\&f(\vec{y}, x, \vec{z}) = \alpha_2[\dot{\lambda}\vec{w}.f(\vec{y}, x_1, \vec{z}); \vec{y}, x_1, \vec{z}] \leftarrow x = 1 \cdot x_1 + u \wedge 1 \leq u \wedge u < 1 + 1.\end{aligned}$$

By simplifying the last two clauses (see Par. **??**) we obtain (1) and (2).

The clauses (1) and (2) are called the *initial clauses* of the primitive recursive clausal definition S. We will often say that the function $f(\vec{y}, x, \vec{z})$ is defined by primitive recursive definition on x, or even shorter by primitive recursion on x. The variables $\vec{y}$ and $\vec{z}$ are called parameters; they may be empty. We have

$$\vdash_{\mathrm{PA}} f(\vec{y}, 0, \vec{z}) = \alpha_1^\star[\vec{y}, \vec{z}] \tag{3}$$
$$\vdash_{\mathrm{PA}} f(\vec{y}, x+1, \vec{z}) = \alpha_2^\star[\dot{\lambda}\vec{w}.f(\vec{y}, x, \vec{z}); \vec{y}, x, \vec{z}]. \tag{4}$$

11.2.2 Exponentiation. The exponentiation function x^y is defined by primitive recursion on y as a primitive recursive function:

$$\begin{aligned}&x^0 = 1\\&x^{y+1} = x \cdot x^y.\end{aligned}$$

We list here some properties of the exponentiation function:

$$\vdash_{\mathrm{PA}} x^y = 0 \leftrightarrow x = 0 \land y > 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} x^y = 1 \leftrightarrow x = 1 \lor y = 0 \tag{2}$$
$$\vdash_{\mathrm{PA}} x^{y+z} = x^y \cdot x^z \tag{3}$$
$$\vdash_{\mathrm{PA}} x > 0 \land y \geq z \rightarrow x^{y \dot{-} z} = x^y \div x^z \tag{4}$$
$$\vdash_{\mathrm{PA}} x > 1 \land x^y = x^z \rightarrow y = z \tag{5}$$
$$\vdash_{\mathrm{PA}} x > 1 \rightarrow x^y \leq x^z \leftrightarrow y \leq z \tag{6}$$
$$\vdash_{\mathrm{PA}} x > 1 \rightarrow x^y < x^z \leftrightarrow y < z. \tag{7}$$

The properties are proved as follows. Property (1) is proved by induction on y. In the base case (1) trivially holds since by definition $x^0 = 1 \neq 0$. In the inductive case we have

$$x^{y+1} = 0 \overset{\mathrm{def}}{\Leftrightarrow} x \cdot x^y = 0 \Leftrightarrow x = 0 \lor x^y = 0 \overset{\mathrm{IH}}{\Leftrightarrow} x = 0 \lor (x = 0 \land y > 0) \Leftrightarrow$$
$$\Leftrightarrow x = 0 \Leftrightarrow x = 0 \lor y + 1 > 0.$$

Property (2) is similar. Property (3) is proved by induction on y similarly as the property 8.1.12(6). In the proof of the property (4) assume $x > 0$ and prove

$$\forall z(y \geq z \rightarrow x^{y \dot{-} z} = x^y \div x^z) \tag{8}$$

by induction on y. In the base case when $y = 0$ take and z such that $0 \geq z$, i.e. $z = 0$, and we have

$$x^{0 \dot{-} 0} = x^0 \overset{\mathrm{def}}{=} 1 = 1 \div 1 \overset{\mathrm{def}}{=} x^0 \div x^0.$$

In the inductive case when $y = y_1 + 1$ for some y_1 take any z such that $y \geq z$ and consider two cases. If $z = 0$ then we have

$$x^{y \dot{-} 0} = x^y = x^y \div 1 \overset{\mathrm{def}}{=} x^y \div x^0.$$

If $z = z_1 + 1$ for some z_1 then $y_1 \geq z_1$ and we have

$$x^{y_1+1 \dot{-} (z_1+1)} = x^{y_1 \dot{-} z_1} \overset{\mathrm{IH}}{=} x^{y_1} \div x^{z_1} \overset{9.0.17(5)}{=}$$
$$= x \cdot x^{y_1} \div (x \cdot x^{z_1}) \overset{\mathrm{def}}{=} x^{y_1+1} \div x^{z_1+1}.$$

The remaining properties are proved similarly.

11.2.3 Summation. The *summation* function $\sum_{i=0}^{n} i$ computing the sum

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + \cdots + n$$

is a primitive recursive function by primitive recursive definition:

$\sum_{i=0}^{0} i = 0$
$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + n + 1.$

Its basic property

$$\vdash_{\mathrm{PA}} \sum_{i=0}^{n} i = n \cdot (n+1) \div 2. \tag{1}$$

is proved by induction on n. In the base case we have

$$\sum_{i=0}^{0} i \overset{\mathrm{def}}{=} 0 = 0 \cdot (0+1) \div 2.$$

In the inductive case we have

$$\sum_{i=0}^{n+1} i \overset{\mathrm{def}}{=} \sum_{i=0}^{n} i + n + 1 \overset{\mathrm{IH}}{=} n \cdot (n+1) \div 2 + n + 1 =$$
$$= \big(n \cdot (n+1) + 2 \cdot (n+1)\big) \div 2 = (n+1) \cdot (n+1+1) \div 2.$$

11.2.4 Factorial. The function $n!$ computing the *factorial of* n

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$$

is defined by primitive recursion as a primitive recursive function:

$0! = 1$
$(n+1)! = (n+1) \cdot n!.$

The function satisfies

$$\vdash_{\mathrm{PA}} 0 < i \leq n \rightarrow i \mid n!. \tag{1}$$

Property (1) is proved by induction on n. In the base case there is nothing to prove. In the inductive case assume $0 < i \leq n+1$ and consider two cases. If $i \leq n$ then by IH

$$i \mid n! \overset{9.0.17(8)}{\Rightarrow} i \mid (n+1) \cdot n! \overset{\mathrm{def}}{\Rightarrow} i \mid (n+1)!.$$

Otherwise, if $i = n+1$, we obtain by 7.5.1(2)

$$n+1 \mid n+1 \overset{9.0.17(8)}{\Rightarrow} n+1 \mid (n+1) \cdot n! \overset{\mathrm{def}}{\Rightarrow} n+1 \mid (n+1)!.$$

11.2.5 Square root. The square root function $\lfloor\sqrt{x}\rfloor$ yields the greatest number whose square does not exceed x:

$$\vdash_{\mathrm{PA}} \lfloor\sqrt{x}\rfloor^2 \leq x < (\lfloor\sqrt{x}\rfloor + 1)^2. \tag{1}$$

We can derive primitive recursive definition for $\lfloor\sqrt{x}\rfloor$ by assuming (as IH) that (1) holds and then considering the relation between $x+1$ and $(\lfloor\sqrt{x}\rfloor+1)^2$. There are two cases. If

$$\lfloor\sqrt{x}\rfloor^2 \leq x < x+1 < (\lfloor\sqrt{x}\rfloor+1)^2$$

holds then it clearly suffices to set: $\lfloor\sqrt{x+1}\rfloor := \lfloor\sqrt{x}\rfloor$. Otherwise we must have

$$\lfloor\sqrt{x}\rfloor^2 \leq x < (\lfloor\sqrt{x}\rfloor+1)^2 = x+1 < (\lfloor\sqrt{x}\rfloor+2)^2$$

and it suffices to set $\lfloor\sqrt{x+1}\rfloor := \lfloor\sqrt{x}\rfloor+1$. This idea is expressed by the following primitive recursive definition:

$$\begin{aligned}
&\lfloor\sqrt{0}\rfloor = 0\\
&\lfloor\sqrt{x+1}\rfloor = \lfloor\sqrt{x}\rfloor \leftarrow x+1 < (\lfloor\sqrt{x}\rfloor+1)^2\\
&\lfloor\sqrt{x+1}\rfloor = \lfloor\sqrt{x}\rfloor+1 \leftarrow x+1 = (\lfloor\sqrt{x}\rfloor+1)^2.
\end{aligned}$$

11.2.6 Square root with assignments. We will investigate more programs (algorithms) for the square root function $\lfloor\sqrt{x}\rfloor$ because the one given in Par. 11.2.5, although quite pleasing mathematically, is unfeasible in practice for many reasons. One of them is the twofold computation of $\lfloor\sqrt{x}\rfloor$ for every value x: once in the test and once in the result. This causes an exponential blowup of 2^x recursions in order to compute $\lfloor\sqrt{x}\rfloor$. The blowup is prevented by the *assignment* in the following clausal definition of the recursive value $\lfloor\sqrt{x}\rfloor$ to an auxiliary variable s:

$$\begin{aligned}
&\lfloor\sqrt{0}\rfloor = 0\\
&\lfloor\sqrt{x+1}\rfloor = s \leftarrow \lfloor\sqrt{x}\rfloor = s \wedge x+1 < (s+1)^2\\
&\lfloor\sqrt{x+1}\rfloor = s+1 \leftarrow \lfloor\sqrt{x}\rfloor = s \wedge x+1 = (s+1)^2.
\end{aligned}$$

11.2.7 Primitive recursive clausal definitions with substitution in parameters. Initial clauses of primitive recursive clausal definitions *with substitution in parameters* are of a form

$$\begin{aligned}
&f(\vec{y},x,\vec{z}) = \alpha_1[\vec{y},\vec{z}] \leftarrow x = 0\\
&f(\vec{y},x,\vec{z}) = \alpha_2[\dot{\lambda}\vec{y}w\vec{z}.f(\vec{y},x_1,\vec{z});\vec{y},x_1,\vec{z}] \leftarrow x = x_1+1.
\end{aligned}$$

Note that recursive applications of f in the generalized term α_2 are of the form $f(\vec{\tau},x_1,\vec{\rho})$, where the terms $\vec{\tau}$ and $\vec{\rho}$ may be different from the variables $\vec{y}$ and $\vec{z}$, respectively. If for instance $\tau_i \not\equiv y_i$ then we say that the definition uses the *substitution* in the parameter y_i.

11.2.8 Decreasing factorial. The function $(n)_{[k]}$ computing the product

$$(n)_{[k]} = \overbrace{n\cdot(n \dot{-} 1)\cdot\cdots\cdot(n \dot{-}(k \dot{-} 1))}^{k\text{-times}}$$

is defined by primitive recursion on k with substitution in parameter as a primitive recursive function:

$(n)_{[0]} = 1$
$(n)_{[k+1]} = n \cdot (n \dot{-} 1)_{[k]}.$

We list here some its properties:

$$\vdash_{\text{PA}} (n)_{[k]} = 0 \leftrightarrow n < k \tag{1}$$
$$\vdash_{\text{PA}} k \leq n \rightarrow (n)_{[k]} \cdot (n \dot{-} k)! = n! \tag{2}$$
$$\vdash_{\text{PA}} (n)_{[n]} = n! \tag{3}$$
$$\vdash_{\text{PA}} (n)_{[k+1]} = (n)_{[k]} \cdot (n \dot{-} k) \tag{4}$$
$$\vdash_{\text{PA}} (n+1)_{[k]} = k \cdot (n)_{[k \dot{-} 1]} + (n)_{[k]} \tag{5}$$
$$\vdash_{\text{PA}} k! \mid (n)_{[k]}. \tag{6}$$

The properties are proved as follows. Property (1) is proved by induction on k with induction formula $\forall n\,(1)$, ie with

$$\forall n((n)_{[k]} = 0 \leftrightarrow n < k).$$

The base case trivially holds since by definition $(n)_{[0]} = 1 \neq 0$. In the inductive case take any n and we have

$$\begin{aligned}(n)_{[k+1]} = 0 \overset{\text{def}}{\Leftrightarrow} n \cdot (n \dot{-} 1)_{[k]} = 0 \Leftrightarrow n = 0 \vee (n \dot{-} 1)_{[k]} = 0 \overset{\text{IH}}{\Leftrightarrow}\\ \Leftrightarrow n = 0 \vee n \dot{-} 1 < k \Leftrightarrow n < k+1.\end{aligned}$$

Property (2) is proved by induction on k with the induction formula $\forall n\,(2)$. The base case trivially holds since by definition $(n)_{[0]} \cdot (n \dot{-} 0)! = 1 \cdot n! = n!$. In the inductive case take any $n \geq k+1$. Then $n \dot{-} 1 \geq k$ and we have

$$(n)_{[k+1]} \cdot \big(n \dot{-}(k+1)\big)! \overset{\text{def}}{=} n \cdot (n \dot{-} 1)_{[k]} \cdot (n \dot{-} 1 \dot{-} k)! \overset{\text{IH}}{=} n \cdot (n \dot{-} 1)! \overset{\text{def}}{=} n!.$$

Property (3) follows from (2) by substituting n for k.

Property (4) is proved by induction on k with induction formula $\forall n\,(4)$. In the base case take any n and we have

$$(n)_{[1]} \overset{\text{def}}{=} n \cdot (n \dot{-} 1)_{[0]} \overset{\text{def}}{=} n \overset{\text{def}}{=} (n)_{[0]} \cdot n = (n)_{[0]} \cdot (n \dot{-} 0).$$

In the inductive case take any n and we have

$$(n)_{[k+2]} \overset{\text{def}}{=} n \cdot (n \dot{-} 1)_{[k+1]} \overset{\text{IH}}{=} n \cdot (n \dot{-} 1)_{[k]} \cdot (n \dot{-} 1 \dot{-} k) \overset{\text{def}}{=} (n)_{[k+1]} \cdot (n \dot{-}(k+1)).$$

In the proof of the property (5) we consider two cases. If $k > n+1$ then by (1): $(n+1)_{[k]} = (n)_{[k \dot{-} 1]} = (n)_{[k]} = 0$ and (5) holds trivially. If $k \leq n+1$ then we consider two subcases. If $k = 0$ then (5) follows from the definition. If $k \neq 0$ then we have

$$(n+1)_{[k]} \overset{\text{def}}{=} (n+1)\cdot(n)_{[k \dot- 1]} = k\cdot(n)_{[k \dot- 1]} + (n)_{[k \dot- 1]}\cdot(n \dot-(k \dot- 1)) \overset{(4)}{=}$$
$$= k\cdot(n)_{[k \dot- 1]} + (n)_{[k]}.$$

In order to show that (6) holds we first prove

$$\vdash_{\text{PA}} \forall k(k \neq 0 \rightarrow k! \mid (n)_{[k]}) \tag{7}$$

by induction on n. In the base case take any $k \neq 0$ and we get $k! \mid 0$ by 7.5.1(6) and thus $k! \mid (0)_{[k]}$ by definition. In the inductive case take any $k \neq 0$ and we obtain by twice applications of IH: $(k \dot- 1)! \mid (n)_{[k \dot- 1]}$ and $k! \mid (n)_{[k]}$. From 9.0.17(8) we get $k! \mid k\cdot(n)_{[k \dot- 1]}$ and thus by 9.0.17(7)

$$k! \mid k\cdot(n)_{[k \dot- 1]} + (n)_{[k]} \overset{(5)}{\Rightarrow} k! \mid (n+1)_{[k]}.$$

Now we can prove (6). If $k \neq 0$ then we apply (7). Otherwise, when $k = 0$, we have $0! = 1$ by definition and thus $0! \mid (n)_{[0]}$ by 7.5.1(5).

11.2.9 Binomial coefficients. The binomial coefficients $\binom{n}{k}$ can be introduced into PA by the following explicit definition

$$\vdash_{\text{PAx}} \binom{n}{k} = (n)_{[k]} \div k!.$$

We have

$$\vdash_{\text{PA}} \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}. \tag{1}$$

Property (1) is proved as follows

$$\binom{n+1}{k+1} \overset{\text{def}}{=} (n)_{[k+1]} \div (k+1)! \overset{11.2.8(5)}{=}$$
$$= \big((k+1)\cdot(n)_{[k]} + (n)_{[k+1]}\big) \div (k+1)! \overset{11.2.8(6);9.0.17(6)}{=}$$
$$= (k+1)\cdot(n)_{[k]} \div (k+1)! + (n)_{[k+1]} \div (k+1)! \overset{\text{def}}{=}$$
$$= (k+1)\cdot(n)_{[k]} \div \big((k+1)\cdot k!\big) + (n)_{[k+1]} \div (k+1)! \overset{9.0.17(5)}{=}$$
$$= (n)_{[k]} \div k! + (n)_{[k+1]} \div (k+1)! \overset{\text{def}}{=} \binom{n}{k} + \binom{n}{k+1}.$$

11.2.10 Fibonacci function. The function $\text{fib}(n)$ yielding the n-th element of the *sequence of Fibonacci* is defined by course of values recursion as a primitive recursive function:

$$\text{fib}(0) = 1 \tag{1}$$
$$\text{fib}(1) = 1 \tag{2}$$
$$\text{fib}(n+2) = \text{fib}(n+1) + \text{fib}(n). \tag{3}$$

We can, for instance, compute $\mathrm{fib}(4) = 3$ as follows:

$$\mathrm{fib}(4) \overset{(3)}{=} \mathrm{fib}(3) + \mathrm{fib}(2) \overset{2\times(3)}{=} \mathrm{fib}(2) + \mathrm{fib}(1) + \mathrm{fib}(1) + \mathrm{fib}(0) \overset{(3);2\times(2);(1)}{=}$$
$$\mathrm{fib}(1) + \mathrm{fib}(0) + 1 + 1 + 0 \overset{(2);(1)}{=} 1 + 0 + 2 = 3.$$

The only problem is that the computation sequence is too long. In order to compute the number $\mathrm{fib}(n+2)$ one needs to use the recurrence (3) exactly $\mathrm{fib}(n+2)$ times as can be proved by a simple induction proof. The Fibonacci function grows as fast as the exponential function and to compute the function in this way is simply too wasteful. The following Pascal-like program computes $\mathrm{fib}(n)$ into the variable b:

$a := 1$; $b := 0$;
while $n > 0$ *do*
    $n := n - 1$; $c := a$; $a := a + b$; $b := c$;

The reader will note that the loop is executed only n times. This example is usually given as the 'standard argument' against declarative programming where the recursive version is clearly inferior to the imperative one. The argument is fallacious as one should define an auxiliary ternary function $f(n, a, b)$ with two *accumulators* a and b by primitive recursion on n with substitution in parameters as a primitive recursive function:

$f(0, a, b) = b$
$f(n + 1, a, b) = f(n, a + b, a)$.

and then we could take the following property as an explicit definition of the Fibonacci function:

$$\vdash_{\mathrm{PA}} \mathrm{fib}(n) = f(n, 1, 1). \tag{4}$$

The number of recursions of $f(n, a, b)$ is exactly the same as the number of iterations of the loop of the imperative program.

It remains to show that (4) holds. First we prove

$$\vdash_{\mathrm{PA}} \forall k\, f(n, \mathrm{fib}(k+1), \mathrm{fib}(k)) = \mathrm{fib}(n+k) \tag{5}$$

by induction on n. In the base case take any k and we have

$$f(0, \mathrm{fib}(k+1), \mathrm{fib}(k)) \overset{\mathrm{def}}{=} \mathrm{fib}(k) = \mathrm{fib}(0+k).$$

In the inductive case take any k and we have

$$f(n+1, \mathrm{fib}(k+1), \mathrm{fib}(k)) \overset{\mathrm{def}}{=} f(n, \mathrm{fib}(k+1) + \mathrm{fib}(k), \mathrm{fib}(k+1)) \overset{\mathrm{def}}{=}$$
$$= f(n, \mathrm{fib}(k+2), \mathrm{fib}(k+1)) \overset{\mathrm{IH}}{=} \mathrm{fib}(n+k+1) = \mathrm{fib}(n+1+k).$$

We are now ready to prove (4):

$$\mathrm{fib}(n) \overset{(5)}{=} f(n, \mathrm{fib}(1), \mathrm{fib}(0)) \overset{\mathrm{def}}{=} f(n, 1, 1).$$

11.3 Course of Values Recursion

11.3.1 Course of values recursive clausal definitions. Initial clauses of *course of values recursive clausal definitions* are clauses of a form

$$f(\vec{y},x,\vec{z}) = \alpha[\dot{\lambda}\vec{y}x\vec{z}.f(\vec{y},x,\vec{z});\vec{y},x,\vec{z}]$$

regular in measure x.

11.3.2 Integer division. Consider the following course of values recursive definition on x of the integer division $x \div y$:

$$x \div y = 0 \leftarrow y > 0 \land x < y$$
$$x \div y = (x \dot{-} y) \div y + 1 \leftarrow y > 0 \land x \geq y.$$

We claim that

$$\vDash_{\mathrm{PA}} \ y > 0 \rightarrow \exists r(x = x \div y \cdot y + r \land r < y). \tag{1}$$

The property is proved by complete induction on x. Assume $y > 0$, take any x and consider two cases. If $x < y$ then we satisfy (1) with substitution $r := x$ since we have

$$x \div y \cdot y + x \stackrel{\text{def}}{=} 0 \cdot y + x = x.$$

If $x \geq y$ then $x \dot{-} y < x$ and thus by IH applied to $x \dot{-} y$ there is a number r such that

$$x \dot{-} y = (x \dot{-} y) \div y \cdot y + r \land r < y. \tag{2}$$

We satisfy (1) with substitution $r := r$ since we have

$$x \div y \cdot y + r \stackrel{\text{def}}{=} ((x \dot{-} y) \div y + 1) \cdot y + r = (x \dot{-} y) \div y \cdot y + y + r \stackrel{(2)}{=}$$
$$= x \dot{-} y + y = x.$$

11.3.3 Greatest common divisor. Consider the following clausal definition of the greatest common divisor:

$$\gcd(x,0) = x$$
$$\gcd(x,y) = \gcd(y, x \bmod y) \leftarrow y > 0.$$

Since $\vDash_{\mathrm{PA}} \ y > 0 \rightarrow x \bmod y < y$ the definition of $\gcd(x,y)$ is by course of values recursion on y with substitution in parameter x. The idea of the algorithm is based on the observation

$$\vDash_{\mathrm{PA}} \ y > 0 \rightarrow z \mid x \land z \mid y \leftrightarrow z \mid y \land z \mid x \bmod y$$

which follows from the following facts

$$\vdash_{\text{PA}} y > 0 \to x = x \div y \cdot y + x \bmod y$$
$$\vdash_{\text{PA}} y > 0 \wedge z \mid x \wedge z \mid y \to z \mid x \bmod y$$
$$\vdash_{\text{PA}} y > 0 \wedge z \mid y \wedge z \mid x \bmod y \to z \mid x.$$

We claim that

$$\vdash_{\text{PA}} x > 0 \vee y > 0 \to \gcd(x,y) \mid x \wedge \gcd(x,y) \mid y \tag{1}$$
$$\vdash_{\text{PA}} (x > 0 \vee y > 0) \wedge z \mid x \wedge z \mid y \to z \leq \gcd(x,y). \tag{2}$$

Properties (1) and (2) are proved by complete induction on y with induction formulas $\forall x\,(1)$ and $\forall x\,(2)$, respectively.

11.3.4 Course of values recursive definitions with measure. Initial clauses of *course of values recursive clausal definitions with measure* are regular clauses of a form

$$f(\vec{x}) = \alpha[\dot{\lambda}\vec{x}.f(\vec{x}); \vec{x}].$$

11.3.5 Greatest common divisor. Consider the following course of values recursive definition with measure $x + y$ of the greatest common divisor $\gcd(x,y)$:

$$\gcd(x,y) = \gcd(x, y \dot{-} x) \leftarrow x > 0 \wedge y > 0 \wedge x < y$$
$$\gcd(x,y) = x \leftarrow x > 0 \wedge y > 0 \wedge x = y$$
$$\gcd(x,y) = \gcd(x \dot{-} y, y) \leftarrow x > 0 \wedge y > 0 \wedge x > y.$$

We claim that

$$\vdash_{\text{PA}} x > 0 \wedge y > 0 \to \gcd(x,y) \mid x \wedge \gcd(x,y) \mid y \tag{1}$$
$$\vdash_{\text{PA}} x > 0 \wedge y > 0 \wedge z \mid x \wedge z \mid y \to z \leq \gcd(x,y). \tag{2}$$

Property (1) is proved by measure induction with measure $x + y$.

11.3.6 Bottom up program for $\lfloor\sqrt{x}\rfloor$. The program for $\lfloor\sqrt{x}\rfloor$ given in Par. 11.2.6 can be improved in two respects. The first one is the shortening of the computation which goes from x, to $x-1, \ldots,$ until it reaches 0 and then it does the comparisons and the incrementation by one on the way back. As we already have commented above, the program is mathematically pleasing but every programmer will come up with a 'bottom up' program which searches starting with 0 for the smallest number s such that $x < (s+1)^2$. For this need an auxiliary function $f(x,r)$ defined by course of values recursion with measure $x \dot{-} r^2$:

$$f(x,r) = r \leftarrow x < (r+1)^2$$
$$f(x,r) = f(x, r+1) \leftarrow x \geq (r+1)^2.$$

We can now define the square root explicitly by

$$\vdash_{\text{PAx}} \lfloor\sqrt{x}\rfloor = f(x,0). \tag{1}$$

Note that only $\lfloor\sqrt{x}\rfloor$ tests are needed.

11.3.7 A faster program for $\lfloor\sqrt{x}\rfloor$ with accumulators. The second improvement is the saving of the repeated multiplication in the test $x+1 < (s+1)^2$ of the program for $\lfloor\sqrt{x}\rfloor$ in Par. 11.2.6 by an additional accumulator argument s maintained at the value $s = r^2$ during the computation of the following clausal definition of the ternary function $f(x,r,s)$:

$$f(x,r,s) = r \leftarrow s + 2\cdot r + 1 = s_1 \wedge x < s_1$$
$$f(x,r,s) = f(x, r+1, s_1) \leftarrow s + 2\cdot r + 1 = s_1 \wedge x \geq s_1 \,.$$

Note that this is a course of values recursive definition with measure $x \dot{-} s$. We can now define the square root function explicitly

$$\vdash_{\mathrm{PAx}} \lfloor\sqrt{x}\rfloor = f(x,0,0). \tag{1}$$

We claim that

$$\vdash_{\mathrm{PA}} \lfloor\sqrt{x}\rfloor^2 \leq x < (\lfloor\sqrt{x}\rfloor + 1)^2. \tag{2}$$

We first prove the following property of the function f:

$$\vdash_{\mathrm{PA}} r^2 \leq x \rightarrow f(x,r,r^2)^2 \leq x < (f(x,r,r^2)+1)^2 \tag{3}$$

by measure induction with measure $x \dot{-} r$. Assume $r^2 \leq x$, let $s := r^2 + 2\cdot r + 1 = (r+1)^2$ and consider two cases. If $x < s$ then (3) holds since we have

$$f(x,r,r^2)^2 \stackrel{\text{def}}{=} r^2 \leq x < s = (r+1)^2 \stackrel{\text{def}}{=} (f(x,r,r^2)+1)^2.$$

If $x \geq s$ then $x \dot{-} (r+1) < x \dot{-} r$ and thus by IH applied to x and $r+1$ we obtain

$$f(x, r+1, (r+1)^2)^2 \leq x < \bigl(f(x, r+1, (r+1)^2) + 1\bigr)^2. \tag{4}$$

From this we get (3) as follows

$$\begin{aligned} f(x,r,r^2)^2 &\stackrel{\text{def}}{=} f(x, r+1, (r+1)^2)^2 \stackrel{(4)}{\leq} x \stackrel{(4)}{<} \\ &< \bigl(f(x,r+1,(r+1)^2)+1\bigr)^2 \stackrel{\text{def}}{=} (f(x,r,r^2)+1)^2. \end{aligned}$$

We are now in position to prove (2):

$$\lfloor\sqrt{x}\rfloor^2 \stackrel{(1)}{=} f(x,0,0)^2 \stackrel{(3)}{\leq} x \stackrel{(3)}{<} (f(x,0,0)+1)^2 \stackrel{(1)}{=} (\lfloor\sqrt{x}\rfloor + 1)^2.$$

11.3.8 Simulation of for-loops by recursion. Consider the following Pascal-like program computing $\sum_{i=0}^{n} i$ into the variable a:

$a := 0;$
for $j := 1$ *to* n *do*
    $a := a + j;$.

We can simulate the for-loop by the following course of values recursive definition with measure $n + 1 \dot{-} j$:

$f(n, j, a) = a \leftarrow j > n$
$f(n, j, a) = f(n, j + 1, a + j) \leftarrow j \le n.$

We claim that

$$\vdash_{\mathrm{PA}} \sum_{i=0}^{n} i = f(n, 1, 0). \tag{1}$$

We first prove the following property of the function f:

$$\vdash_{\mathrm{PA}} 0 < j \le n + 1 \to f(n, j, \sum_{i=0}^{j \dot{-} 1} i) = \sum_{i=0}^{n} i \tag{2}$$

by measure induction with measure $n + 1 \dot{-} j$. Assume $0 < j \le n + 1$ and consider two cases. If $j = n + 1$ then (2) follows by definition. If $j \le n$ then $n + 1 \dot{-} (j + 1) < n + 1 \dot{-} j$ and we get (2) as follows

$$f(n, j, \sum_{i=0}^{j \dot{-} 1} i) \overset{\text{def}}{=} f(n, j + 1, \sum_{i=0}^{j \dot{-} 1} i + j) \overset{\text{def}}{=} f(n, j + 1, \sum_{i=0}^{j} i) =$$
$$= f(n, j + 1, \sum_{i=0}^{j+1 \dot{-} 1} i) \overset{\text{IH}}{=} \sum_{i=0}^{n} i.$$

We are now in position to prove (1):

$$\sum_{i=0}^{n} i \overset{(2)}{=} f(n, 1, \sum_{i=0}^{1 \dot{-} 1} i) = f(n, 1, \sum_{i=0}^{0} i) \overset{\text{def}}{=} f(n, 1, 0).$$

11.4 Recursion on Notation

Binary arithmetic

11.4.1 Binary representation of $\mathbb{N}$. We introduce two *binary successor* functions by explicit definitions:

$$\vdash_{\mathrm{PAx}} x\mathbf{0} = 2 \cdot x \tag{1}$$
$$\vdash_{\mathrm{PAx}} x\mathbf{1} = 2 \cdot x + 1. \tag{2}$$

Binary numerals are the least class of terms satisfying the following:

– the constant 0 is a binary numeral,
– if τ is a binary numeral distinct from 0 so is $\tau\mathbf{0}$,

– if τ is a binary numeral so is $\tau\mathbf{1}$.

We give here some examples of binary numerals:

$$
\begin{aligned}
0 &= 0\\
0\mathbf{1} &= 2\cdot 0+1 = 1\\
0\mathbf{10} &= 2\cdot(2\cdot 0+1) = 2\\
0\mathbf{11} &= 2\cdot(2\cdot 0+1)+1 = 3\\
0\mathbf{100} &= 2\cdot(2\cdot(2\cdot 0+1)) = 4\\
0\mathbf{101} &= 2\cdot(2\cdot(2\cdot 0+1))+1 = 5.
\end{aligned}
$$

11.4.2 Binary case analysis. We have the following principle of *binary case analysis*:

$$\vdash_{\mathrm{PA}} x = 0 \lor \exists y(y > 0 \land x = y\mathbf{0}) \lor \exists y\, x = y\mathbf{1}. \tag{1}$$

Property (1) follows directly from

$$\vdash_{\mathrm{PA}} x = x \div 2 \cdot 2 + x \bmod 2 \land x \bmod 2 < 2$$

holding by 7.4.8(1).

11.4.3 Binary induction. Let T be a proper extension of PA containing the binary successors, $\phi[x]$ a formula of $\mathcal{L}_T$ with the indicated variable x free and with possibly additional parameters. The formula of *binary induction on x for $\phi[x]$* is the following one:

$$\phi[0] \land \forall x(x > 0 \land \phi[x] \to \phi[x\mathbf{0}]) \land \forall x(\phi[x] \to \phi[x\mathbf{1}]) \to \phi[x].$$

11.4.4 Theorem. *Every proper extension T of PA containing the binary successors proves the schema of binary induction:*

$$T \vdash \phi[0] \land \forall x(x > 0 \land \phi[x] \to \phi[x\mathbf{0}]) \land \forall x(\phi[x] \to \phi[x\mathbf{1}]) \to \phi[x].$$

Proof. The principle of binary induction is reduced to mathematical induction as follows. Assume

$$\phi[0] \tag{1}$$

$$\forall x(x > 0 \land \phi[x] \to \phi[x\mathbf{0}]) \tag{2}$$

$$\forall x(\phi[x] \to \phi[x\mathbf{1}]) \tag{3}$$

and prove

$$\forall x(x < n \to \phi[x]) \tag{4}$$

by induction on n. In the base case, when $n = 0$, there is nothing to prove. In the inductive case take any x such that $x < n + 1$ and consider three cases. If $x = 0$ then $\phi[0]$ follows from the assumption (1). If $x = y\mathbf{0}$ for some $y > 0$ then, since $y < x \leq n$, we have $\phi[y]$ from IH: (4) and we get $\phi[y\mathbf{0}]$ from (2). The case when $x = y\mathbf{1}$ is proved similarly. This ends the proof of (4) and we obtain $\phi[x]$ by substituting $x + 1$ for n in (4). ◻

11.4.5 Binary recursion. Initial clauses for clausal definitions with binary recursion are of a form

$$f(\vec{y},x,\vec{z}) = \alpha_1[\vec{y},\vec{z}] \leftarrow x = 0$$
$$f(\vec{y},x,\vec{z}) = \alpha_2[\dot{\lambda}\vec{y}w\vec{z}.f(\vec{y},x_1,\vec{z});\vec{y},x_1,\vec{z}] \leftarrow x = x_1\mathbf{0} \land x_1 > 0$$
$$f(\vec{y},x,\vec{z}) = \alpha_2[\dot{\lambda}\vec{y}w\vec{z}.f(\vec{y},x_1,\vec{z});\vec{y},x_1,\vec{z}] \leftarrow x = x_1\mathbf{1}.$$

Note that the clauses are regular in the argument x.

11.4.6 Binary size. The *binary size* function $|x|_b$ yields the number of binary successors in the binary numeral denoting the number x. The function is defined by parameterless binary recursion as a primitive recursive function:

$$|0|_b = 0$$
$$|x\mathbf{0}|_b = |x|_b + 1 \leftarrow x > 0$$
$$|x\mathbf{1}|_b = |x|_b + 1.$$

The function satisfies the following

$$\vdash_{\mathrm{PA}} |x|_b = 0 \leftrightarrow x = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} |x|_b = n \leftrightarrow 2^n \div 2 \leq x < 2^n \tag{2}$$

Property (1) is proved by simple case analysis. Property (2) is a direct consequence of the following

$$2^{|x|_b} \div 2 \leq x < 2^{|x|_b} \tag{3}$$
$$\vdash_{\mathrm{PA}} \forall x(2^n \div 2 \leq x < 2^n \rightarrow |x|_b = n). \tag{4}$$

We prove (3) by binary induction on x. In the base case when $x = 0$ we have

$$2^{|0|_b} \div 2 \stackrel{\text{def}}{=} 2^0 \div 2 = 1 \div 2 = 0 \leq 0 < 1 = 2^0 \stackrel{\text{def}}{=} 2^{|0|_b}.$$

In the inductive case when $x = y\mathbf{0}$ for some $y > 0$ we have $|y|_b > 0$ by (1) and thus

$$2^{|y|_b} = 2 \cdot 2^{|y|_b \dot{-} 1} = 2 \cdot (2 \cdot 2^{|y|_b \dot{-} 1} \div 2) = 2 \cdot (2^{|y|_b} \div 2). \tag{5}$$

We obtain

$$2^{|y\mathbf{0}|_b} \div 2 \stackrel{\text{def}}{=} 2^{|y|_b+1} \div 2 = 2 \cdot 2^{|y|_b} \div 2 = 2^{|y|_b} \stackrel{(5)}{=}$$
$$= 2 \cdot (2^{|y|_b} \div 2) \stackrel{\text{IH}}{\leq} 2 \cdot y \stackrel{\text{IH}}{<} 2 \cdot 2^{|y|_b} = 2^{|y|_b+1} \stackrel{\text{def}}{=} 2^{|y\mathbf{0}|_b}.$$

The inductive case when $x = y\mathbf{1}$ is similar.

We prove (4) by induction on n. In the base case take any x and assume $x < 2^0 = 1$. Then $x = 0$ and we get $|0|_b = 0$ by definition. In the inductive take any x and assume $2^{n'} \div 2 \leq x < 2^{n'}$, ie

$$2^n \leq x < 2 \cdot 2^n. \tag{6}$$

We consider three cases. If $x = 0$ then (6) leads to contradiction. If $x = y\mathbf{0}$ for some $y > 0$ then $2^n \div 2 \leq y < 2^n$ from (6) and thus

$$|y\mathbf{0}|_b \stackrel{\text{def}}{=} |y|_b + 1 \stackrel{\text{IH}}{=} n + 1 = n'.$$

The case when $x = y\mathbf{1}$ is similar.

11.4.7 Program computing the successor function in binary representation. Consider the following program computing the successor function x' in binary representation:

$0' = 0\mathbf{1}$
$x\mathbf{0}' = x\mathbf{1} \leftarrow x > 0$
$x\mathbf{1}' = x'\mathbf{0}$.

We can visualize the above program as a binary example of the algorithm taught on decimal numerals in the elementary school:

$$\begin{array}{r} 0 \\ \mathbf{1} \\ \hline 0\mathbf{1} \end{array} \qquad \begin{array}{r} x\mathbf{0} \\ \mathbf{1} \\ \hline x\mathbf{1} \end{array} \qquad \begin{array}{r} x\mathbf{1} \\ \mathbf{1} \\ \hline x'\mathbf{0} \end{array}.$$

Let us denote temporarily by $S(x)$ the function defined by the above clausal definition. We claim that

$$S(x) = x'. \tag{1}$$

Property (1) is proved by binary induction on x. In the base case when $x = 0$ we have

$$S(0) \stackrel{\text{def}}{=} 0\mathbf{1} = 0'.$$

In the inductive case when $x = y\mathbf{0}$ for some $y > 0$ we have

$$S(y\mathbf{0}) \stackrel{\text{def}}{=} y\mathbf{1} = (y\mathbf{0})'.$$

In the inductive case when $x = y\mathbf{1}$ we have

$$S(y\mathbf{1}) \stackrel{\text{def}}{=} S(y)\mathbf{0} \stackrel{\text{IH}}{=} y'\mathbf{1} = y\mathbf{1}'.$$

11.4.8 Program computing the addition function in binary representation. The addition function $x + y$ has the following clausal definition by binary recursion on x with substitution in the parameter y:

$0 + y = y$
$x\mathbf{0} + 0 = x\mathbf{0} \leftarrow x > 0$
$x\mathbf{0} + y\mathbf{0} = (x + y)\mathbf{0} \leftarrow x > 0 \land y > 0$
$x\mathbf{0} + y\mathbf{1} = (x + y)\mathbf{1} \leftarrow x > 0$
$x\mathbf{1} + 0 = x\mathbf{1}$
$x\mathbf{1} + y\mathbf{0} = (x + y)\mathbf{1}$
$x\mathbf{1} + y\mathbf{1} = (x + y)'\mathbf{0}$.

The recurrences in the 'elementary school' form are:

$$\begin{array}{r} 0\\ y\\ \hline y \end{array}\qquad \begin{array}{r} x\mathbf{0}\\ 0\\ \hline x\mathbf{0} \end{array}\qquad \begin{array}{r} x\mathbf{0}\\ y\mathbf{0}\\ \hline (x+y)\mathbf{0} \end{array}\qquad \begin{array}{r} x\mathbf{0}\\ y\mathbf{1}\\ \hline (x+y)\mathbf{1} \end{array}$$

$$\begin{array}{r} x\mathbf{1}\\ 0\\ \hline x\mathbf{1} \end{array}\qquad \begin{array}{r} x\mathbf{1}\\ y\mathbf{0}\\ \hline (x+y)\mathbf{1} \end{array}\qquad \begin{array}{r} x\mathbf{1}\\ y\mathbf{1}\\ \hline (x+y)'\mathbf{0} \end{array}.$$

We can, for instance, compute $3+5=8$ as follows:

$$\begin{aligned} 0\mathbf{11} + 0\mathbf{101} &= (0\mathbf{1} + 0\mathbf{10})'\mathbf{0} = ((0 + 0\mathbf{1})\mathbf{1})'\mathbf{0} = (0\mathbf{11})'\mathbf{0} = \\ &= (0\mathbf{1})'\mathbf{00} = 0'\mathbf{000} = 0\mathbf{1000}. \end{aligned}$$

Let us denote temporarily by $x +_b y$ the function defined by the above clausal definition. We prove

$$\vdash_{\mathrm{PA}} x +_b y = x + y \tag{1}$$

by binary induction on x with induction formula $\forall y(1)$. In the base case when $x = 0$ take any y and we have

$$0 +_b y \stackrel{\text{def}}{=} y = 0 + y.$$

In the inductive case when $x = x_1\mathbf{1}$ for some x_1 take any y and consider three cases. If $y = 0$ then we have

$$x_1\mathbf{1} +_b 0 \stackrel{\text{def}}{=} x_1\mathbf{1} = x_1\mathbf{1} + 0.$$

If $y = y_1\mathbf{0}$ for some $y_1 > 0$ then we have

$$x_1\mathbf{1} +_b y_1\mathbf{0} \stackrel{\text{def}}{=} (x_1 +_b y_1)\mathbf{1} \stackrel{\text{IH}}{=} (x_1 + y_1)\mathbf{1} = x_1\mathbf{1} + y_1\mathbf{0}.$$

If $y = y_1\mathbf{1}$ for some y_1 then we have

$$x_1\mathbf{1} +_b y_1\mathbf{1} \stackrel{\text{def}}{=} (x_1 +_b y_1)'\mathbf{0} \stackrel{\text{IH}}{=} (x_1 + y_1)'\mathbf{0} = x_1\mathbf{1} + y_1\mathbf{1}.$$

The inductive case when $x = x_1\mathbf{1}$ is similar.

11.4.9 Program computing the equality predicate in binary representation. The equality predicate $x = y$ has the following clausal definition by binary recursion on x with substitution in the parameter y:

$0 = 0$
$x\mathbf{0} = y\mathbf{0} \leftarrow x > 0 \land y > 0 \land x = y$
$x\mathbf{1} = y\mathbf{1} \leftarrow x = y.$

Let us denote temporarily by $x =_b y$ the predicate defined by the above clausal definition. We prove

$$\vdash_{\mathrm{PA}} x =_b y \leftrightarrow x = y \tag{1}$$

by binary induction on x with induction formula $\forall y(1)$.

In the base case when $x = 0$ take any y and consider three cases. If $y = 0$ then $0 =_b 0$ by definition and we are done. If $y = y_1\mathbf{0}$ for some $y_1 > 0$ or $y = y_1\mathbf{1}$ for some y_1 then $0 \neq_b y$ by definition and since also $0 \neq y$ we get $0 =_b y \leftrightarrow 0 = y$.

In the inductive case when $x = x_1\mathbf{0}$ for some $x_1 > 0$ take any y and consider three cases. If $y = y_1\mathbf{0}$ for some $y_1 > 0$ then we have

$$x_1\mathbf{0} =_b y_1\mathbf{0} \overset{\text{def}}{\Leftrightarrow} x_1 =_b y_1 \overset{\text{IH}}{\Leftrightarrow} x_1 = y_1 \Leftrightarrow x_1\mathbf{0} = y_1\mathbf{0}.$$

Otherwise, if either $y = 0$ or $y = y_1\mathbf{1}$ for some y_1 then $x_1\mathbf{0} \neq_b y$ by definition and since also $x_1\mathbf{0} \neq y$ we get $x_1\mathbf{0} =_b y \leftrightarrow x_1\mathbf{0} = y$. The inductive case when $x = x_1\mathbf{1}$ is similar.

p-ary arithmetic

11.4.10 p-ary case analysis. For a base $p > 1$ we have the principle of *p-ary case analysis*:

$$\vdash_{\mathrm{PA}} \exists y \exists z(x = p \cdot y + z \land z < p). \tag{1}$$

Property (1) follows directly from

$$\vdash_{\mathrm{PA}} x = x \div p \cdot p + x \bmod p \land x \bmod p < p$$

holding by 7.4.8(1).

11.4.11 p-ary induction. Let T be a proper extension of PA, p a constant of T such that $T \vdash p > 1$, $\phi[x]$ a formula of $\mathcal{L}_T$ with the indicated variable x free and with possibly additional parameters, and y and z new variables. The formula of *p-ary induction on x for $\phi[x]$* is the following one:

$$\forall z(z < p \to \phi[z]) \land \forall y \forall z(z < p \land y > 0 \land \phi[y] \to \phi[p \cdot y + z]) \to \phi[x].$$

11.4.12 Theorem. *Every proper extension T of PA proves the schema of p-ary induction:*

$$T \vdash \forall z(z < p \to \phi[z]) \land \forall y \forall z(z < p \land y > 0 \land \phi[y] \to \phi[p \cdot y + z]) \to \phi[x] \ .$$

Proof. The principle of p-ary induction is reduced to mathematical induction as follows. Assume

$$\forall z(z < p \to \phi[z]) \tag{1}$$
$$\forall y \forall z(z < p \land y > 0 \land \phi[y] \to \phi[p \cdot y + z]) \tag{2}$$

and prove

$$\forall x(x < n \to \phi[x]) \tag{3}$$

by induction on n. In the base case, when $n = 0$, there is nothing to prove. In the inductive case take any x such that $x < n + 1$. By 11.4.10(1) there are numbers y and $z < p$ such that $x = p \cdot y + z$. We consider two cases. If $y = 0$ then $\phi[x]$ follows from the assumption (1). If $y > 0$ then, since $y < x \leq n$, we have $\phi[y]$ from IH: (3) and we get $\phi[p \cdot y + z]$ from (2). This ends the proof of (3) and we obtain $\phi[x]$ by substituting $x + 1$ for n in (3). □

11.4.13 p-ary recursion. Initial clauses for clausal definitions with p-ary recursion are of a form:

$$f(\vec{y}, x, \vec{z}) = \alpha_1[\vec{y}, \vec{z}, r] \leftarrow x = p{\cdot}x_1{+}r \land r < p \land x_1 = 0$$
$$f(\vec{y}, x, \vec{z}) = \alpha_2[\lambda \vec{y} w \vec{z}.f(\vec{y}, x_1, \vec{z}); \vec{y}, x_1, \vec{z}, r] \leftarrow x = p{\cdot}x_1{+}r \land r < p \land x_1 > 0.$$

Note that the clauses are regular in the argument x.

11.4.14 A fast program for the square root function. From the point of view of computational complexity the improvement of the accumulator program for the function $\lfloor\sqrt{x}\rfloor$ in Par. 11.3.7 over the program in Par. 11.2.6 is insignificant because both programs work in the monadic representation. We can obtain a fast $O(|x|_b)$ program for $\lfloor\sqrt{x}\rfloor$ by recalling a high school algorithm working with the decimal, or rather centennial, notation because it considers two decimal digits at a time. The recursion does not work well in the decimal notation because we have $\lfloor\sqrt{10{\cdot}x + d}\rfloor \approx \lfloor\sqrt{10}\rfloor{\cdot}\lfloor\sqrt{x}\rfloor$ while it works well in the centennial notation because $\lfloor\sqrt{100{\cdot}x + d}\rfloor \approx 10{\cdot}\lfloor\sqrt{x}\rfloor$.

The same works in the 4-ary representation where for every z there are unique numbers x and i such that $z = 4 \cdot x + i$ and $i < 4$. The reason why we have chosen this range for i is that we have $|i|_b = 2$ and we can make use of fast pattern matching with the numeric pattern $4 \cdot x + i$ (just consider the last two binary digits of the binary representation of z) and fast multiplication $4 \cdot y + i$ (just append the two binary digits of i at the end of y).

Thus assume as IH that we have for $x > 0$

$$\lfloor\sqrt{x}\rfloor^2 \leq x < (\lfloor\sqrt{x}\rfloor + 1)^2.$$

From the last we obtain $x \leq \lfloor\sqrt{x}\rfloor^2 + 2 \cdot \lfloor\sqrt{x}\rfloor$ and so we get for $i < 4$:

$$\begin{aligned}(2 \cdot \lfloor\sqrt{x}\rfloor)^2 \leq 4 \cdot x \leq 4 \cdot x + i \leq 4 \cdot \lfloor\sqrt{x}\rfloor^2 + 8 \cdot \lfloor\sqrt{x}\rfloor + i <\\ < 4 \cdot \lfloor\sqrt{x}\rfloor^2 + 8 \cdot \lfloor\sqrt{x}\rfloor + 4 = (2 \cdot \lfloor\sqrt{x}\rfloor + 2)^2.\end{aligned}$$

This means that we have

$$2 \cdot \lfloor\sqrt{x}\rfloor \leq \lfloor\sqrt{4 \cdot x + i}\rfloor \leq 2 \cdot \lfloor\sqrt{x}\rfloor + 1$$

and so the following clausal definition is a fast program for $\lfloor\sqrt{x}\rfloor$:

$$\begin{aligned}
&\lfloor\sqrt{4 \cdot x + i}\rfloor = \mathrm{sgn}(i) \leftarrow i < 4 \wedge x = 0\\
&\lfloor\sqrt{4 \cdot x + i}\rfloor = s \leftarrow i < 4 \wedge x > 0 \wedge 2 \cdot \lfloor\sqrt{x}\rfloor = s \wedge 4 \cdot x + i < (s+1)^2\\
&\lfloor\sqrt{4 \cdot x + i}\rfloor = s + 1 \leftarrow i < 4 \wedge x > 0 \wedge 2 \cdot \lfloor\sqrt{x}\rfloor = s \wedge 4 \cdot x + i \geq (s+1)^2.
\end{aligned}$$

The reader will note that the assignment $2 \cdot \lfloor\sqrt{x}\rfloor = s$ is crucial to the speed of the program because without it we would have two recursive invocations in the test $4 \cdot x + i < (2 \cdot x + 1) \cdot (2 \cdot x + 1)$. Consequently, as the depth of recursion is $O(|x|_b)$, we would have $O(2^{|x|_b}) = O(x)$ recursive invocations and the definition would not be any faster than the one by primitive recursion.

Dyadic arithmetic

11.4.15 Dyadic representation of $\mathbb{N}$. We introduce two *dyadic successor* functions by explicit definitions:

$$\vdash_{\mathrm{PAx}} x\mathbf{1} = 2 \cdot x + 1 \tag{1}$$

$$\vdash_{\mathrm{PAx}} x\mathbf{2} = 2 \cdot x + 2. \tag{2}$$

Dyadic numerals are the least class of terms satisfying the following:

– the constant 0 is a dyadic numeral,
– if τ is a dyadic numeral so are $\tau\mathbf{1}$ and $\tau\mathbf{2}$.

We give here some examples of dyadic numerals:

$$\begin{aligned}
0 &= 0\\
0\mathbf{1} &= 2 \cdot 0 + 1 = 1\\
0\mathbf{2} &= 2 \cdot 0 + 2 = 2\\
0\mathbf{11} &= 2 \cdot (2 \cdot 0 + 1) + 1 = 3\\
0\mathbf{12} &= 2 \cdot (2 \cdot 0 + 1) + 2 = 4\\
0\mathbf{21} &= 2 \cdot (2 \cdot 0 + 2) + 1 = 5\\
0\mathbf{22} &= 2 \cdot (2 \cdot 0 + 2) + 2 = 6\\
0\mathbf{111} &= 2 \cdot (2 \cdot (2 \cdot 0 + 1) + 1) + 1 = 7.
\end{aligned}$$

11.4.16 Dyadic case analysis. We have the following principle of *dyadic case analysis*:

$$\vdash_{\mathrm{PA}} x = 0 \vee \exists y\, x = y\mathbf{1} \vee \exists y\, x = y\mathbf{2}. \tag{1}$$

Property (1) follows from

$$\begin{aligned}
&\vdash_{\mathrm{PA}} x \neq 0 \rightarrow\\
&\qquad x = (x \dot{-} 1) \div 2 \cdot 2 + (x \dot{-} 1) \bmod 2 + 1 \wedge 0 < (x \dot{-} 1) \bmod 2 + 1 \leq 2
\end{aligned}$$

which is a direct consequence of

$$\vdash_{\mathrm{PA}} x \dot{-} 1 = (x \dot{-} 1) \div 2 \cdot 2 + (x \dot{-} 1) \bmod 2 \wedge (x \dot{-} 1) \bmod 2 < 2$$

holding by 7.4.8(1).

11.4.17 Dyadic induction. Let T be a proper extension of PA containing the dyadic successors, $\phi[x]$ a formula of $\mathcal{L}_T$ with the indicated variable x free and with possibly additional parameters. The formula of *dyadic induction on x for* $\phi[x]$ is the following one:

$$\phi[0] \wedge \forall x(\phi[x] \to \phi[x\mathbf{1}]) \wedge \forall x(\phi[x] \to \phi[x\mathbf{2}]) \to \phi[x].$$

11.4.18 Theorem. *Every proper extension T of PA containing the dyadic successors proves the schema of dyadic induction:*

$$T \vdash \phi[0] \wedge \forall x(\phi[x] \to \phi[x\mathbf{1}]) \wedge \forall x(\phi[x] \to \phi[x\mathbf{2}]) \to \phi[x].$$

Proof. We can reduce the principle of dyadic induction to mathematical induction similarly as in the case of binary induction (see the proof of Thm. 11.4.4). □

11.4.19 Dyadic recursion. Initial clauses for clausal definitions with dyadic recursion are of a form

$$f(\vec{y}, x, \vec{z}) = \alpha_1[\vec{y}, \vec{z}] \leftarrow x = 0$$
$$f(\vec{y}, x, \vec{z}) = \alpha_2[\dot{\lambda}\vec{y}w\vec{z}.f(\vec{y}, x_1, \vec{z}); \vec{y}, x_1, \vec{z}] \leftarrow x = x_1\mathbf{1}$$
$$f(\vec{y}, x, \vec{z}) = \alpha_2[\dot{\lambda}\vec{y}w\vec{z}.f(\vec{y}, x_1, \vec{z}); \vec{y}, x_1, \vec{z}] \leftarrow x = x_1\mathbf{2}.$$

Note that the clauses are regular in the argument x.

11.4.20 Dyadic size. The *dyadic size* function $|x|_d$ yields the number of dyadic successors in the dyadic numeral denoting the number x. The function is defined by parameterless dyadic recursion as a primitive recursive function:

$$|0|_d = 0$$
$$|x\mathbf{1}|_d = |x|_d + 1$$
$$|x\mathbf{2}|_d = |x|_d + 1.$$

The function satisfies the following

$$\vdash_{\mathrm{PA}} |x|_d = 0 \leftrightarrow x = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} |x|_d = n \leftrightarrow 2^n \leq x + 1 < 2^{n+1}. \tag{2}$$

Property (1) is proved by simple dyadic case analysis. Property (2) is proved by induction on n with induction formula $\forall x\,(2)$. In the base take any x and we have

$$|x|_d = 0 \overset{(1)}{\Leftrightarrow} x = 0 \Leftrightarrow 1 \leq 0+1 < 2 \Leftrightarrow 2^0 \leq 0+1 < 2^{0+1}.$$

In the inductive case take any x and consider three cases. If $x = 0$ then the claim follows from the following facts: $|0|_d = 0 \neq n+1$ and $2^{n+1} > 1 = 0+1$. If $x = y\mathbf{1}$ for some y then we have

$$\begin{aligned}|y\mathbf{1}|_d = n+1 &\overset{\text{def}}{\Leftrightarrow} |y|_d = n \overset{\text{IH}}{\Leftrightarrow} 2^n \leq y+1 < 2^{n+1} \overset{9.0.17(1);7.3.6(3)}{\Leftrightarrow} \\ &\Leftrightarrow 2\cdot 2^n \leq 2\cdot(y+1) < 2\cdot 2^{n+1} \Leftrightarrow 2^{n+1} \leq y\mathbf{1}+1 < 2^{n+2}.\end{aligned}$$

If $x = y\mathbf{2}$ for some y then we have

$$\begin{aligned}|y\mathbf{2}|_d = n+1 &\overset{\text{def}}{\Leftrightarrow} |y|_d = n \overset{\text{IH}}{\Leftrightarrow} 2^n \leq y+1 < 2^{n+1} \overset{9.0.17(3);9.0.17(4)}{\Leftrightarrow} \\ &\Leftrightarrow 2\cdot 2^n \leq 2\cdot(y+1)+1 < 2\cdot 2^{n+1} \Leftrightarrow 2^{n+1} \leq y\mathbf{2}+1 < 2^{n+2}.\end{aligned}$$

11.4.21 Dyadic concatenation. The binary function $x \star y$, called *dyadic concatenation*, yields a number whose dyadic representation is obtained from dyadic representations of x and y by appending the digits of y after the digits of x. The dyadic concatenation function $x \star y$ is the arithmetization of the word function concatenating words over the alphabet $\{\mathbf{1}, \mathbf{2}\}$ and it is defined by dyadic recursion on y as a primitive recursive function:

$$\begin{aligned}&x \star 0 = x \\ &x \star y\mathbf{1} = (x \star y)\mathbf{1} \\ &x \star y\mathbf{2} = (x \star y)\mathbf{2}.\end{aligned}$$

From the reccurrences we get

$$\vdash_{\text{PA}} x \star y = x \cdot 2^{|y|_d} + y \tag{1}$$
$$\vdash_{\text{PA}} x \star y = 0 \leftrightarrow x = 0 \land y = 0 \tag{2}$$
$$\vdash_{\text{PA}} 0 \star y = y \tag{3}$$
$$\vdash_{\text{PA}} (x \star y) \star z = x \star (y \star z) \tag{4}$$
$$\vdash_{\text{PA}} |x \star y|_d = |x|_d + |y|_d. \tag{5}$$

We prove here only the properties (1) and (4). The remaining properties are left to the reader as an exercise.

Property (1) is proved by dyadic induction on y. In the base case we have

$$x \star 0 \overset{\text{def}}{=} x = x \cdot 1 + 0 = x \cdot 2^0 + 0 \overset{\text{def}}{=} x \cdot 2^{|0|_d} + 0.$$

In the inductive case when $y = y_1\mathbf{1}$ we have

$$\begin{aligned}x \star y_1\mathbf{1} &\overset{\text{def}}{=} (x \star y_1)\mathbf{1} \overset{\text{IH}}{=} (x \cdot 2^{|y_1|_d} + y_1)\mathbf{1} = 2\cdot(x \cdot 2^{|y_1|_d} + y_1) + 1 = \\ &= x \cdot 2^{|y_1|_d+1} + 2\cdot y_1 + 1 \overset{\text{def}}{=} x \cdot 2^{|y_1\mathbf{1}|_d} + y_1\mathbf{1}.\end{aligned}$$

The inductive case when $y = y_1\mathbf{2}$ is proved similarly.

Property (4) is proved by dyadic induction on z. In the base case we have

$$(x \star y) \star 0 \overset{\text{def}}{=} x \star y \overset{\text{def}}{=} x \star (y \star 0).$$

In the inductive case when $z = z_1\mathbf{2}$ we have

$$(x \star y) \star z_1\mathbf{1} \overset{\text{def}}{=} ((x \star y) \star z_1)\mathbf{1} \overset{\text{IH}}{=} (x \star (y \star z_1))\mathbf{1} \overset{\text{def}}{=} x \star (y \star z_1)\mathbf{1} \overset{\text{def}}{=} x \star (y \star z_1\mathbf{1}).$$

The inductive case when $z = z_1\mathbf{2}$ is proved similarly.

11.4.22 Dyadic reversal.

$Rev_d(0) = 0$
$Rev_d(x\mathbf{1}) = 0\mathbf{1} \star Rev_d(x)$
$Rev_d(x\mathbf{2}) = 0\mathbf{2} \star Rev_d(x).$

From the reccurrences we get

$$\vdash_{\text{PA}} Rev_d(x) = 0 \leftrightarrow x = 0 \tag{1}$$
$$\vdash_{\text{PA}} Rev_d(x \star y) = Rev_d(y) \star Rev_d(x) \tag{2}$$
$$\vdash_{\text{PA}} Rev_d\, Rev_d(x) = x \tag{3}$$
$$\vdash_{\text{PA}} Rev_d(x) = Rev_d(y) \rightarrow x = y \tag{4}$$
$$\vdash_{\text{PA}} |Rev_d(x)|_d = |x|_d. \tag{5}$$

Property (2) is proved by dyadic induction on y. In the base case we have

$$Rev_d(x \star 0) \overset{\text{def}}{=} Rev_d(x) \overset{11.4.21(3)}{=} 0 \star Rev_d(x).$$

In the inductive case when $y = y_1\mathbf{1}$ we have

$$\begin{aligned} Rev_d(x \star y_1\mathbf{1}) &\overset{\text{def}}{=} Rev_d((x \star y_1)\mathbf{1}) \overset{\text{def}}{=} \\ &= 0\mathbf{1} \star Rev_d(x \star y_1) \overset{\text{IH}}{=} 0\mathbf{1} \star (Rev_d(y_1) \star Rev_d(x)) \overset{11.4.21(4)}{=} \\ &= (0\mathbf{1} \star Rev_d(y_1)) \star Rev_d(x) \overset{\text{def}}{=} Rev_d(y_1\mathbf{1}) \star Rev_d(x). \end{aligned}$$

The inductive case when $y = y_1\mathbf{2}$ is proved similarly.

Property (3) is dyadic by induction on x. (3). Property (4) follows from (3). The remaining properties are left to the reader as an exercise.

11.4.23 Cancellation laws for dyadic concatenation. Cancellation rules for the dyadic concatenation are:

$$\vdash_{\text{PA}} x \star z = y \star z \rightarrow x = y \tag{1}$$
$$\vdash_{\text{PA}} z \star x = z \star y \rightarrow x = y. \tag{2}$$

Property (1) is proved by dyadic induction on z. In the base case we have

$$x \star 0 = y \star 0 \overset{\text{def}}{\Rightarrow} x = y.$$

In the inductive case when $z = z_1\mathbf{1}$ we have

$$x \star z_1\mathbf{1} = y \star z_1\mathbf{1} \overset{\text{def}}{\Rightarrow} (x \star z_1)\mathbf{1} = (y \star z_1)\mathbf{1} \Rightarrow x \star z_1 = y \star z_1 \overset{\text{IH}}{\Rightarrow} x = y.$$

The inductive case when $z = z_1\mathbf{2}$ is proved similarly.

Property (2) is proved as follows:

$$z \star x = z \star y \Rightarrow Rev_d(z \star x) = Rev_d(z \star y) \overset{11.4.22(2)}{\Rightarrow} Rev_d(x) \star Rev_d(z) =$$
$$= Rev_d(y) \star Rev_d(z) \overset{(1)}{\Rightarrow} Rev_d(x) = Rev_d(y) \overset{11.4.22(4)}{\Rightarrow} x = y.$$

11.5 Exercises

11.5.1 Exercise. Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} \min(x,y) = \min(y,x)\\
&\vdash_{\mathrm{PA}} \min(x,\min(y,z)) = \min(\min(x,y),z)\\
&\vdash_{\mathrm{PA}} \min(x,0) = 0.
\end{aligned}$$

11.5.2 Exercise. Find an explicit clausal definition of the maximum function $\max(x,y)$ satisfying

$$\begin{aligned}
&\vdash_{\mathrm{PA}} \max(x,y) \geq x\\
&\vdash_{\mathrm{PA}} \max(x,y) \geq y\\
&\vdash_{\mathrm{PA}} \max(x,y) = x \lor \max(x,y) = y.
\end{aligned}$$

Prove that the function has the required properties.

11.5.3 Exercise. Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} \max(x,y) = \max(y,x)\\
&\vdash_{\mathrm{PA}} \max(x,\max(y,z)) = \max(\max(x,y),z)\\
&\vdash_{\mathrm{PA}} \max(x,0) = x.
\end{aligned}$$

11.5.4 Exercise. Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} \min(x,y) \leq \max(x,y)\\
&\vdash_{\mathrm{PA}} \min(x,y) = \max(x,y) \leftrightarrow x = y\\
&\vdash_{\mathrm{PA}} \min(x,\max(y,z)) = \max(\min(x,y),\min(x,z))\\
&\vdash_{\mathrm{PA}} \max(x,\min(y,z)) = \min(\max(x,y),\max(x,z)).
\end{aligned}$$

11.5.5 Exercise. Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} \min(x+y, x+z) = x + \min(y,z)\\
&\vdash_{\mathrm{PA}} \max(x+y, x+z) = x + \max(y,z)\\
&\vdash_{\mathrm{PA}} \min(x\cdot y, x\cdot z) = x \cdot \min(y,z)\\
&\vdash_{\mathrm{PA}} \max(x\cdot y, x\cdot z) = x \cdot \max(y,z)\\
&\vdash_{\mathrm{PA}} \min(x \dot{-} y, x \dot{-} z) = x \dot{-} \max(y,z)\\
&\vdash_{\mathrm{PA}} \min(y \dot{-} x, z \dot{-} x) = \min(y,z) \dot{-} x\\
&\vdash_{\mathrm{PA}} \max(x \dot{-} y, x \dot{-} z) = x \dot{-} \min(y,z)\\
&\vdash_{\mathrm{PA}} \max(y \dot{-} x, z \dot{-} x) = \max(y,z) \dot{-} x.
\end{aligned}$$

11.5.6 Exercise. Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} x \le y \to \min(x,z) \le \min(y,z)\\
&\vdash_{\mathrm{PA}} x \ge y \to \min(x,z) \ge \min(y,z)\\
&\vdash_{\mathrm{PA}} x \le y \to \max(x,z) \le \max(y,z)\\
&\vdash_{\mathrm{PA}} x \ge y \to \max(x,z) \ge \max(y,z).
\end{aligned}$$

11.5.7 Exercise. Find an explicit clausal definition of the ternary function $Median(x,y,z)$ satisfying

$$\begin{aligned}
&\vdash_{\mathrm{PA}} x \le y \le z \to Median(x,y,z) = y\\
&\vdash_{\mathrm{PA}} Median(x,y,z) = Median(y,x,z)\\
&\vdash_{\mathrm{PA}} Median(x,y,z) = Median(x,z,y).
\end{aligned}$$

Prove that the function has the required properties.

11.5.8 Exercise. Consider the following primitive recursive definition of the integer division function $x \div y$:

$$\begin{aligned}
&0 \div y = 0\\
&(x+1) \div y = q \leftarrow x \div y = q \land x + 1 \dot{-} q \cdot y < y\\
&(x+1) \div y = q + 1 \leftarrow x \div y = q \land x + 1 \dot{-} q \cdot y \ge y.
\end{aligned}$$

Prove

$$\vdash_{\mathrm{PA}} y > 0 \to \exists r(x = x \div y \cdot y + r \land r < y).$$

11.5.9 Exercise. Let f be a function such that

$$\vdash_{\mathrm{PA}} \forall x \exists y\, x < f(y) \land f(0) = 0.$$

Prove

$$\vdash_{\mathrm{PA}} \exists r(f(r) \le x < f(r+1)).$$

Hint. First prove the following property

$$\vdash_{\mathrm{PA}} x < f(y) \to \exists r(f(r) \le x < f(r+1)).$$

11.5.10 Exercise. Let f be a function such that $\vdash_{\mathrm{PA}} \exists y\, x < fg(x)$ and $\vdash_{\mathrm{PA}} f(0) = 0$. Consider the following clausal definition of the function $r(x)$:

$$\begin{aligned}
&r_1(0,x) = 0\\
&r_1(y+1,x) = y \leftarrow f(y) \le x\\
&r_1(y+1,x) = r_1(y,x) \leftarrow f(y) > x
\end{aligned}$$

$$r(x) = r_1(g(x),x).$$

Prove

$$\vdash_{\mathrm{PA}} f\,r(x) \le x < f(r(x)+1).$$

11.5.11 Exercise. Consider the following primitive recursive definition on y with substitution in parameter x of the modified subtraction function $x \dot{-} y$:

$$\begin{aligned}
&x \dot{-} 0 = x\\
&0 \dot{-} y' = 0\\
&x' \dot{-} y' = x \dot{-} y.
\end{aligned}$$

Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} x \ge y \to x = y + (x \dot{-} y)\\
&\vdash_{\mathrm{PA}} x \le y \to x \dot{-} y = 0.
\end{aligned}$$

11.5.12 Exercise. Consider the function $f(n,a)$ defined by primitive recursion on n with substitution in parameter:

$$\begin{aligned}
&f(0,a) = a\\
&f(n+1,a) = f(n,a+n+1).
\end{aligned}$$

Prove

$$\vdash_{\mathrm{PA}} \sum_{i=0}^{n} i = f(n,0).$$

Hint. First prove the following property

$$\vdash_{\mathrm{PA}} f(n,a) = \sum_{i=0}^{n} i + a.$$

11.5.13 Exercise. Consider the function $f(n, a)$ defined by primitive recursion on n with substitution in parameter:

$$f(0, a) = a$$
$$f(n+1, a) = f(n, a \cdot (n+1)).$$

Prove

$$\vdash_{\mathrm{PA}} n! = f(n, 1).$$

11.5.14 Exercise. Consider the following functions $f(n)$ and $g(n, a, b, c)$:

$$f(0) = 0$$
$$f(1) = 1$$
$$f(2) = 2$$
$$f(n+3) = f(n+2) + f(n+1) + f(n)$$

$$g(0, a, b, c) = c$$
$$g(n+1, a, b, c) = g(n, a+b+c, a, b).$$

Prove

$$\vdash_{\mathrm{PA}} f(n) = g(n, 2, 1, 0).$$

11.5.15 Exercise. Consider the following functions $f(n)$ and $g(n, a, b, c)$:

$$f(0) = 0$$
$$f(1) = 1$$
$$f(n+2) = f(n+1) + f(n) + n$$

$$g(0, k, a, b) = b$$
$$g(n+1, k, a, b) = g(n, k+1, a+b+k, a) \ .$$

Prove

$$\vdash_{\mathrm{PA}} f(n) = g(n, 0, 1, 0).$$

Hint. First prove the following property

$$\vdash_{\mathrm{PA}} g(n, k, f(k+1), f(k)) = f(n+k).$$

11.5.16 Exercise. Consider the following course of values recursive definition on x of the remainder function $x \bmod y$: recursion on x as follows:

$$x \bmod y = x \leftarrow y > 0 \land x < y$$
$$x \bmod y = (x \dot{-} y) \bmod y \leftarrow y > 0 \land x \geq y.$$

Prove

$$\vdash_{\mathrm{PA}} y > 0 \rightarrow \exists q(x = q \cdot y + x \bmod y \land x \bmod y < y).$$

11.5.17 Exercise. Let f be a function such that $\vdash_{\mathrm{PA}} \exists y\, x < fg(x)$ and $\vdash_{\mathrm{PA}} f(0) = 0$. Consider the following clausal definition of the function $r(x)$:

$$r_1(y,x) = y \leftarrow x < f(y+1)$$
$$r_1(y,x) = r_1(y+1,x) \leftarrow x \geq f(y+1) \wedge y < g(x)$$

$$r(x) = r_1(0,x).$$

Prove

$$\vdash_{\mathrm{PA}} f\,r(x) \leq x < f(r(x)+1).$$

11.5.18 Exercise. Consider the function $f(n,j,a)$ defined by course of values recursion with measure $n \dot{-} j$:

$$f(n,j,a) = a \leftarrow j = n$$
$$f(n,j,a) = f(n,m+1,a+m+1) \leftarrow j < n.$$

Prove

$$\vdash_{\mathrm{PA}} \sum_{i=0}^{n} i = f(n,0,0).$$

11.5.19 Exercise. Consider the function $f(n,i,a)$ defined by course of values recursion with measure

$$f(n,i,a) = a \leftarrow i > n$$
$$f(n,i,a) = f(n,i+1,i \cdot a) \leftarrow i \leq n.$$

Prove

$$\vdash_{\mathrm{PA}} n! = f(n,1,1).$$

11.5.20 Exercise. Consider the function $f(n,i,a)$ defined by course of values recursion with measure

$$f(n,i,a) = a \leftarrow i = n$$
$$f(n,i,a) = f(n,i+1,(i+1) \cdot a) \leftarrow i < n.$$

Prove

$$\vdash_{\mathrm{PA}} n! = f(n,0,1).$$

11.5.21 Exercise. Define the predecessor function $x \dot{-} 1$ by binary recursion and verify your implementation.

11.5.22 Exercise. Define the multiplication function $x \cdot y$ by binary recursion and verify your implementation.

11.5.23 Exercise. Define the exponentiation function x^y by binary recursion and verify your implementation.

11.5.24 Exercise. Define by binary recursion the trichotomic comparision function $Comp(x, y)$ satisfying:

$$\vdash_{\text{PA}} Comp(x, y) = 0 \leftrightarrow x < y$$
$$\vdash_{\text{PA}} Comp(x, y) = 1 \leftrightarrow x = y$$
$$\vdash_{\text{PA}} Comp(x, y) = 2 \leftrightarrow x > y.$$

Prove that the function has the required properties.

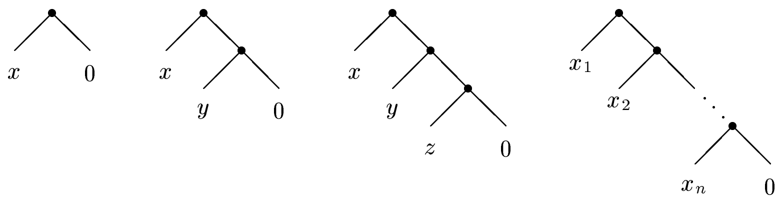
11.5.25 Exercise. Define the predicate $x \leq y$ by binary recursion and verify your implementation.

11.5.26 Exercise. Define the predicate $x < y$ by binary recursion and verify your implementation.

12. Programs Operating on Lists

12.1 Lists

12.1.1 List representation of $\mathbb{N}$. There is a simple way of arithmetizing finite sequences over natural numbers. We assign the code 0 to the empty sequence $\emptyset$. The non-empty sequence $x_1\, x_2\, \ldots\, x_n$ is coded by the number $(x_1, x_2, \ldots, x_n, 0)$ (see Fig. 12.1). The reader will note that the assignment of codes is one to one, every finite sequence of natural numbers is coded by exactly one natural number, and vice versa, every natural number is the code of exactly one finite sequence of natural numbers. Codes of finite sequences are called *lists* in computer science and this is how we will be calling them from now on.



$x, 0$ $\quad$ $x, y, 0$ $\quad$ $x, y, z, 0$ $\quad$ $x_1, x_2, \ldots, x_n, 0$

Fig. 12.1. Lists

12.1.2 Case analysis on lists. We have the following principle of *list case analysis* (see 8.3.14(4)):

$$\vdash_{\mathrm{PA}}\ x = 0 \lor \exists v \exists w\, x = v, w.$$

12.1.3 List induction. Let T be a proper extension of PA containing the pairing function, $\phi[x]$ a formula of $\mathcal{L}_T$ with the indicated variable x free and with possibly additional parameters, and v and w new variables. The formula of *list induction on x for $\phi[x]$* is the following one:

$$\phi[0] \wedge \forall v \forall w(\phi[w] \rightarrow \phi[v,w]) \rightarrow \phi[x].$$

12.1.4 Theorem. *Every proper extension T of PA containing the pairing function proves the schema of list induction:*

$$T \vdash \phi[0] \wedge \forall v \forall w(\phi[w] \rightarrow \phi[v,w]) \rightarrow \phi[x].$$

Proof. The principle of list induction is reduced to mathematical induction as follows. Assume

$$\phi[0] \tag{1}$$

$$\forall v \forall w(\phi[w] \rightarrow \phi[v,w]) \tag{2}$$

and prove

$$\forall x(x < n \rightarrow \phi[x]) \tag{3}$$

by induction on n. In the base case, when $n = 0$, there is nothing to prove. In the inductive case take any x such that $x < n+1$. We consider two cases. If $x = 0$ then $\phi[0]$ follows from the assumption (1). If $x = v, w$ for some v and w then, since $w < x \leq n$, we have $\phi[w]$ from IH: (3) and we get $\phi[v,w]$ from (2). This ends the proof of (3) and we obtain $\phi[x]$ by substituting $x+1$ for n in (3). □

12.1.5 List recursion. Initial clauses for clausal definitions with list recursion are of a form

$f(\vec{y}, x, \vec{z}) = \alpha_1[\vec{y}, \vec{z}] \leftarrow x = 0$
$f(\vec{y}, x, \vec{z}) = \alpha_2[\dot{\lambda} \vec{y} w_1 \vec{z}.f(\vec{y}, w, \vec{z}); \vec{y}, \vec{z}, v, w] \leftarrow x = v, w.$

12.1.6 Length of lists. The list $x_1, x_2, \ldots, x_n, 0$ codes a finite sequence of natural numbers of length n and we say that the list has the *length* n. The length function has the following clausal definition by list recursion:

$L(0) = 0$
$L(v, w) = L(w) + 1.$

We have

$$\vdash_{\text{PA}} L(x) = 0 \leftrightarrow x = 0 \tag{1}$$

$$\vdash_{\text{PA}} L(x) \leq |x|_p \tag{2}$$

$$\vdash_{\text{PA}} \exists x\, L(x) = n. \tag{3}$$

Property (1) is proved by straightforward list case analysis. Property (2) is proved by list induction. The base case when $x = 0$ holds directly by definition and in the inductive case we have

$$L(v,w) \stackrel{\text{def}}{=} L(w) + 1 \stackrel{\text{IH}}{\leq} |w|_p + 1 \leq |v|_p + |w|_p + 1 = |v,w|_p.$$

Property (3) is proved by induction on n. In the base case when $n = 0$ it suffices to take $x := 0$. In the inductive case we have by IH that $n = L(y)$ for some y. Then $L(0,y) \stackrel{\text{def}}{=} L(y) + 1 = n+1$ and thus it suffices to take $x := 0, y$.

12.1.7 List indexing. The *list indexing* function $(x)_i$ yields the i-th element of the list x (counting from 0) or 0 if $i \geq L(x)$. The indexing function $(x)_i$ is defined by primitive recursion on i with substitution in parameter:

$$(v, w)_0 = v$$
$$(v, w)_{i+1} = (w)_i .$$

We have

$$\vdash_{\mathrm{PA}} (x)_i = H\,T^i(x). \tag{1}$$

Property (1) is proved by induction on i with the induction formula $\forall x(1)$. In the base case take any x and consider two cases. If $x = 0$ then

$$(0)_0 \stackrel{\text{def}}{=} 0 = H(0) = H\,T^0(0).$$

If $x = v, w$ then

$$(v, w)_0 \stackrel{\text{def}}{=} v = H(v, w) = H\,T^0(v, w).$$

In the inductive case take any x and consider two cases. If $x = 0$ then

$$(0)_{i+1} \stackrel{\text{def}}{=} 0 = H(0) \stackrel{8.3.18(6)}{=} H\,T^{i+1}(0).$$

If $x = v, w$ then

$$(v, w)_{i+1} \stackrel{\text{def}}{=} (w)_i \stackrel{\text{IH}}{=} H\,T^i(w) = H\,T^i\,T(v, w) \stackrel{8.3.18(7)}{=} H\,T^{i+1}(v, w).$$

12.1.8 Equality test for lists. We have

$$\vdash_{\mathrm{PA}} x = y \leftrightarrow L(x) = L(y) \land \forall i(i < L(x) \to (x)_i = (y)_i). \tag{1}$$

Property (1) is proved by list induction on x with the induction formula $\forall y(1)$. In the base case when $x = 0$ we consider two cases. If $y = 0$ then (1) holds trivially since $L(0) = 0$ by definition. If $y = v_2, w_2$ then (1) follows from $0 \neq v_2, w_2$ and $L(0) = 0 \neq L(w_2) + 1 = L(v_2, w_2)$. In the inductive case when $x = v_1, w_2$ we consider two cases. If $y = 0$ then we obtain (1) as before. If $y = v_2, w_2$ then we have

$$\begin{aligned}
&v_1, w_1 = v_2, w_2 \Leftrightarrow v_1 = v_2 \land w_1 = w_2 \stackrel{\text{IH}}{\Leftrightarrow} \\
&v_1 = v_2 \land L(w_1) = L(w_2) \land \forall i(i < L(w_1) \to (w_1)_i = (w_2)_i) \stackrel{(*)}{\Leftrightarrow} \\
&L(v_1, w_1) = L(v_2, w_2) \land \forall i(i < L(v_1, w_1) \to (v_1, w_1)_i = (v_2, w_2)_i).
\end{aligned}$$

The step marked by $(*)$ follows from the following properties

$$\begin{aligned}\vdash_{\mathrm{PA}}\ & v_1 = v_2 \land \forall i(i < L(w_1) \to (w_1)_i = (w_2)_i) \to \\ & \forall i(i \leq L(w_1) \to (v_1, w_1)_i = (v_2, w_2)_i)\end{aligned} \tag{2}$$

$$\vdash_{\mathrm{PA}} \forall i(i \le L(w_1) \to (v_1, w_1)_i = (v_2, w_2)_i) \to v_1 = v_2 \tag{3}$$

$$\begin{aligned}\vdash_{\mathrm{PA}} &\forall i(i \le L(w_1) \to (v_1, w_1)_i = (v_2, w_2)_i) \to \\ &\quad \forall i(i < L(w_1) \to (w_1)_i = (w_2)_i).\end{aligned} \tag{4}$$

Property (3) is proved as follows. Assume its antecedent, take any $i \le L(w_2)$, and consider two cases. If $i = 0$ then we have

$$(v_1, w_1)_0 = v_1 \overset{\text{hyp}}{=} v_2 = (v_2, w_2)_0.$$

If $i = j + 1$ for some j, then $j < L(w_2)$. We have

$$(v_1, w_1)_{j+1} = (w_1)_j \overset{\text{hyp}}{=} (w_2)_j = (v_2, w_2)_{j+1}.$$

We obtain the property (3) by instantiation of its antecedent by $i := 0$:

$$v_1 = (v_1, w_1)_0 \overset{\text{hyp}}{=} (v_2, w_2)_0 = v_2.$$

In the proof of the property (4) assume its antecedent, take any $i < L(w_2)$, instantiate the antecedent by $i := i + 1$, and we have

$$(w_1)_i = (v_1, w_1)_{i+1} \overset{\text{hyp}}{=} (v_2, w_2)_{i+1} = (w_2)_i.$$

12.1.9 Concatenation of lists. The *list concatenation* function $x \oplus y$ is defined by list recursion on x:

$$\begin{aligned}&0 \oplus y = y \\ &(v, w) \oplus y = v, w \oplus y.\end{aligned}$$

We have

$$\vdash_{\mathrm{PA}} x \oplus y = 0 \leftrightarrow x = 0 \land y = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} x \oplus 0 = x \tag{2}$$
$$\vdash_{\mathrm{PA}} x \oplus (y \oplus z) = (x \oplus y) \oplus z \tag{3}$$
$$\vdash_{\mathrm{PA}} x \oplus y = x \oplus z \to y = z \tag{4}$$
$$\vdash_{\mathrm{PA}} x \oplus z = y \oplus z \to x = y \tag{5}$$
$$\vdash_{\mathrm{PA}} x \oplus (a, 0) = y \oplus (b, 0) \to x = y \land a = b \tag{6}$$
$$\vdash_{\mathrm{PA}} |x \oplus y|_p = |x|_p + |y|_p \tag{7}$$
$$\vdash_{\mathrm{PA}} L(x \oplus y) = L(x) + L(y) \tag{8}$$
$$\vdash_{\mathrm{PA}} i < L(x) \to (x \oplus y)_i = (x)_i \tag{9}$$
$$\vdash_{\mathrm{PA}} i < L(y) \to (x \oplus y)_{L(x)+i} = (y)_i \tag{10}$$
$$\vdash_{\mathrm{PA}} x \ne 0 \leftrightarrow \exists y \exists a\, x = y \oplus (a, 0). \tag{11}$$

Property (1) is proved by a simple list case analysis on x. Properties (2) and (3) are proved by a straightforward list induction on x. Property (4) is proved by list induction on x. The base case is straightforward and in the inductive case we have

$$(v,w) \oplus y = (v,w) \oplus z \overset{\text{def}}{\Leftrightarrow} v,w \oplus y = v,w \oplus z \Leftrightarrow w \oplus y = w \oplus z \overset{\text{IH}}{\Rightarrow} y = z.$$

In the proof of (5) we need the following auxiliary property

$$\vdash_{\text{PA}} \forall x(x \oplus y = y \to x = 0) \tag{12}$$

which can be proved by list induction on y. Property (5) is proved by list induction on x with the induction formula $\forall y(5)$. In the base case when $x = 0$ take any y and consider two cases. If $y = 0$ then (5) follows from definition. The case when $y = v_2, w_2$ leads to contradiction with $0 \neq v_2, w_2$:

$$0 \oplus z = (v_2,w_2) \oplus z \overset{\text{def}}{\Leftrightarrow} z = (v_2,w_2) \oplus z \overset{(12)}{\Rightarrow} 0 = v_2, w_2.$$

In the inductive case when $x = v_1, w_1$ take any y and consider two cases. The case when $y = 0$ leads to contradiction by similar arguments as above. If $y = v_2, w_2$ then

$$\begin{aligned}
&(v_1,w_1) \oplus z = (v_2,w_2) \oplus z \overset{\text{def}}{\Leftrightarrow} v_1, w_1 \oplus z = v_2, w_2 \oplus z \Leftrightarrow \\
&v_1 = v_2 \land w_1 \oplus z = w_2 \oplus z \overset{\text{IH}}{\Rightarrow} v_1 = v_2 \land w_1 = w_2 \Leftrightarrow v_1, w_1 = v_2, w_2.
\end{aligned}$$

The remaining properties are left to the reader.

12.1.10 Alternative definition of list concatenation. The following property

$$\begin{aligned}
\vdash_{\text{PA}} x \oplus y = z \leftrightarrow L(z) = L(x) + L(y) \land \qquad& \\
\land \forall i\big(i < L(z) \to (i < L(x) \to (z)_i = (x)_i) \land& \qquad (1)\\
\land (i \geq L(x) \to (z)_i = (y)_{i \,\dot{-}\, L(x)})\big)&
\end{aligned}$$

can be used as an alternative (contextual) definition of list concatenation.

The property is proved by list induction on x with the induction formula $\forall z(1)$. The base case follows from 12.1.8(1). In the inductive case when $x = v_1, w_1$ take any z and consider two cases. If $z = 0$ then (1) trivially holds since both sides of the equivalence are false. If $z = v_2, w_2$ then we have

$$\begin{aligned}
&(v_1,w_1) \oplus y = v_2, w_2 \overset{\text{def}}{\Leftrightarrow} v_1, w_1 \oplus y = v_2, w_2 \Leftrightarrow v_1 = v_2 \land w_1 \oplus y = w_2 \overset{\text{IH}}{\Leftrightarrow} \\
&v_1 = v_2 \land L(w_2) = L(w_1) + L(y) \land \\
&\quad \forall i\big(i < L(w_2) \to (i < L(w_1) \to (w_2)_i = (w_1)_i) \land \\
&\qquad\qquad (i \geq L(w_1) \to (w_2)_i = (y)_{i \,\dot{-}\, L(w_1)})\big) \overset{(*)}{\Leftrightarrow} \\
&L(v_2,w_2) = L(v_1,w_1) + L(y) \land \\
&\quad \forall i\big(i < L(v_2,w_2) \to (i < L(v_1,w_1) \to (v_2,w_2)_i = (v_1,w_1)_i) \land \\
&\qquad\qquad (i \geq L(v_1,w_1) \to (v_2,w_2)_i = (y)_{i \,\dot{-}\, L(v_1,w_1)})\big).
\end{aligned}$$

The step marked by $(*)$ follows from the following properties

$$\begin{aligned}&\vdash_{\mathrm{PA}} v_1 = v_2 \land \forall i(i < L(w_1) \to (w_2)_i = (w_1)_i) \to \\ &\qquad \forall i(i \leq L(w_1) \to (v_2, w_2)_i = (v_1, w_1)_i)\end{aligned} \tag{2}$$

$$\begin{aligned}&\vdash_{\mathrm{PA}} v_1 = v_2 \land \forall i(L(w_1) \leq i < L(w_2) \to (w_2)_i = (y)_{i \dot{-} L(w_1)}) \to \\ &\qquad \forall i(L(w_1) < i \leq L(w_2) \to (v_2, w_2)_i = (y)_{i \dot{-} (L(w_1)+1)})\end{aligned} \tag{3}$$

$$\vdash_{\mathrm{PA}} \forall i(i \leq L(w_1) \to (v_2, w_2)_i = (v_1, w_1)_i) \to v_1 = v_2 \tag{4}$$

$$\begin{aligned}&\vdash_{\mathrm{PA}} \forall i(i \leq L(w_1) \to (v_2, w_2)_i = (v_1, w_1)_i) \to \\ &\qquad \forall i(i < L(w_1) \to (w_2)_i = (w_1)_i)\end{aligned} \tag{5}$$

$$\begin{aligned}&\vdash_{\mathrm{PA}} \forall i(L(w_1) < i \leq L(w_2) \to (v_2, w_2)_i = (y)_{i \dot{-} (L(w_1)+1)}) \to \\ &\qquad \forall i(L(w_1) \leq i < L(w_2) \to (w_2)_i = (y)_{i \dot{-} L(w_1)}).\end{aligned} \tag{6}$$

Property (2) is proved as follows. Assume the antecedent of the property, take any $i \leq L(w_1)$, and consider two cases. If $i = 0$ then we have

$$(v_2, w_2)_0 = v_2 \stackrel{\text{hyp}}{=} v_1 = (v_1, w_1)_0.$$

If $i = j + 1$ for some j then $j < L(w_1)$ and we have

$$(v_2, w_2)_{j+1} = (w_2)_j \stackrel{\text{hyp}}{=} (w_1)_j = (v_1, w_1)_{j+1}.$$

Property (3) is proved as follows. Assume the antecedent of the property, take any i such that $L(w_1) < i \leq L(w_2)$. Then $L(w_1) \leq i \dot{-} 1 < L(w_2)$ and we have

$$(v_2, w_2)_i = (w_2)_{i \dot{-} 1} \stackrel{\text{hyp}}{=} (y)_{i \dot{-} 1 \dot{-} L(w_1)} = (y)_{i \dot{-} (L(w_1)+1)}.$$

Property (4) is proved by instantiation of its antecedent by $i := 0$:

$$v_1 = (v_1, w_1)_0 \stackrel{\text{hyp}}{=} (v_2, w_2)_0 = v_2.$$

Property (5) is proved as follows. Assume the antecedent of the property, take any $i < L(w_1)$, and we have

$$(w_2)_i = (v_2, w_2)_{i+1} \stackrel{\text{hyp}}{=} (v_1, w_1)_{i+1} = (w_1)_i.$$

Property (6) is proved as follows. Assume the antecedent of the property, take any i such that $L(w_1) \leq i < L(w_2)$. Note that $L(w_1) < i + 1 \leq L(w_2)$. We have

$$(w_2)_i = (v_2, w_2)_{i+1} \stackrel{\text{hyp}}{=} (y)_{i+1 \dot{-} (L(w_1)+1)} = (y)_{i \dot{-} L(w_1)}.$$

12.1.11 List membership. The *list membership* predicate $x \,\varepsilon\, y$ is defined by list recursion on y:

$x \,\varepsilon\, v,w \leftarrow x = v$
$x \,\varepsilon\, v,w \leftarrow x \neq v \wedge x \,\varepsilon\, w.$

We have

$$\vdash_{\mathrm{PA}} x \not\varepsilon\, 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} x \,\varepsilon\, v,w \leftrightarrow x = v \vee x \,\varepsilon\, w \tag{2}$$
$$\vdash_{\mathrm{PA}} x \,\varepsilon\, y \oplus z \leftrightarrow x \,\varepsilon\, y \vee x \,\varepsilon\, z. \tag{3}$$

Properties (1) and (2) straighforward. Property (3) is proved by list induction on y. The base is trivial and in the inductive case we have

$$x \,\varepsilon\, (v,w) \oplus z \Leftrightarrow x \,\varepsilon\, v,w \oplus z \overset{(2)}{\Leftrightarrow} x = v \vee x \,\varepsilon\, w \oplus z \overset{\mathrm{IH}}{\Leftrightarrow}$$
$$x = v \vee x \,\varepsilon\, w \vee x \,\varepsilon\, z \overset{(2)}{\Leftrightarrow} x \,\varepsilon\, v,w \vee x \,\varepsilon\, z.$$

12.1.12 Alternative definition of list membership. The following is the basic property of list membership predicate

$$\vdash_{\mathrm{PA}} x \,\varepsilon\, y \leftrightarrow \exists i(i < L(y) \wedge (y)_i = x). \tag{1}$$

The property is proved by list induction on y. The base case is straightforward and in the inductive case we have

$$x \,\varepsilon\, v,w \overset{12.1.11(2)}{\Leftrightarrow} x = v \vee x \,\varepsilon\, w \overset{\mathrm{IH}}{\Leftrightarrow} x = v \vee \exists i(i < L(w) \wedge (w)_i = x) \overset{(*)}{\Leftrightarrow}$$
$$\exists i(i < L(v,w) \wedge (v,w)_i = x).$$

The step marked by $(*)$ follows from the following properties

$$\vdash_{\mathrm{PA}} x = v \rightarrow \exists i(i \leq L(w) \wedge (v,w)_i = x) \tag{2}$$
$$\vdash_{\mathrm{PA}} \exists i(i < L(w) \wedge (w)_i = x) \rightarrow \exists i(i \leq L(w) \wedge (v,w)_i = x) \tag{3}$$
$$\vdash_{\mathrm{PA}} \exists i(i \leq L(w) \wedge (v,w)_i = x) \rightarrow x = v \vee \exists i(i < L(w) \wedge (w)_i = x). \tag{4}$$

Property (2) follows from

$$x = v \Rightarrow 0 \leq L(w) \wedge (v,w)_0 = v = x.$$

Property (3) follows from

$$i < L(w) \wedge (w)_i = x \Rightarrow i + 1 \leq L(w) \wedge (v,w)_{i+1} = (w)_i = x.$$

Property (4) is proved as follows. Suppose that we have $i \leq L(w)$ and $(v,w)_i = x$ for some i. We consider two cases. If $i = 0$ then

$$x \overset{\mathrm{hyp}}{=} (v,w)_0 = v \Rightarrow x = v.$$

If $i = j + 1$ then

$$j < L(w) \wedge x \overset{\mathrm{hyp}}{=} (v,w)_{j+1} = (w)_j \Rightarrow \exists i(i < L(w) \wedge (w)_i = x).$$

12.1.13 List reversal. The function *Rev* reversing lists has the following clausal definition by list recursion:

$$Rev(0) = 0$$
$$Rev(v, w) = Rev(w) \oplus (v, 0).$$

We have

$$\vdash_{\mathrm{PA}} Rev(x) = 0 \leftrightarrow x = 0 \qquad (1)$$
$$\vdash_{\mathrm{PA}} Rev(x \oplus y) = Rev(y) \oplus Rev(x) \qquad (2)$$
$$\vdash_{\mathrm{PA}} Rev\, Rev(x) = x \qquad (3)$$
$$\vdash_{\mathrm{PA}} Rev(x) = Rev(y) \rightarrow x = y \qquad (4)$$
$$\vdash_{\mathrm{PA}} \exists y\, Rev(y) = x \qquad (5)$$
$$\vdash_{\mathrm{PA}} x \;\varepsilon\; Rev(y) \leftrightarrow x \;\varepsilon\; y \qquad (6)$$
$$\vdash_{\mathrm{PA}} |Rev(x)|_p = |x|_p \qquad (7)$$
$$\vdash_{\mathrm{PA}} L\, Rev(x) = L(x). \qquad (8)$$

Property (1) is proved by a simple list case analysis on x. Property (2) is proved by a straightforward list induction on x. Property (3) is proved by list induction on x. The base case is straightforward and in the inductive case we have

$$Rev\, Rev((v, w) \oplus y) = Rev\, Rev(v, w \oplus y) \stackrel{\text{def}}{=} Rev(Rev(w \oplus y) \oplus (v, 0)) \stackrel{(2)}{=}$$
$$= Rev(v, 0) \oplus Rev\, Rev(w \oplus y) \stackrel{2\times\text{def;IH}}{=} 0 \oplus (v, 0) \oplus w \oplus y = (v, w) \oplus y.$$

Property (4) is proved as follows

$$Rev(x) = Rev(y) \Rightarrow Rev\, Rev(x) = Rev\, Rev(y) \stackrel{(3)}{\Leftrightarrow} x = y.$$

Property (5) follows from (3). The remaining properties are left to the reader.

12.1.14 Alternative definition of list reversal. The following property

$$\vdash_{\mathrm{PA}} Rev(x) = y \leftrightarrow L(y) = L(x) \land \forall i(i < L(y) \rightarrow (y)_i = (x)_{L(y) \dot{-} (i+1)}) \qquad (1)$$

can be used as an alternative (contextual) definition of list reversal.

The property is proved by list induction on x with the induction formula $\forall y(1)$. The base case is straightforward. In the inductive case when $x = v_1, w_1$ take any y and consider two cases. If $y = 0$ then (1) trivially holds since both sides of the equivalence are false. If $y \neq 0$ then $y = w_2 \oplus (v_2, 0)$ for some v_2 and w_2 by 12.1.9(11). We have

$$Rev(v_1, w_1) = w_2 \oplus (v_2, 0) \stackrel{\text{def}}{\Leftrightarrow} Rev(w_1) \oplus (v_1, 0) = w_2 \oplus (v_2, 0) \stackrel{12.1.9(6)}{\Leftrightarrow}$$
$$v_1 = v_2 \land Rev(w_1) = w_2 \stackrel{\text{IH}}{\Leftrightarrow}$$
$$v_1 = v_2 \land L(w_2) = L(w_1) \land \forall i(i < L(w_2) \rightarrow (w_2)_i = (w_1)_{L(w_2) \dot{-} (i+1)}) \stackrel{(*)}{\Leftrightarrow}$$

$$L(w_2 \oplus (v_2,0)) = L(v_1,w_1) \land$$
$$\forall i(i < L(w_2 \oplus (v_2,0)) \rightarrow (w_2 \oplus (v_2,0))_i = (v_1,w_1)_{L(w_2 \oplus (v_2,0)) \dot{-} (i+1)}).$$

The step marked by $(*)$ follows from the following properties

$$\vdash_{\mathrm{PA}} L(w_2 \oplus (v_2,0)) = L(w_2) + 1 \tag{2}$$

$$\vdash_{\mathrm{PA}} v_1 = v_2 \land \forall i(i < L(w_2) \rightarrow (w_2)_i = (w_1)_{L(w_2) \dot{-} (i+1)}) \rightarrow \forall i(i \leq L(w_2) \rightarrow (w_2 \oplus (v_2,0))_i = (v_1,w_1)_{L(w_2) \dot{-} i}) \tag{3}$$

$$\vdash_{\mathrm{PA}} \forall i(i \leq L(w_2) \rightarrow (w_2 \oplus (v_2,0))_i = (v_1,w_1)_{L(w_2) \dot{-} i}) \rightarrow v_1 = v_2 \tag{4}$$

$$\vdash_{\mathrm{PA}} \forall i(i \leq L(w_2) \rightarrow (w_2 \oplus (v_2,0))_i = (v_1,w_1)_{L(w_2) \dot{-} i}) \rightarrow \forall i(i < L(w_2) \rightarrow (w_2)_i = (w_1)_{L(w_2) \dot{-} (i+1)}). \tag{5}$$

Property (2) is a consequence of 12.1.9(8). Property (3) is proved as follows. Assume the antecedent of the property, take any $i \leq L(w_2)$, and consider two cases. If $i < L(w_2)$ then we have

$$(w_2 \oplus (v_2,0))_i \overset{12.1.9(9)}{=} (w_2)_i \overset{\mathrm{hyp}}{=} (w_1)_{L(w_2) \dot{-} (i+1)} = (v_1,w_1)_{L(w_2) \dot{-} i}.$$

If $i = L(w_2)$ then we have

$$(w_2 \oplus (v_2,0))_{L(w_2)} \overset{12.1.9(10)}{=} (v_2,0)_0 = v_2 \overset{\mathrm{hyp}}{=} v_1 = (w_1)_{L(w_2) \dot{-} L(w_2)}.$$

Property (4) is obtained by instantiating its antecedent by $i := L(w_2)$:

$$v_1 = (v_1,w_1)_{L(w_2) \dot{-} L(w_2)} \overset{\mathrm{hyp}}{=} (w_2 \oplus (v_2,0))_{L(w_2)} \overset{12.1.9(10)}{=} (v_2,0)_0 = v_2.$$

Property (5) is proved as follows. Assume the antecedent of the property, take any $i < L(w_2)$, and we have

$$(w_2)_i \overset{12.1.9(9)}{=} (w_2 \oplus (v_2,0))_i \overset{\mathrm{hyp}}{=} (v_1,w_1)_{L(w_2) \dot{-} i} = (w_1)_{L(w_2) \dot{-} (i+1)}.$$

12.1.15 Fast list reversal. The function *Rev* repeatedly invokes list concatenation to append an element to the end of a list. Namely, it takes $O(L(x)^2)$ operations to compute $Rev(x)$. This is clearly wasteful and we can ask the question wether $Rev(x)$ cannot be computed in $O(L(x))$ steps. By accumulating the reversed list into an *accumulator* a we can perform the reversal of x in $O(L(x))$ operations with the help of an accumulator function. The binary accumulator function $f(x,a)$ is defined by list recursion on x with substitution in parameter:

$$f(0,a) = a$$
$$f((v,w),a) = f(w,v,a).$$

We have

$$\vdash_{\mathrm{PA}} Rev(x) = f(x,0) \tag{1}$$

as a simple consequence of a more general property

$$\vdash_{\mathrm{PA}} \forall a\, f(x,a) = Rev(x) \oplus a. \tag{2}$$

Property (2) is proved by list induction. The base case is straightforward and in the inductive case we have

$$\begin{aligned} f((v,w),a) &\stackrel{\text{def}}{=} f(w,v,a) \stackrel{\text{IH}}{=} Rev(w) \oplus (v,a) = \\ &= Rev(w) \oplus (v,0) \oplus a \stackrel{\text{def}}{=} Rev(v,w) \oplus a. \end{aligned}$$

12.2 Operations on Lists

12.2.1 List modification. The *list modification* function $x[i := a]$ takes a list x and yields a new list with i-th element replaced by a. The function satisfies

$$\vdash_{\mathrm{PA}} i < L(x) \to L(x[i := a]) = L(x) \tag{1}$$
$$\vdash_{\mathrm{PA}} i < L(x) \to (x[i := a])_i = a \tag{2}$$
$$\vdash_{\mathrm{PA}} i < L(x) \land j < L(x) \land j \neq i \to (x[i := a])_j = (x)_j \tag{3}$$

and it is defined by primitive recursion on i with substitution in parameter x as a primitive recursive function:

$$\begin{aligned} &(v,w)[0 := a] = a, w \\ &(v,w)[i+1 := a] = v, w[i := a]. \end{aligned}$$

Property $\forall x(1)$ is proved by induction on i. In the base case take any x and assume $0 < L(x)$. Then $x = v, w$ for some v and w and we have

$$L((v,w)[0 := a]) \stackrel{\text{def}}{=} L(a,w) = L(w) + 1 = L(v,w).$$

In the induction case take any x and assume $i + 1 < L(x)$. Then $x = v, w$ for some v and w, and thus $i < L(w)$. We have

$$\begin{aligned} L((v,w)[i+1 := a]) &\stackrel{\text{def}}{=} L(v, w[i := a]) = L(w[i := a]) + 1 \stackrel{\text{IH}}{=} \\ &= L(w) + 1 = L(v,w). \end{aligned}$$

Property $\forall x(2)$ is proved by induction on i. In the base case take any x and assume $0 < L(x)$. Then $x = v, w$ for some v and w and we have

$$((v,w)[0 := a])_0 \stackrel{\text{def}}{=} (a,w)_0 = a.$$

In the inductive case take any x and assume $i+1 < L(x)$. Then $x = v, w$ for some v and w, and thus $i < L(w)$. We have

$$((v,w)[i+1 := a])_{i+1} \stackrel{\text{def}}{=} (v, w[i := a])_{i+1} = (w[i := a])_i \stackrel{\text{IH}}{=} a.$$

Property $\forall x \forall j(3)$ is proved by induction on i. In the base case take any x and j, and assume $0 < L(x)$, $j \neq 0$, and $j < L(x)$. Then $x = v, w$ for some v and w, and $j = k+1$ for some k. We have

$$((v,w)[0 := a])_{k+1} \stackrel{\text{def}}{=} (a,w)_{k+1} = (w)_k = (v,w)_{k+1}.$$

In the inductive case take any x and j, and assume $i+1 < L(x)$, $j \neq i$, and $j < L(x)$. Then $x = v, w$ for some v and w, and thus $i < L(w)$. We consider two cases. If $j = 0$ then we have

$$((v,w)[i+1 := a])_0 \stackrel{\text{def}}{=} (v, w[i := a])_0 = v = (v,w)_0.$$

If $j = k+1$ for some k then $k \neq i$ and $k < L(w)$. We have

$$\begin{aligned} ((v,w)[i+1 := a])_{k+1} &\stackrel{\text{def}}{=} (v, w[i := a])_{k+1} = (w[i := a])_k \stackrel{\text{IH}}{=} \\ &= (w)_k = (v,w)_{k+1} \end{aligned}$$

12.2.2 Map. Let $f(x)$ be arbitrary but fixed function. The function $Map(x)$ applies f to each element of a list. The function satisfies

$$\vdash_{\text{PA}} L\, Map(x) = L(x) \tag{1}$$
$$\vdash_{\text{PA}} i < L(x) \rightarrow (Map(x))_i = f((x)_i) \tag{2}$$

and it is defined by list recursion as a primitive recursive function in f:

$$\begin{aligned} &Map(0) = 0 \\ &Map(v,w) = f(v), Map(w). \end{aligned}$$

Property (1) is proved by a straightforward list induction. Property $\forall i(2)$ is proved by list induction on x. In the base case there is nothing to prove. In the inductive case when $x = v, w$ take any i such that $i < L(v,w) = L(w)+1$ and consider two cases. If $i = 0$ then we have

$$(Map(v,w))_0 \stackrel{\text{def}}{=} (f(v), Map(w))_0 = f(v) = f((v,w)_0).$$

If $i = j+1$ for some j then $j < L(w)$ and we have

$$\begin{aligned} (Map(v,w))_{j+1} &\stackrel{\text{def}}{=} (f(v), Map(w))_{j+1} = (Map(w))_j \stackrel{\text{IH}}{=} \\ &= f((w)_j) = f((v,w)_{j+1}). \end{aligned}$$

12.2.3 Zip and unzip. The function $Zip(x,y)$ takes two lists of the same length and yields a list of pairs of the corresponding elements. The function satisfies

$$\vdash_{\mathrm{PA}} L(x) = L(y) \rightarrow L\,Zip(x,y) = L(x) \tag{1}$$

$$\vdash_{\mathrm{PA}} L(x) = L(y) \wedge i < L(x) \rightarrow (Zip(x,y))_i = (x)_i,(y)_i \tag{2}$$

and it is defined by list recursion with substitution in parameter as a primitive recursive function:

$$Zip(0,0) = 0$$
$$Zip((v_1,w_1),v_2,w_2) = (v_1,v_2), Zip(w_1,w_2).$$

The function $Unzip(z)$ - the inverse of Zip, takes a list of pairs to a pair of lists. The function satisfies

$$\vdash_{\mathrm{PA}} L(x) = L(y) \rightarrow Unzip\ Zip(x,y) = x,y \tag{3}$$

and it is defined by list recursion as a primitive recursive function:

$$Unzip(0) = 0,0$$
$$Unzip((v_1,v_2),w) = (v_1,w_1),v_2,w_2 \leftarrow Unzip(w) = w_1,w_2.$$

Property $\forall y(1)$ is proved by list induction on x. In the base case take any y and assume $L(0) = L(y)$. Then $y = 0$ and we are done since $L\,Zip(0,0) = L(0)$ from the definition. In the inductive case when $x = v_1,w_1$ take any y and assume $L(v_1,w_1) = L(w_1)+1 = L(y)$. Then $y = v_2,w_2$ for some v_2 and w_2, and thus $L(w_1) = L(w_2)$. We have

$$L\,Zip((v_1,w_1),v_2,w_2) \stackrel{\mathrm{def}}{=} L((v_1,v_2),Zip(w_1,w_2)) = L\,Zip(w_1,w_2)+1 \stackrel{\mathrm{IH}}{=}$$
$$= L(w_1)+1 = L(v_1,w_1).$$

Property $\forall x \forall y(2)$ is proved by induction on i. In the base case take any x and y such that $0 < L(x) = L(y)$. Then $x = v_1,w_1$ and $y = v_2,w_2$ for some v_i and w_i. Clearly $L(w_1) = L(w_2)$ and thus we obtain

$$(Zip((v_1,w_1),v_2,w_2))_0 \stackrel{\mathrm{def}}{=} ((v_1,v_2),Zip(w_1,w_2))_0 =$$
$$= v_1,v_2 = (v_1,w_1)_0,(v_2,w_2)_0.$$

In the inductive case take any x and y such that $i+1 < L(x) = L(y)$. Then $x = v_1,w_1$ and $y = v_2,w_2$ for some v_i and w_i. Clearly $i < L(w_1) = L(w_2)$ and thus we obtain

$$(Zip((v_1,w_1),v_2,w_2))_{i+1} \stackrel{\mathrm{def}}{=} ((v_1,v_2),Zip(w_1,w_2))_{i+1} = (Zip(w_1,w_2))_i \stackrel{\mathrm{IH}}{=}$$
$$= (w_1)_i,(w_2)_i = (v_1,w_1)_{i+1},(v_2,w_2)_{i+1}.$$

Property $\forall y(3)$ is proved by list induction on x and is left to the reader.

12.2.4 Interval. The function $[m\mathinner{..}n]$ yields the list of numbers from m to n. The function satisfies

$$\vdash_{\text{PA}} L\,[m\mathinner{..}n] = n + 1 \dot{-} m \tag{1}$$
$$\vdash_{\text{PA}} i < n + 1 \dot{-} m \to ([m\mathinner{..}n])_i = m + i \tag{2}$$

and it is defined by course of values recursion with measure $n + 1 \dot{-} m$ as a primitive recursive function:

$[m\mathinner{..}n] = 0 \leftarrow m > n$
$[m\mathinner{..}n] = m, [m+1\mathinner{..}n] \leftarrow m \leq n.$

Property (1) is proved by measure induction with measure $n + 1 \dot{-} m$. Take any m, n and consider two cases. If $m > n$ then we have

$$L\,[m\mathinner{..}n] \overset{\text{def}}{=} L(0) = 0 = n + 1 \dot{-} m.$$

If $m \leq n$ then we have

$$L\,[m\mathinner{..}n] \overset{\text{def}}{=} L(m, [m+1\mathinner{..}n]) = L\,[m+1\mathinner{..}n] + 1 \overset{\text{IH}}{=}$$
$$= n + 1 \dot{-} (m+1) + 1 = n + 1 \dot{-} m.$$

Property $\forall i(2)$ is proved by measure induction with measure $n+1 \dot{-} m$. Take any m, n, i such that $i < n + 1 \dot{-} m$ and consider two cases. If $m > n$ then there is nothing to prove. If $m \leq n$ then consider two cases. If $i = 0$ then we have

$$([m\mathinner{..}n])_0 \overset{\text{def}}{=} (m, [m+1\mathinner{..}n])_0 = m = m + 0.$$

If $i = j + 1$ for some j then $j < n + 1 \dot{-} m \dot{-} 1 = n + 1 \dot{-} (m + 1)$. We have

$$([m\mathinner{..}n])_{j+1} \overset{\text{def}}{=} (m, [m+1\mathinner{..}n])_{j+1} = ([m+1\mathinner{..}n])_j \overset{\text{IH}}{=}$$
$$= (m + 1) + j = m + (j + 1).$$

12.2.5 Elements with even and odd indices. The function $\mathit{Ieven}(x)$ returns the list of all elements occurring in a list at even indices. The function satisfies

$$\vdash_{\text{PA}} L\,\mathit{Ieven}(x) = (L(x) + 1) \div 2 \tag{1}$$
$$\vdash_{\text{PA}} 2 \cdot i < L(x) \to (\mathit{Ieven}(x))_i = (x)_{2\,\cdot\,i} \tag{2}$$

and it is defined by by course of values recursion with measure $L(x)$ as a primitive recursive function:

$\mathit{Ieven}(0) = 0$
$\mathit{Ieven}(u, 0) = u, 0$
$\mathit{Ieven}(u, v, w) = u, \mathit{Ieven}(w).$

The function $\mathit{Iodd}(x)$ returns the list of all elements occurring in a list at odd indices. The function satisfies

$$\vdash_{\mathrm{PA}} L\,\mathit{Iodd}(x) = L(x) \div 2 \tag{3}$$
$$\vdash_{\mathrm{PA}} 2 \cdot i + 1 < L(x) \to (\mathit{Iodd}(x))_i = (x)_{2\,\cdot\,i+1} \tag{4}$$

and it is defined by course of values recursion with measure $L(x)$ as a primitive recursive function:

$$\mathit{Iodd}(0) = 0$$
$$\mathit{Iodd}(u, 0) = 0$$
$$\mathit{Iodd}(u, v, w) = v, \mathit{Iodd}(w).$$

We prove (1) by measure induction with measure $L(x)$. Take any x and consider three cases. If $x = 0$ then we have

$$L\,\mathit{Ieven}(0) \stackrel{\text{def}}{=} L(0) = 0 = (0 + 1) \div 2 = (L(0) + 1) \div 2.$$

If $x = u, 0$ for some u then we have

$$L\,\mathit{Ieven}(u, 0) \stackrel{\text{def}}{=} L(u, 0) = 1 = (1 + 1) \div 2 = (L(u, 0) + 1) \div 2.$$

If $x = u, v, w$ for some u, v, and w, then we have

$$\begin{aligned} L\,\mathit{Ieven}(u, v, w) &\stackrel{\text{def}}{=} L(u, \mathit{Ieven}(w)) = L\,\mathit{Ieven}(w) + 1 \stackrel{\text{IH}}{=} (L(w) + 1) \div 2 + 1 = \\ &= (L(w) + 3) \div 2 = (L(u, v, w) + 1) \div 2. \end{aligned}$$

We prove $\forall i(2)$ by measure induction with measure $L(x)$. Take any x and i such that $2 \cdot i < L(x)$ and consider three cases. If $x = 0$ then there is nothing to prove since $L(0) = 0$. If $x = u, 0$ for some u then $2 \cdot i < L(u, 0) = 1$ yields $i = 0$. We have

$$(\mathit{Ieven}(u, 0))_0 \stackrel{\text{def}}{=} (u, 0)_0 = (u, 0)_{2\,\cdot\,0}.$$

If $x = u, v, w$ for some u, v, and w, then $2 \cdot i < L(u, v, w) = L(w) + 2$. We consider two subcases. If $i = 0$ then we have

$$(\mathit{Ieven}(u, v, w))_0 \stackrel{\text{def}}{=} (u, \mathit{Ieven}(w))_0 = u = (u, v, w)_0 = (u, v, w)_{2\,\cdot\,0}.$$

If $i = j + 1$ for some j then $2 \cdot j < L(w)$ and we have

$$\begin{aligned} (\mathit{Ieven}(u, v, w))_{j+1} &\stackrel{\text{def}}{=} (u, \mathit{Ieven}(w))_{j+1} = (\mathit{Ieven}(w))_j \stackrel{\text{IH}}{=} \\ &= (w)_{2\,\cdot\,j} = (u, v, w)_{2\,\cdot\,j+2} = (u, v, w)_{2\,\cdot(j+1)}. \end{aligned}$$

Properties (3) and (4) are proved similarly.

12.2.6 Combining two lists. Let x and y be lists such that the length of x is at most one more than the length of y. The function $Combine(x,y)$ combines the lists x and y into one list. The function satisfies

$$\vdash_{\mathrm{PA}} L(x) = L(y) \lor L(x) = L(y)+1 \to L\ Combine(x,y) = L(x) + L(y) \quad (1)$$

$$\vdash_{\mathrm{PA}} (L(x) = L(y) \lor L(x) = L(y)+1) \land 2\cdot i < L(x)+L(y) \to (Combine(x,y))_{2\cdot i} = (x)_i \quad (2)$$

$$\vdash_{\mathrm{PA}} (L(x) = L(y) \lor L(x) = L(y)+1) \land 2\cdot i+1 < L(x)+L(y) \to (Combine(x,y))_{2\cdot i+1} = (y)_i \quad (3)$$

and it is defined by list recursion with substitution in parameter as a primitive recursive function:

$$Combine(0,0) = 0$$
$$Combine((v_1,w_1),0) = v_1,w_1$$
$$Combine((v_1,w_1),v_2,w_2) = v_1,v_2,Combine(w_1,w_2).$$

Property $\forall y(1)$ is proved list induction on x. In the base when $x=0$ take any y such that $L(0) = L(y) \lor L(0) = L(y)+1$. Then $y=0$ and we have

$$L\ Combine(0,0) \stackrel{\mathrm{def}}{=} L(0) = 0 = L(0) + L(0).$$

In the inductive case when $x = v_1,w_1$ take any y such that $L(v_1,w_1) = L(y) \lor L(v_1,w_1) = L(y)+1$ and consider two cases. If $y=0$ then we have

$$L\ Combine((v_1,w_1),0) \stackrel{\mathrm{def}}{=} L(v_1,w_1) = L(v_1,w_1) + L(0).$$

If $y = v_2,w_2$ for some v_2 and w_2 then $L(w_1) = L(w_2) \lor L(w_1) = L(w_2)+1$ and we have

$$L\ Combine((v_1,w_1),v_2,w_2) \stackrel{\mathrm{def}}{=} L(v_1,v_2,Combine(w_1,w_2)) =$$
$$= L\ Combine(w_1,w_2) + 2 \stackrel{\mathrm{IH}}{=} L(w_1) + L(w_2) + 2 = L(v_1,w_1) + L(v_2,w_2).$$

Property $\forall y \forall i(2)$ is proved list induction on x. In the base case when $x=0$ there is nothing to prove. In the inductive case when $x = v_1,w_1$ take any y,i such that $L(v_1,w_1) = L(y) \lor L(v_1,w_1) = L(y)+1$ and $2\cdot i < L(v_1,w_1)+L(y)$. We consider two cases. If $y=0$ then $i=0$ and we have

$$(Combine((v_1,w_1),0))_{2\cdot 0} \stackrel{\mathrm{def}}{=} (v_1,w_1)_0.$$

If $y = v_2,w_2$ for some v_2 and w_2 then we consider two subcases. If $i=0$ then we have

$$(Combine((v_1,w_1),v_2,w_2))_{2\cdot 0} \stackrel{\mathrm{def}}{=} (v_1,w_1,Combine(w_1,w_2))_0 =$$
$$= v_1 = (v_1,w_1)_0.$$

If $i = j + 1$ for some j then $2 \cdot j < L(w_1) + L(w_2)$ and we have

$$(\mathit{Combine}((v_1, w_1), v_2, w_2))_{2 \cdot (j+1)} \stackrel{\text{def}}{=} (v_1, w_1, \mathit{Combine}(w_1, w_2))_{2 \cdot j+2} =$$
$$= (\mathit{Combine}(w_1, w_2))_j \stackrel{\text{IH}}{=} (w_1)_j = (v_1, w_1)_j.$$

Property (3) is proved similarly.

12.2.7 Take and drop. The function $\mathit{Take}(n, x)$ yields the initial segment of a list x of length n if $n \leq L(x)$. The function satisfies

$$\vdash_{\text{PA}} n \leq L(x) \to L\ \mathit{Take}(n, x) = n \tag{1}$$
$$\vdash_{\text{PA}} n \leq L(x) \to \exists y\, x = \mathit{Take}(n, x) \oplus y \tag{2}$$

and it is defined by primitive recursion on n with substitution in parameter as a primitive recursive function:

$\mathit{Take}(0, x) = 0$
$\mathit{Take}(n + 1, v, w) = v, \mathit{Take}(n, w).$

The function $\mathit{Drop}(n, x)$ removes the initial segment of a list x of length n if $n \leq L(x)$. The function satisfies

$$\vdash_{\text{PA}} n \leq L(x) \to L\ \mathit{Drop}(n, x) = L(x) \dot{-} n \tag{3}$$
$$\vdash_{\text{PA}} n \leq L(x) \to \exists y\, x = y \oplus \mathit{Drop}(n, x) \tag{4}$$

and it is defined by primitive recursion on n with substitution in parameter as a primitive recursive function:

$\mathit{Drop}(0, x) = x$
$\mathit{Drop}(n + 1, v, w) = \mathit{Drop}(n, w).$

Property $\forall x(1)$ is proved by induction on n. In the base case take any x and we have

$$L\ \mathit{Take}(0, x) \stackrel{\text{def}}{=} L(0) = 0.$$

In the inductive case take any x such that $n + 1 \leq L(x)$. Then $x = v, w$ for some v and w, and $n \leq L(w)$. We have

$$L\ \mathit{Take}(n + 1, v, w) \stackrel{\text{def}}{=} L(v, \mathit{Take}(n, w)) = L\ \mathit{Take}(n, w) + 1 \stackrel{\text{IH}}{=} n + 1.$$

Property $\forall x(2)$ is proved by induction on n. In the base case it suffices to take $y := x$ in (2) since $\mathit{Take}(0, x) \oplus x \stackrel{\text{def}}{=} 0 \oplus x = x$. In the inductive case assume $n + 1 \leq L(x)$. Then $x = v, w$ for some v and w. Since $n \leq L(w)$ we get from IH that $w = \mathit{Take}(n, w) \oplus y$ for some y. We have

$$v, w = v, \mathit{Take}(n, w) \oplus y = (v, \mathit{Take}(n, w)) \oplus y \stackrel{\text{def}}{=} \mathit{Take}(n + 1, v, w) \oplus y.$$

Properties (3) and (4) are left to the reader.

12.2.8 Minimum and maximum of lists. The function $\mathit{Minl}(x)$ yields the minimum of a non-empty list. The function satisfies

$$\vdash_{\mathrm{PA}} x \neq 0 \to \mathit{Minl}(x) \mathrel{\varepsilon} x \tag{1}$$

$$\vdash_{\mathrm{PA}} x \neq 0 \land a \mathrel{\varepsilon} x \to \mathit{Minl}(x) \leq a \tag{2}$$

and it is defined by list recursion as a primitive recursive function:

$$\begin{aligned}
&\mathit{Minl}(v, w) = v \leftarrow w = 0\\
&\mathit{Minl}(v, w) = \min(v, \mathit{Minl}(w)) \leftarrow w \neq 0.
\end{aligned}$$

The function $\mathit{Maxl}(x)$ yields the maximum of a non-empty list. The function satisfies

$$\vdash_{\mathrm{PA}} x \neq 0 \to \mathit{Maxl}(x) \mathrel{\varepsilon} x \tag{3}$$

$$\vdash_{\mathrm{PA}} x \neq 0 \land a \mathrel{\varepsilon} x \to a \leq \mathit{Maxl}(x) \tag{4}$$

and it is defined by list recursion as a primitive recursive function:

$$\begin{aligned}
&\mathit{Maxl}(v, w) = v \leftarrow w = 0\\
&\mathit{Maxl}(v, w) = \max(v, \mathit{Maxl}(w)) \leftarrow w \neq 0.
\end{aligned}$$

Property (1) is proved by list induction. In the base case there is nothing to prove. The inductive case when $x = v, w$ is a consequence of the following simple case analysis:

$$\begin{aligned}
&w = 0 \Rightarrow \mathit{Minl}(v, 0) \stackrel{\text{def}}{=} v \mathrel{\varepsilon} v, 0\\
&w \neq 0 \land v \leq \mathit{Minl}(w) \Rightarrow \mathit{Minl}(v, w) \stackrel{\text{def}}{=} v \mathrel{\varepsilon} v, w\\
&w \neq 0 \land v > \mathit{Minl}(w) \Rightarrow \mathit{Minl}(v, w) \stackrel{\text{def}}{=} \mathit{Minl}(w) \stackrel{\text{IH}}{\varepsilon} w \Rightarrow \mathit{Minl}(v, w) \mathrel{\varepsilon} v, w.
\end{aligned}$$

Property (2) is proved by list induction. In the base case there is nothing to prove. In the inductive case when $x = v, w$ assume $a \mathrel{\varepsilon} v, w$ and consider two cases. If $w = 0$ then $a = v$ and thus $\mathit{Minl}(v, 0) \stackrel{\text{def}}{=} v \leq a$. If $w \neq 0$ then $\mathit{Minl}(v, w) \leq a$ is a consequence of the following simple case analysis:

$$\begin{aligned}
&v \leq \mathit{Minl}(w) \land a = v \Rightarrow \mathit{Minl}(v, w) \stackrel{\text{def}}{=} v = a\\
&v \leq \mathit{Minl}(w) \land a \mathrel{\varepsilon} w \Rightarrow \mathit{Minl}(v, w) \stackrel{\text{def}}{=} v \leq \mathit{Minl}(w) \stackrel{\text{IH}}{\leq} a\\
&v > \mathit{Minl}(w) \land a = v \Rightarrow \mathit{Minl}(v, w) \stackrel{\text{def}}{=} \mathit{Minl}(w) < v = a\\
&v > \mathit{Minl}(w) \land a \mathrel{\varepsilon} w \Rightarrow \mathit{Minl}(v, w) \stackrel{\text{def}}{=} \mathit{Minl}(w) \stackrel{\text{IH}}{\leq} a.
\end{aligned}$$

Properties (3) and (4) are proved similarly.

12.2.9 Deleting elements from lists. The function $\mathit{Delall}(a,x)$ removes all occurrences of a in the list x. The function satisfies

$$\vdash_{\mathrm{PA}} b \,\varepsilon\, \mathit{Delall}(a,x) \leftrightarrow b \,\varepsilon\, x \wedge b \neq a \tag{1}$$

and it is defined by list recursion on x as a primitive recursive function:

$$\begin{aligned}
&\mathit{Delall}(a,0) = 0\\
&\mathit{Delall}(a,v,w) = \mathit{Delall}(a,w) \leftarrow a = v\\
&\mathit{Delall}(a,v,w) = v, \mathit{Delall}(a,w) \leftarrow a \neq v.
\end{aligned}$$

Property (1) is proved by list induction on x. The base case when $x = 0$ is straightforward since $\mathit{Delall}(a,0) \stackrel{\text{def}}{=} 0$. In the inductive case when $x = v,w$ consider two case. If $a = v$ then we have

$$\begin{aligned}
&b \,\varepsilon\, \mathit{Delall}(a,v,w) \stackrel{\text{def}}{\Leftrightarrow} b \,\varepsilon\, \mathit{Delall}(a,w) \stackrel{\text{IH}}{\Leftrightarrow} b \,\varepsilon\, w \wedge b \neq a \Leftrightarrow\\
&(b = v \vee b \,\varepsilon\, w) \wedge b \neq a \stackrel{12.1.11(2)}{\Leftrightarrow} b \,\varepsilon\, v,w \wedge b \neq a.
\end{aligned}$$

If $a \neq v$ then we have

$$\begin{aligned}
&b \,\varepsilon\, \mathit{Delall}(a,v,w) \stackrel{\text{def}}{\Leftrightarrow} b \,\varepsilon\, v, \mathit{Delall}(a,w) \stackrel{12.1.11(2)}{\Leftrightarrow} b = v \vee b \,\varepsilon\, \mathit{Delall}(a,w) \stackrel{\text{IH}}{\Leftrightarrow}\\
&b = v \vee b \,\varepsilon\, w \wedge b \neq a \Leftrightarrow (b = v \vee b \,\varepsilon\, w) \wedge b \neq a \stackrel{12.1.11(2)}{\Leftrightarrow} b \,\varepsilon\, v,w \wedge b \neq a.
\end{aligned}$$

12.2.10 Filter. Let $A(x)$ be arbitrary but fixed predicate. The function $\mathit{Filter}(x)$ removes all elements from a list which do not satisfy the predicate. The function satisfies

$$\vdash_{\mathrm{PA}} a \,\varepsilon\, \mathit{Filter}(x) \leftrightarrow a \,\varepsilon\, x \wedge A(a) \tag{1}$$

and it is defined by list recursion as a primitive recursive predicate in the predicate A:

$$\begin{aligned}
&\mathit{Filter}(0) = 0\\
&\mathit{Filter}(v,w) = v, \mathit{Filter}(w) \leftarrow A(v)\\
&\mathit{Filter}(v,w) = \mathit{Filter}(w) \leftarrow \neg A(v).
\end{aligned}$$

Property (1) is proved by list induction on x. The base case is straightforward and in the inductive case when $x = v,w$ we consider two cases. If $A(v)$ then we have

$$\begin{aligned}
&a \,\varepsilon\, \mathit{Filter}(v,w) \stackrel{\text{def}}{\Leftrightarrow} a \,\varepsilon\, v, \mathit{Filter}(v,w) \stackrel{12.1.11(2)}{\Leftrightarrow} a = v \vee a \,\varepsilon\, \mathit{Filter}(w) \stackrel{\text{IH}}{\Leftrightarrow}\\
&a = v \vee a \,\varepsilon\, w \wedge A(a) \stackrel{(*)}{\Leftrightarrow} (a = v \vee a \,\varepsilon\, w) \wedge A(a) \stackrel{12.1.11(2)}{\Leftrightarrow} a \,\varepsilon\, v,w \wedge A(a).
\end{aligned}$$

The equivalence marked by $(*)$ can be proved by a simple case analysis on whether $a = v$ or $a \neq v$ holds. The case when $\neg A(v)$ is similar.

12.2.11 Counting the number of occurrences in lists. The function $\#(a, x)$ counts the number of occurrences of the element a in the list x. The function is defined by list recursion on x as a primitive recursive function:

$\#(a, 0) = 0$
$\#(a, v, w) = \#(a, w) + 1 \leftarrow a = v$
$\#(a, v, w) = \#(a, w) \leftarrow a \neq v.$

The function satisfies:

$$\vdash_{\text{PA}} \forall a \, \#(a, x) = 0 \leftrightarrow x = 0 \tag{1}$$
$$\vdash_{\text{PA}} a \,\varepsilon\, x \leftrightarrow \#(a, x) \neq 0 \tag{2}$$
$$\vdash_{\text{PA}} \#(a, x \oplus y) = \#(a, x) + \#(a, y). \tag{3}$$

12.2.12 Removal of duplicates from lists. The function $\mathit{Nodoubles}(x)$ removes duplicates from a list. The function satisfies

$$\vdash_{\text{PA}} a \,\varepsilon\, \mathit{Nodoubles}(x) \leftrightarrow a \,\varepsilon\, x \tag{1}$$
$$\vdash_{\text{PA}} a \,\varepsilon\, \mathit{Nodoubles}(x) \rightarrow \#(a, \mathit{Nodoubles}(x)) = 1 \tag{2}$$

and it is defined by list recursion as a primitive recursive function:

$\mathit{Nodoubles}(0) = 0$
$\mathit{Nodoubles}(v, w) = \mathit{Nodoubles}(w) \leftarrow v \,\varepsilon\, w$
$\mathit{Nodoubles}(v, w) = v, \mathit{Nodoubles}(w) \leftarrow v \not\varepsilon\, w.$

12.3 Combinatorial Functions over Lists

12.3.1 Suffix relation. The binary predicate $x \sqsupset y$ holds if the list y is a suffix of the list x, ie

$$\vdash_{\text{PAx}} x \sqsupset y \leftrightarrow \exists z \, x = z \oplus y.$$

The predicate has the following basic properties:

$$\vdash_{\text{PA}} 0 \sqsupset y \leftrightarrow y = 0 \tag{1}$$
$$\vdash_{\text{PA}} v, w \sqsupset y \leftrightarrow y = v, w \lor w \sqsupset y. \tag{2}$$

12.3.2 Generating suffixes. The function $\mathit{Suffixes}(x)$ returns a list of all suffixes of the list x. The function satisfies

$$\vdash_{\text{PA}} y \,\varepsilon\, \mathit{Suffixes}(x) \leftrightarrow x \sqsupset y \tag{1}$$

and it is defined by list recursion as a primitive recursive function:

$\mathit{Suffixes}(0) = 0, 0$
$\mathit{Suffixes}(v, w) = (v, w), \mathit{Suffixes}(w).$

Property (1) is proved by list induction on x. In the base case when $x = 0$ we have

$$y \mathrel{\varepsilon} \mathit{Suffixes}(0) \overset{\text{def}}{\Leftrightarrow} y \mathrel{\varepsilon} 0,0 \Leftrightarrow y = 0 \overset{12.3.1(1)}{\Leftrightarrow} 0 \sqsupset y.$$

In the inductive case when $x = v, w$ we have

$$y \mathrel{\varepsilon} \mathit{Suffixes}(v,w) \overset{\text{def}}{\Leftrightarrow} y \mathrel{\varepsilon} (v,w), \mathit{Suffixes}(w) \Leftrightarrow y = v,w \lor y \mathrel{\varepsilon} \mathit{Suffixes}(w) \overset{\text{IH}}{\Leftrightarrow}$$
$$\Leftrightarrow y = v,w \lor w \sqsupset y \overset{12.3.1(2)}{\Leftrightarrow} v,w \sqsupset y.$$

12.3.3 Auxiliary function. Consider the function $\mathit{Mape}(y,x)$ defined by by list recursion on x as a primitive recursive function:

$\mathit{Mape}(y,0) = 0$
$\mathit{Mape}(y,v,w) = (y,v), \mathit{Mape}(y,w).$

The function satisfies:

$$\vdash_{\mathrm{PA}} z \mathrel{\varepsilon} \mathit{Mape}(y,x) \leftrightarrow \exists z_1(z_1 \mathrel{\varepsilon} x \land z = y, z_1). \tag{1}$$

12.3.4 Prefix relation. The binary predicate $y \sqsubset x$ holds if the list y is a prefix of the list x, ie

$$\vdash_{\mathrm{PAx}} y \sqsubset x \leftrightarrow \exists z\, x = y \oplus z.$$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} y \sqsubset 0 \leftrightarrow y = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} y \sqsubset v,w \leftrightarrow y = 0 \lor \exists z(z \sqsubset w \land y = v, z). \tag{2}$$

12.3.5 Generating prefixes. The function $\mathit{Prefixes}(x)$ returns a list of all prefixes of the list x. The function satisfies

$$\vdash_{\mathrm{PA}} y \mathrel{\varepsilon} \mathit{Prefixes}(x) \leftrightarrow y \sqsubset x \tag{1}$$

and it is defined by list recursion as a primitive recursive function:

$\mathit{Prefixes}(0) = 0,0$
$\mathit{Prefixes}(v,w) = 0, \mathit{Mape}(v, \mathit{Prefixes}(w)).$

Property $\forall y(1)$ is proved by list induction on x. In the base case when $x = 0$ take any y and we have

$$y \mathrel{\varepsilon} \mathit{Prefixes}(0) \overset{\text{def}}{\Leftrightarrow} y \mathrel{\varepsilon} 0,0 \Leftrightarrow y = 0 \overset{12.3.4(1)}{\Leftrightarrow} y \sqsubset 0.$$

In the inductive case when $x = v, w$ take any y and we have

$$y \mathrel{\varepsilon} \mathit{Prefixes}(v,w) \overset{\text{def}}{\Leftrightarrow} y \mathrel{\varepsilon} 0, \mathit{Mape}(v, \mathit{Prefixes}(w)) \Leftrightarrow$$
$$\Leftrightarrow y = 0 \lor y \mathrel{\varepsilon} \mathit{Mape}(v, \mathit{Prefixes}(w)) \overset{12.3.3(1)}{\Leftrightarrow}$$
$$\Leftrightarrow y = 0 \lor \exists z(z \mathrel{\varepsilon} \mathit{Prefixes}(w) \land y = v, z) \overset{\text{IH}}{\Leftrightarrow}$$
$$\Leftrightarrow y = 0 \lor \exists z(z \sqsubset w \land y = v, z) \overset{12.3.4(2)}{\Leftrightarrow} y \sqsubset v, w.$$

12.3.6 Segments. The binary predicate $y \subset x$ holds if the list y is a contiguous segment of the list x, ie

$$\vdash_{\mathrm{PAx}} y \subset x \leftrightarrow \exists z_1 \exists z_2\, x = z_1 \oplus y \oplus z_2.$$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} y \subset 0 \leftrightarrow y = 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} y \subset v, w \leftrightarrow \exists z(z \sqsubset w \land y = v, z) \lor y \subset w. \tag{2}$$

12.3.7 Generating segments. The function $\mathit{Segments}(x)$ returns a list of all segments of the list x. The function satisfies

$$\vdash_{\mathrm{PA}} y \mathrel{\varepsilon} \mathit{Segments}(x) \leftrightarrow y \subset x \tag{1}$$

and it is defined by list recursion as a primitive recursive function:

$\mathit{Segments}(0) = 0, 0$
$\mathit{Segments}(v, w) = \mathit{Mape}(v, \mathit{Prefixes}(w)) \oplus \mathit{Segments}(w).$

Property (1) is proved by list induction on x. In the base case when $x = 0$ we have

$$y \mathrel{\varepsilon} \mathit{Segments}(0) \overset{\text{def}}{\Leftrightarrow} y \mathrel{\varepsilon} 0, 0 \Leftrightarrow y = 0 \overset{12.3.6(1)}{\Leftrightarrow} y \subset 0.$$

In the inductive case when $x = v, w$ we have

$$y \mathrel{\varepsilon} \mathit{Segments}(v,w) \overset{\text{def}}{\Leftrightarrow} y \mathrel{\varepsilon} \mathit{Mape}(v, \mathit{Prefixes}(w)) \oplus \mathit{Segments}(w) \Leftrightarrow$$
$$\Leftrightarrow y \mathrel{\varepsilon} \mathit{Mape}(v, \mathit{Prefixes}(w)) \lor y \mathrel{\varepsilon} \mathit{Segments}(w) \overset{12.3.3(1),\text{IH}}{\Leftrightarrow}$$
$$\Leftrightarrow \exists z(z \mathrel{\varepsilon} \mathit{Prefixes}(w) \land y = v, z) \lor y \subset w \overset{12.3.5(1)}{\Leftrightarrow}$$
$$\Leftrightarrow \exists z(z \sqsubset w \land y = v, z) \lor y \subset w \overset{12.3.6(2)}{\Leftrightarrow} y \subset v, w.$$

12.3.8 Subsequences. The binary predicate $y \triangleleft x$ holds if the list y is a subsequence of the list x. The predicate $y \triangleleft x$ is defined by list recursion on x with substitution in parameter y::

$y \triangleleft 0 \leftarrow y = 0$
$y \triangleleft v_1, w_1 \leftarrow y = 0$
$y \triangleleft v_1, w_1 \leftarrow y = v_2, w_2 \land v_2 = v_1 \land w_2 \triangleleft w_1$
$y \triangleleft v_1, w_1 \leftarrow y = v_2, w_2 \land v_2 \neq v_1 \land y \triangleleft w_1.$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} y \vartriangleleft 0 \leftrightarrow y = 0 \tag{1}$$

$$\vdash_{\mathrm{PA}} y \vartriangleleft v, w \leftrightarrow \exists z(z \vartriangleleft w \wedge y = v, z) \vee y \vartriangleleft w. \tag{2}$$

12.3.9 Generating subsequences. The function $Subsqs(x)$ returns a list of all subsequences of the list x. The function satisfies

$$\vdash_{\mathrm{PA}} y \,\varepsilon\, Subsqs(x) \leftrightarrow y \vartriangleleft x \tag{1}$$

and it is defined by list recursion as a primitive recursive function:

$Subsqs(0) = 0, 0$
$Subsqs(v, w) = Mape(v, Subsqs(w)) \oplus Subsqs(w).$

Property $\forall y(1)$ is proved by list induction on x. In the base case when $x = 0$ take any y and we have

$$y \,\varepsilon\, Subsqs(0) \overset{\text{def}}{\Leftrightarrow} y \,\varepsilon\, 0, 0 \Leftrightarrow y = 0 \overset{12.3.8(1)}{\Leftrightarrow} y \vartriangleleft 0.$$

In the inductive case when $x = v, w$ take any y and we have

$$\begin{aligned} y \,\varepsilon\, Subsqs(v, w) &\overset{\text{def}}{\Leftrightarrow} y \,\varepsilon\, Mape(v, Subsqs(w)) \oplus Subsqs(w) \Leftrightarrow \\ &\Leftrightarrow y \,\varepsilon\, Mape(v, Subsqs(w)) \vee y \,\varepsilon\, Subsqs(w) \overset{12.3.3(1),\text{IH}}{\Leftrightarrow} \\ &\Leftrightarrow \exists z(z \,\varepsilon\, Subsqs(w) \wedge y = v, z) \vee y \vartriangleleft w \overset{\text{IH}}{\Leftrightarrow} \\ &\Leftrightarrow \exists z(z \vartriangleleft w \wedge y = v, z) \vee y \vartriangleleft w \overset{12.3.8(2)}{\Leftrightarrow} y \vartriangleleft v, w. \end{aligned}$$

12.3.10 Insertion relation. The ternary predicate $y \approx x[\downarrow a]$ holds if the list y is obtained from the list x by insertion of a into x, ie

$$\vdash_{\mathrm{PAx}} y \approx x[\downarrow a] \leftrightarrow \exists z_1 \exists z_2(x = z_1 \oplus z_2 \wedge y = z_1 \oplus (a, z_2)).$$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} y \approx 0[\downarrow a] \leftrightarrow y = a, 0$$

$$\vdash_{\mathrm{PA}} y \approx (v, w)[\downarrow a] \leftrightarrow y = a, v, w \vee \exists z(z \approx w[\downarrow a] \wedge y = v, z).$$

12.3.11 Permutations. The binary predicate $y \sim x$ holds if the list y is a permutation of the list x. The predicate is defined explicitly as follows

$$\vdash_{\mathrm{PAx}} x \sim y \leftrightarrow \forall a \,\#(a, x) = \#(a, y).$$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} y \sim 0 \leftrightarrow y = 0 \tag{1}$$

$$\vdash_{\mathrm{PA}} y \sim v, w \leftrightarrow \exists z(z \sim w \wedge y \approx z[\downarrow v]). \tag{2}$$

12.3.12 Generating permutations. The function $Perms(x)$ returns a list of all permutations of the list x. The function satisfies

$$\vdash_{\mathrm{PA}} y \,\varepsilon\, Perms(x) \leftrightarrow y \sim x \tag{1}$$

and it is defined by list recursion as a primitive recursive function:

$$\begin{aligned}
&Interleave(y,0) = (y,0),0\\
&Interleave(y,v,w) = (y,v,w), Mape(v, Interleave(y,w))\\
&Mapi(y,0) = 0\\
&Mapi(y,v,w) = Interleave(y,v) \oplus Mapi(y,w)\\
&Perms(0) = 0,0\\
&Perms(v,w) = Mapi(v, Perms(w)).
\end{aligned}$$

Note that the functions $Interleave(y,x)$ and $Mapi(y,x)$ are defined by list recursion on x.

The auxiliary functions satisfy

$$\vdash_{\mathrm{PA}} z \,\varepsilon\, Interleave(y,x) \leftrightarrow z \approx x[\downarrow y] \tag{2}$$

$$\vdash_{\mathrm{PA}} z \,\varepsilon\, Mapi(y,x) \leftrightarrow \exists z_1(z_1 \,\varepsilon\, x \wedge z \approx z_1[\downarrow y]). \tag{3}$$

Property $\forall y(1)$ is proved by list induction on x. In the base case when $x = 0$ take any y and we have

$$y \,\varepsilon\, Perms(0) \overset{\text{def}}{\Leftrightarrow} y \,\varepsilon\, 0,0 \Leftrightarrow y = 0 \overset{12.3.11(1)}{\Leftrightarrow} y \sim 0.$$

In the inductive case when $x = v,w$ take any y and we have

$$\begin{aligned}
y \,\varepsilon\, Perms(v,w) &\overset{\text{def}}{\Leftrightarrow} y \,\varepsilon\, Mapi(v, Perms(w)) \overset{(3)}{\Leftrightarrow}\\
&\Leftrightarrow \exists z(z \,\varepsilon\, Perms(w) \wedge y \approx z[\downarrow v]) \overset{\text{IH}}{\Leftrightarrow}\\
&\Leftrightarrow \exists z(z \sim w \wedge y \approx z[\downarrow v]) \overset{12.3.11(2)}{\Leftrightarrow}\\
&\Leftrightarrow y \sim v,w.
\end{aligned}$$

12.3.13 List partitions. The binary predicate $y \blacktriangleleft x$ holds if the list y is a partition of the list x, ie

$$\vdash_{\mathrm{PAx}} y \blacktriangleleft x \leftrightarrow \bigcup y = x \wedge 0 \not\varepsilon\, y,$$

where $\bigcup y$ is the list union function defined by list recursion:

$$\begin{aligned}
&\bigcup 0 = 0\\
&\bigcup (v,w) = v \oplus \bigcup w.
\end{aligned}$$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} y \blacktriangleleft 0 \leftrightarrow y = 0 \tag{1}$$

$$\begin{aligned}
&\vdash_{\mathrm{PA}} y \blacktriangleleft v,w \leftrightarrow\\
&\quad \exists z(z \blacktriangleleft w \wedge y = (v,0),z) \vee \exists z_1 \exists z_2(z_1, z_2 \blacktriangleleft w \wedge y = (v,z_1),z_2).
\end{aligned} \tag{2}$$

12.3.14 Generating list partitions. The function $Concps(x)$ returns a list of all partitions of the list x. The function satisfies

$$\vdash_{\mathrm{PA}} y \mathrel{\varepsilon} Concps(x) \leftrightarrow y \blacktriangleleft x \tag{1}$$

and it is defined by list recursion as a primitive recursive function:

$$\begin{aligned}
&Mapc_1(y,0) = 0\\
&Mapc_1(y,v,w) = ((y,0),v), Mapc_1(y,w)
\end{aligned}$$

$$\begin{aligned}
&Mapc_2(y,0) = 0\\
&Mapc_2(y,0,w) = Mapc_2(y,w)\\
&Mapc_2(y,(v_1,v_2),w) = ((y,v_1),v_2), Mapc_2(y,w)
\end{aligned}$$

$$\begin{aligned}
&Concps(0) = 0,0\\
&Concps(v,w) = Mapc_1(v, Concps(w)) \oplus Mapc_2(v, Concps(w)).
\end{aligned}$$

Note that the functions $Mapc_1(y,x)$ and $Mapc_2(y,x)$ are defined by list recursion on x.

The auxiliary functions satisfy

$$\vdash_{\mathrm{PA}} z \mathrel{\varepsilon} Mapc_1(y,x) \leftrightarrow \exists z_1(z_1 \mathrel{\varepsilon} x \land z = (y,0),z_1) \tag{2}$$
$$\vdash_{\mathrm{PA}} z \mathrel{\varepsilon} Mapc_2(y,x) \leftrightarrow \exists z_1 \exists z_2(z_1,z_2 \mathrel{\varepsilon} x \land z = (y,z_1),z_2). \tag{3}$$

Property $\forall y(1)$ is proved by list induction on x. In the base case when $x = 0$ take any y and we have

$$y \mathrel{\varepsilon} Concps(0) \overset{\mathrm{def}}{\Leftrightarrow} y \mathrel{\varepsilon} 0,0 \Leftrightarrow y = 0 \overset{12.3.13(1)}{\Leftrightarrow} y \blacktriangleleft 0.$$

In the inductive case when $x = v,w$ take any y and we have

$$\begin{aligned}
y \mathrel{\varepsilon} &Concps(v,w) \overset{\mathrm{def}}{\Leftrightarrow}\\
&\Leftrightarrow y \mathrel{\varepsilon} Mapc_1(v, Concps(w)) \oplus Mapc_2(v, Concps(w)) \Leftrightarrow\\
&\Leftrightarrow y \mathrel{\varepsilon} Mapc_1(v, Concps(w)) \lor y \mathrel{\varepsilon} Mapc_2(v, Concps(w)) \overset{(2),(3)}{\Leftrightarrow}\\
&\Leftrightarrow \exists z(z \mathrel{\varepsilon} Concps(w) \land y = (v,0),z) \lor\\
&\qquad \lor \exists z_1 \exists z_2(z_1,z_2 \mathrel{\varepsilon} Concps(w) \land y = (v,z_1),z_2) \overset{2\times\mathrm{IH}}{\Leftrightarrow}\\
&\Leftrightarrow \exists z(z \blacktriangleleft w \land y = (v,0),z) \lor\\
&\qquad \lor \exists z_1 \exists z_2(z_1,z_2 \blacktriangleleft w \land y = (v,z_1),z_2) \overset{12.3.13(2)}{\Leftrightarrow}\\
&\Leftrightarrow y \blacktriangleleft v,w.
\end{aligned}$$

12.4 Sorting of Lists

12.4.1 The problem of sorting.

12.4.2 Permutations. Recall that the binary predicate $x \sim y$ holding if the list x is a permutation of the list y is defined explicitly by

$$\vdash_{\mathrm{PAx}} x \sim y \leftrightarrow \forall a\, \#(a,x) = \#(a,y).$$

The predicate has the following properties:

$$\vdash_{\mathrm{PA}} x \sim x \tag{1}$$
$$\vdash_{\mathrm{PA}} x \sim y \to y \sim x \tag{2}$$
$$\vdash_{\mathrm{PA}} x \sim y \wedge y \sim z \to x \sim z \tag{3}$$
$$\vdash_{\mathrm{PA}} x \sim y \to a,x \sim a,y \tag{4}$$
$$\vdash_{\mathrm{PA}} x \sim y \to L(x) = L(y) \tag{5}$$
$$\vdash_{\mathrm{PA}} x_1 \sim y_1 \wedge x_2 \sim y_2 \to x_1 \oplus x_2 \sim y_1 \oplus y_2 \tag{6}$$
$$\vdash_{\mathrm{PA}} x \sim y \wedge a \,\varepsilon\, x \to a \,\varepsilon\, y \tag{7}$$
$$\vdash_{\mathrm{PA}} 0 \sim y \leftrightarrow y = 0 \tag{8}$$
$$\vdash_{\mathrm{PA}} a,b,x \sim b,a,x \tag{9}$$
$$\vdash_{\mathrm{PA}} x_1 \oplus (a,x_2) \sim y_1 \oplus (a,y_2) \leftrightarrow x_1 \oplus x_2 \sim y_1 \oplus y_2 \tag{10}$$
$$\vdash_{\mathrm{PA}} x \sim v,w \leftrightarrow \exists z_1 \exists z_2 (x = z_1 \oplus (v,z_2) \wedge w \sim z_1 \oplus z_2) \tag{11}$$
$$\vdash_{\mathrm{PA}} x \sim v,w \leftrightarrow \exists z (z \sim w \wedge x \approx z[\downarrow v]). \tag{12}$$

Properties (1)-(4), (8), and (9) have straightforward proofs. Properties (6) and (10) follow from 12.2.11(3). Property (7) follows from 12.2.11(2).

The ($\to$)-direction of (11) is proved as follows. Assume $x \sim v,w$. Then $v \,\varepsilon\, x$ by (7) and thus $x = z_1 \oplus (v,z_2)$ for some z_1 and z_2 by 12.6.1(1). Note also that $w \sim z_1 \oplus z_2$ by (10). The ($\leftarrow$)-direction of (11) follows from (10).

Property (12) follows from

$$\begin{aligned}
&x \sim v,w \overset{(11)}{\Leftrightarrow} \exists z_1 \exists z_2 (x = z_1 \oplus (v,z_2) \wedge w \sim z_1 \oplus z_2) \Leftrightarrow \\
&\exists z_3 \exists z_4 \big(\exists z_1 \exists z_2 (x = z_1 \oplus (v,z_2) \wedge z_3 \oplus z_4 = z_1 \oplus z_2) \wedge w \sim z_3 \oplus z_4\big) \overset{\mathrm{def}}{\Leftrightarrow} \\
&\exists z_3 \exists z_4 (x \approx (z_3 \oplus z_4)[\downarrow v] \wedge w \sim z_3 \oplus z_4) \Leftrightarrow \exists z (z \sim w \wedge x \approx z[\downarrow v]).
\end{aligned}$$

Property $\forall y(5)$ is proved by list induction on x. The base case is straightforward. In the inductive case when $x = v,w$ take any y such that $v,w \sim y$. Then $y = z_1 \oplus (v,z_2)$ and $w \sim z_1 \oplus z_2$ for some z_1 and z_2 by (11). We have

$$\begin{aligned}
L(v,w) &= L(w) + 1 \overset{\mathrm{IH}}{=} L(z_1 \oplus z_2) + 1 \overset{12.1.9(8)}{=} L(z_1) + L(z_2) + 1 = \\
&= L(z_1) + L(v,z_2) \overset{12.1.9(8)}{=} L(z_1 \oplus (v,z_2)).
\end{aligned}$$

12.4.3 List comparision predicates. The predicate $a \preceq x$ holds if $a \leq b$ for every element b of the list x, ie

$$\vdash_{\mathrm{PAx}} a \preceq x \leftrightarrow \forall b (b \,\varepsilon\, x \to a \leq b).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} a \preceq 0 \tag{1}$$
$$\vdash_{\mathrm{PA}} a \preceq v,w \leftrightarrow a \leq v \wedge a \preceq w \tag{2}$$
$$\vdash_{\mathrm{PA}} a \leq b \wedge b \preceq x \rightarrow a \preceq x \tag{3}$$
$$\vdash_{\mathrm{PA}} a \preceq x \oplus y \leftrightarrow a \preceq x \wedge a \preceq y \tag{4}$$
$$\vdash_{\mathrm{PA}} x \sim y \rightarrow a \preceq x \leftrightarrow a \preceq y. \tag{5}$$

The predicate $a \succeq x$ holds if $a \geq b$ for every element b of the list x, ie

$$\vdash_{\mathrm{PAx}} a \succeq x \leftrightarrow \forall b(b \,\varepsilon\, x \rightarrow a \geq b).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} a \succeq 0 \tag{6}$$
$$\vdash_{\mathrm{PA}} a \succeq v,w \leftrightarrow a \geq v \wedge a \succeq w \tag{7}$$
$$\vdash_{\mathrm{PA}} a \geq b \wedge b \succeq x \rightarrow a \succeq x \tag{8}$$
$$\vdash_{\mathrm{PA}} a \succeq x \oplus y \leftrightarrow a \succeq x \wedge a \succeq y \tag{9}$$
$$\vdash_{\mathrm{PA}} x \sim y \rightarrow a \succeq x \leftrightarrow a \succeq y. \tag{10}$$

The predicate $x \preceq_s y$ holds if $a \leq b$ for every elements a and b of the lists x and y respectively, ie

$$\vdash_{\mathrm{PAx}} x \preceq_s y \leftrightarrow \forall a \forall b(a \,\varepsilon\, x \wedge b \,\varepsilon\, y \rightarrow a \leq b).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} 0 \preceq_s y \tag{11}$$
$$\vdash_{\mathrm{PA}} v,w \preceq_s y \rightarrow v \preceq y \wedge w \preceq_s y \tag{12}$$
$$\vdash_{\mathrm{PA}} x \preceq_s 0 \tag{13}$$
$$\vdash_{\mathrm{PA}} x \preceq_s v,w \leftrightarrow v \succeq x \wedge x \preceq_s w \tag{14}$$
$$\vdash_{\mathrm{PA}} a \succeq x \wedge a \preceq y \rightarrow x \preceq_s y. \tag{15}$$

Properties (1)-(3) are straightforward. Property (4) is proved by list induction on x. The base case follows from (1). In the inductive case we have

$$a \preceq (v,w) \oplus y \Leftrightarrow a \preceq v, w \oplus y \overset{(2)}{\Leftrightarrow} a \leq v \wedge a \preceq w \oplus y \overset{\mathrm{IH}}{\Leftrightarrow}$$
$$a \leq v \wedge a \preceq w \wedge a \preceq y \overset{(2)}{\Leftrightarrow} a \preceq v,w \wedge a \preceq y.$$

Property $\forall y(5)$ is proved by list induction on x. The base case is straightforward. In the inductive case when $x = v,w$ take any y such that $v,w \sim y$. Then $y = z_1 \oplus (v, z_2)$ and $w \sim z_1 \oplus z_2$ for some z_1 and z_2 by 12.4.2(11). We have

$$a \preceq v, w \overset{(2)}{\Leftrightarrow} a \leq v \wedge a \preceq w \overset{\mathrm{IH}}{\Leftrightarrow} a \leq v \wedge a \preceq z_1 \oplus z_2 \overset{(4)}{\Leftrightarrow}$$
$$a \leq v \wedge a \preceq z_1 \wedge a \preceq z_2 \overset{(2)}{\Leftrightarrow} a \preceq z_1 \wedge a \preceq v, z_2 \overset{(4)}{\Leftrightarrow} a \preceq z_1 \oplus (v, z_2).$$

Properties (6)-(10) are proved similarly. Properties (11)-(15) are straightforward.

12.4.4 Ordered lists. The predicate $Ord(x)$ holds if x is an ordered list. The predicate is defined by

$$\vdash_{\mathrm{PAx}} Ord(x) \leftrightarrow \forall i \forall j (i \leq j \wedge j < L(x) \rightarrow (x)_i \leq (x)_j).$$

The predicate has the following basic properties:

$$\vdash_{\mathrm{PA}} Ord(0) \tag{1}$$
$$\vdash_{\mathrm{PA}} Ord(v, w) \leftrightarrow Ord(w) \wedge v \preceq w \tag{2}$$
$$\vdash_{\mathrm{PA}} Ord(v, w) \rightarrow a \preceq v, w \leftrightarrow a \leq v \tag{3}$$
$$\vdash_{\mathrm{PA}} Ord(x \oplus y) \leftrightarrow Ord(x) \wedge Ord(y) \wedge x \preceq_s y. \tag{4}$$

Properties (1)-(3) are straightforward. Property (4) is proved by list induction on x. The base case follows from 12.4.3(11). In the inductive case we have

$$Ord((v, w) \oplus y) \Leftrightarrow Ord(v, w \oplus y) \overset{(2)}{\Leftrightarrow} Ord(w \oplus y) \wedge v \preceq w \oplus y \overset{\mathrm{IH},12.4.3(2)}{\Leftrightarrow}$$
$$Ord(w) \wedge Ord(y) \wedge w \preceq_s y \wedge v \preceq w \wedge v \preceq y \overset{(2),12.4.3(12)}{\Leftrightarrow}$$
$$Ord(v, w) \wedge Ord(y) \wedge v, w \preceq_s y.$$

12.4.5 Insertion sort. The simplest sorting algorithm is *insertion sort*. Insertion sort works on a non-empty list by recursively sorting the tail and then inserts the first element into the sorted list. The length of computation is $O(L(x)^2)$.

The insertion function $Insert(a, x)$ takes an ordered list x and yields a new one by inserting a into it. The function satisfies

$$\vdash_{\mathrm{PA}} Insert(a, x) \sim a, x \tag{1}$$
$$\vdash_{\mathrm{PA}} Ord(x) \rightarrow Ord\, Insert(a, x) \tag{2}$$

and it is defined by list recursion on x as a primitive recursive function:

$Insert(a, 0) = a, 0$
$Insert(a, v, w) = a, v, w \leftarrow a \leq v$
$Insert(a, v, w) = v, Insert(a, w) \leftarrow a > v.$

The function $Isort(x)$ realizing insertion sort is defined by list recursion as a primitive recursive function:

$Isort(0) = 0$
$Isort(v, w) = Insert(v, Isort(w)).$

We claim that

$$\vdash_{\mathrm{PA}} \mathit{Isort}(x) \sim x \tag{3}$$
$$\vdash_{\mathrm{PA}} \mathit{Ord}\,\mathit{Isort}(x). \tag{4}$$

Property (1) is proved by list induction on x. The base case is straightforward. In the inductive case when $x = v, w$ we consider two cases. If $a \leq v$ then $\mathit{Insert}(a, v, w) \overset{\mathrm{def}}{=} a, v, w \sim a, v, w$. If $a > v$ then

$$\mathit{Insert}(a, v, w) \overset{\mathrm{def}}{=} v, \mathit{Insert}(a, w) \overset{\mathrm{IH}}{\sim} v, a, w \sim a, v, w.$$

As a simple consequence of (1) and 12.4.3(5) we get

$$\vdash_{\mathrm{PA}} b \preceq \mathit{Insert}(a, x) \leftrightarrow b \leq a \wedge b \preceq x. \tag{5}$$

Property (2) is proved by list induction on x. The base case is straightforward. In the inductive case when $x = v, w$ assume $\mathit{Ord}(v, w)$ and consider two cases. If $a \leq v$ then we have

$$\mathit{Ord}\,\mathit{Insert}(a, v, w) \overset{\mathrm{def}}{\Leftrightarrow} \mathit{Ord}(a, v, w) \overset{12.4.4(2)}{\Leftrightarrow} \mathit{Ord}(v, w) \wedge a \preceq v, w.$$

The last follows from assumptions by 12.4.4(3). If $a > v$ then we have

$$\mathit{Ord}\,\mathit{Insert}(a, v, w) \overset{\mathrm{def}}{\Leftrightarrow} \mathit{Ord}(v, \mathit{Insert}(a, w)) \overset{12.4.4(2)}{\Leftrightarrow}$$
$$\mathit{Ord}\,\mathit{Insert}(a, w) \wedge v \preceq \mathit{Insert}(a, w) \overset{(5)}{\Leftrightarrow} \mathit{Ord}\,\mathit{Insert}(a, w) \wedge v \leq a \wedge v \preceq w.$$

The last follows from assumptions and IH.

Property (3) is proved by list induction. The base case is straightforward. In the inductive case we have

$$\mathit{Isort}(v, w) \overset{\mathrm{def}}{=} \mathit{Insert}(v, \mathit{Isort}(w)) \overset{(1)}{\sim} v, \mathit{Isort}(w) \overset{\mathrm{IH}}{\sim} v, w.$$

Property (4) is proved by list induction. The base case follows from 12.4.4(1). In the inductive case when $x = v, w$ assume $\mathit{Ord}(v, w)$. Then $\mathit{Ord}(w)$ by 12.4.4(2) and we get from IH:

$$\mathit{Ord}\,\mathit{Isort}(w) \overset{(2)}{\Rightarrow} \mathit{Ord}\,\mathit{Insert}(v, \mathit{Isort}(w)) \overset{\mathrm{def}}{\Rightarrow} \mathit{Ord}\,\mathit{Isort}(v, w).$$

12.4.6 Merge sort. More efficient sorting algorithm than insertion sort is *merge sort*. It sorts a list by dividing it into two roughly equal parts. Each part is then recursively sorted and the resulting lists are merged into one list. The length of computation is $O(L(x) \cdot \log L(x))$.

The function $\mathit{Msplit}(x)$ divides a list into two lists: the length of the first one is at most one more than the length of the second. The function satisfies

$$\vdash_{\mathrm{PA}} \exists y \exists z\, Msplit(x) = y, z \tag{1}$$
$$\vdash_{\mathrm{PA}} Msplit(x) = y, z \to x \sim y \oplus z \tag{2}$$
$$\begin{aligned} &\vdash_{\mathrm{PA}} Msplit(x) = y, z \to \\ &\quad L(x) = L(y) + L(z) \wedge (L(y) = L(z) \vee L(y) = L(z) + 1) \end{aligned} \tag{3}$$

and it is defined by course of values recursion with measure $L(x)$ as a primitive recursive function:

$$\begin{aligned} &Msplit(0) = 0, 0 \\ &Msplit(u, 0) = (u, 0), 0 \\ &Msplit(u, v, w) = (u, y), v, z \leftarrow Msplit(w) = y, z. \end{aligned}$$

The function $Merge(x, y)$ merges two ordered lists into one list. The function satisfies

$$\vdash_{\mathrm{PA}} Merge(x, y) \sim x \oplus y \tag{4}$$
$$\vdash_{\mathrm{PA}} Ord(x) \wedge Ord(y) \to Ord\, Merge(x, y) \tag{5}$$

and it is defined by course of values recursion with measure $L(x) + L(y)$ as a primitive recursive function:

$$\begin{aligned} &Merge(0, y) = y \\ &Merge((v_1, w_1), 0) = v_1, w_1 \\ &Merge((v_1, w_1), v_2, w_2) = v_1, Merge(w_1, v_2, w_2) \leftarrow v_1 \le v_2 \\ &Merge((v_1, w_1), v_2, w_2) = v_2, Merge((v_1, w_1), w_2) \leftarrow v_1 > v_2. \end{aligned}$$

Merge sort is realized by the function $Msort(x)$ defined by course of values recursion with measure $L(x)$ as a primitive recursive function:

$$\begin{aligned} &Msort(0) = 0 \\ &Msort(u, 0) = u, 0 \\ &Msort(u, v, w) = Merge(Msort(u, y), Msort(v, z)) \leftarrow Msplit(w) = y, z. \end{aligned}$$

We claim that

$$\vdash_{\mathrm{PA}} Msort(x) \sim x \tag{6}$$
$$\vdash_{\mathrm{PA}} Ord\, Msort(x). \tag{7}$$

Property (1) is proved by measure induction with measure $L(x)$. Property $\forall y \forall z(2)$ is proved by the same induction as follows. Take any x, y, and z such that $Msplit(x) = y, z$ and consider three cases. The cases when $x = 0$ or $x = u, 0$ are straightforward. So suppose $x = u, v, w$ for some u, v, and w. By (1) there are y_1 and z_1 such that $Msplit(w) = y_1, z_1$. We have

$$u, v, w \overset{\mathrm{IH}}{\sim} u, v, y_1 \oplus z_1 \sim (u, y_1) \oplus (v, z_1) \overset{\mathrm{def}}{=} y \oplus z.$$

As a simple consequence of (2) and 12.4.2(5) we get

$$\vdash_{\mathrm{PA}} \mathit{Msplit}(x) = y, z \to L(x) = L(y) + L(z). \tag{8}$$

Property (3) follows from (8) and from

$$\vdash_{\mathrm{PA}} \forall y \forall z(\mathit{Msplit}(x) = y, z \to L(y) = L(z) \lor L(y) = L(z) + 1)$$

which is proved by measure induction on x with measure $L(x)$.

Property (4) is proved by measure induction with measure $L(x) + L(y)$. Take any x and y and consider the following cases. The cases when $x = 0$ or $y = 0$ are straightforward. So suppose $x = v_1, w_1$ and $y = v_2, w_2$ for some v_1, w_1, v_2, and w_2. If $v_1 \leq v_2$ then we have

$$\begin{aligned} \mathit{Merge}((v_1, w_1), v_2, w_2) &\stackrel{\mathrm{def}}{=} v_1, \mathit{Merge}(w_1, v_2, w_2) \stackrel{\mathrm{IH}}{\sim} \\ &\sim v_1, w_1 \oplus (v_2, w_2) = (v_1, w_1) \oplus (v_2, w_2). \end{aligned}$$

The case when $v_1 < v_2$ has a similar proof. As a simple consequence of (4) and 12.4.3(5) we get

$$\vdash_{\mathrm{PA}} a \preceq \mathit{Merge}(x, y) \leftrightarrow a \preceq x \land a \preceq y. \tag{9}$$

Property (5) is proved by measure induction with measure $L(x) + L(y)$. Take any x and y and assume $\mathit{Ord}(x)$ and $\mathit{Ord}(y)$. If $x = 0$ or $y = 0$ then the property holds trivially. So suppose $x = v_1, w_1$ and $y = v_2, w_2$ for some v_1, w_1, v_2, and w_2. If $v_1 \leq v_2$ then we have

$$\begin{aligned} &\mathit{Ord}\ \mathit{Merge}((v_1, w_1), v_2, w_2) \stackrel{\mathrm{def}}{\Leftrightarrow} \mathit{Ord}(v_1, \mathit{Merge}(w_1, v_2, w_2)) \stackrel{12.4.4(2)}{\Leftrightarrow} \\ &\mathit{Ord}\ \mathit{Merge}(w_1, v_2, w_2) \land v_1 \preceq \mathit{Merge}(w_1, v_2, w_2) \stackrel{(9)}{\Leftrightarrow} \\ &\mathit{Ord}\ \mathit{Merge}(w_1, v_2, w_2) \land v_1 \preceq w_1 \land v_1 \preceq v_2, w_2. \end{aligned}$$

The last follows from IH and from assumptions by 12.4.4(2) and 12.4.4(3). The case when $v_1 < v_2$ is similar.

Property (6) is proved by measure induction with measure $L(x)$. Take any x and consider three cases. The cases when $x = 0$ or $x = u, 0$ for some u are straightforward. So suppose $x = u, v, w$ for some u, v, and w. By (1) there are y and z such that $\mathit{Msplit}(w) = y, z$. Note that $L(u, y) < L(x)$ and $L(v, z) < L(x)$ by (8). We have

$$\begin{aligned} &\mathit{Msort}(u, v, w) \stackrel{\mathrm{def}}{=} \mathit{Merge}(\mathit{Msort}(u, y), \mathit{Msort}(v, z)) \stackrel{(4)}{\sim} \\ &\quad \sim \mathit{Msort}(u, y) \oplus \mathit{Msort}(v, z) \stackrel{\mathrm{IH}}{\sim} (u, y) \oplus (v, z) \sim u, v, y \oplus z \stackrel{(2)}{\sim} u, v, w. \end{aligned}$$

Property (7) is proved by measure induction with measure $L(x)$. Take any x and consider three cases. The cases when $x = 0$ or $x = u, 0$ for some u are straightforward. So suppose $x = u, v, w$ for some u, v, and w. By (1) there are y and z such that $\mathit{Msplit}(w) = y, z$. Note again that $L(u, y) < L(x)$ and $L(v, z) < L(x)$ by (8). We have by IH

$$Ord\ Msort(u,y) \wedge Ord\ Msort(v,z) \overset{(5)}{\Rightarrow}$$
$$Ord\ Merge(Msort(u,y), Msort(v,z)) \overset{\text{def}}{\Rightarrow} Ord\ Msort(u,v,w).$$

12.4.7 Quicksort. One of the most efficient sorting algorithms is *quicksort*. It sorts a list by selecting one of its elements called *pivot*. Then it splits the list into two parts: with elements lesser and/or greater than the pivot. Each part is recursively sorted and the resulting lists together with the pivot are concatenated into one ordered list. The length of computation is $O(L(x)^2)$ in the worst case and $O(L(x) \cdot \log L(x))$ on average.

The function $Qsplit(p,x)$ splits a list x according to the pivot p into two lists: the first one with elements $\leq p$ and the second with elements $\geq p$. The function satisfies

$$\vdash_{\text{PA}} \exists y \exists z\, Qsplit(p,x) = y,z \tag{1}$$
$$\vdash_{\text{PA}} Qsplit(p,x) = y,z \rightarrow x \sim y \oplus z \tag{2}$$
$$\vdash_{\text{PA}} Qsplit(p,x) = y,z \rightarrow p \succeq y \wedge p \preceq z \tag{3}$$

and it is defined by list recursion on x as a primitive recursive function:

$$Qsplit(p,0) = 0,0$$
$$Qsplit(p,v,w) = (v,y),z \leftarrow v \leq p \wedge Qsplit(p,w) = y,z$$
$$Qsplit(p,v,w) = y,v,z \leftarrow v > p \wedge Qsplit(p,w) = y,z.$$

As a simple consequence of (2) and 12.4.2(5) we get

$$\vdash_{\text{PA}} Qsplit(p,x) = y,z \rightarrow L(x) = L(y) + L(z). \tag{4}$$

Quicksort $Qsort(x)$ is defined by course of values recursion with measure $L(x)$ as a primitive recursive function:

$$Qsort(0) = 0$$
$$Qsort(p,x) = Qsort(y) \oplus (p,0) \oplus Qsort(z) \leftarrow Qsplit(p,x) = y,z.$$

We claim that

$$\vdash_{\text{PA}} Qsort(x) \sim x \tag{5}$$
$$\vdash_{\text{PA}} Ord\ Qsort(x). \tag{6}$$

Property (1) is proved by a straightforward list induction. Property $\forall y \forall z(2)$ is proved by the same induction as follows. The base case is straightforward. In the inductive case when $x = v,w$ take any y and z such that $Qsplit(p,v,w) = y,z$ and consider two cases. If $v \leq p$ then $Qsplit(w) = y_1,z_1$ for some y_1 and z_1 by (1). We have

$$v,w \overset{\text{IH}}{\sim} v,y_1 \oplus z_1 = (v,y_1) \oplus z_1 \overset{\text{def}}{=} y \oplus z.$$

The case when $v > p$ is similar. Property $\forall y \forall z(3)$ is proved by list induction on x. The base case is straightforward. In the inductive case when $x = v,w$

take any y and z such that $Qsplit(p,v,w) = y,z$ and consider two cases. If $v \leq p$ then $Qsplit(w) = y_1,z_1$ for some y_1 and z_1 by (1). We get from IH the following

$$p \succeq y_1 \land p \preceq z_1 \overset{12.4.3(7)}{\Rightarrow} p \succeq v,y_1 \land p \preceq z_1 \overset{\text{def}}{\Rightarrow} p \succeq y \land p \preceq z.$$

The case when $v > p$ is similar.

Property (5) is proved by measure induction with measure $L(x)$. Take any x and consider two cases. If $x = 0$ then the property holds trivially. If $x = p,x_1$ then $Qsplit(p,x_1) = y,z$ for some y and z by (1). Note that $L(y) < L(x)$ and $L(z) < L(x)$ by (4). We have

$$Qsort(p,x_1) \overset{\text{def}}{=} Qsort(y) \oplus (p, Qsort(z)) \overset{\text{IH}}{\sim} y \oplus (p,z) \sim p,y \oplus z \overset{(2)}{\sim} p,x_1.$$

As a simple consequence of (5) and the properties 12.4.3(5)(10) we get

$$\vdash_{\text{PA}} a \preceq Qsort(x) \leftrightarrow a \preceq x \tag{7}$$
$$\vdash_{\text{PA}} a \succeq Qsort(x) \leftrightarrow a \succeq x. \tag{8}$$

Property (6) is proved by measure induction with measure $L(x)$. Take any x and consider two cases. If $x = 0$ then the property holds trivially. If $x = p,x_1$ then $Qsplit(p,x_1) = y,z$ for some y and z by (1). Note again that $L(y) < L(x)$ and $L(z) < L(x)$ by (4). We have

$$Ord\ Qsort(p,x_1) \overset{\text{def}}{\Leftrightarrow} Ord(Qsort(y) \oplus (p, Qsort(z))) \overset{12.4.4(4)}{\Leftrightarrow}$$
$$Ord\ Qsort(y) \land Ord(p, Qsort(z)) \land Qsort(y) \preceq_s p, Qsort(z) \overset{12.4.4(2),12.4.3(14)}{\Leftrightarrow}$$
$$Ord\ Qsort(y) \land Ord\ Qsort(z) \land$$
$$\land\, p \preceq Qsort(z) \land p \succeq Qsort(y) \land Qsort(y) \preceq_s Qsort(z) \overset{12.4.3(15)}{\Leftrightarrow}$$
$$Ord\ Qsort(y) \land Ord\ Qsort(z) \land p \succeq Qsort(y) \land p \preceq Qsort(z).$$

Conditions $Ord\ Qsort(y)$ and $Ord\ Qsort(z)$ follows from IH and conditions $p \succeq Qsort(y)$ and $p \preceq Qsort(z)$ are simple consequences of (3), (7), and (8).

12.5 Applications of Lists

Finite sets

12.5.1 List comparision predicate. The predicate $a \prec x$ holds if $a < b$ for every element b of the list x, ie

$$\vdash_{\text{PAx}} a \prec x \leftrightarrow \forall b(b \,\varepsilon\, x \to a < b).$$

The predicate has the following easy to prove properties:

$$\vdash_{\mathrm{PA}} a \not\prec 0 \quad (1)$$
$$\vdash_{\mathrm{PA}} a \prec v, w \leftrightarrow a < v \lor a \prec w \quad (2)$$
$$\vdash_{\mathrm{PA}} a \prec x \rightarrow a \preceq x \quad (3)$$
$$\vdash_{\mathrm{PA}} a \leq b \land b \prec x \rightarrow a \prec x. \quad (4)$$

12.5.2 Finite sets. The predicate $Set(s)$ holds if s is a (code of) finite set of natural numbers. The predicate is defined by

$$\vdash_{\mathrm{PAx}} Set(s) \leftrightarrow \forall i \forall j (i < j \land j < L(s) \rightarrow (s)_i < (s)_j).$$

The predicate has the following easy to prove properties:

$$\vdash_{\mathrm{PA}} Set(0) \quad (1)$$
$$\vdash_{\mathrm{PA}} Set(a, s) \leftrightarrow Set(s) \land a \prec s \quad (2)$$
$$\vdash_{\mathrm{PA}} Set(a, s) \rightarrow b \prec a, s \leftrightarrow b < a \quad (3)$$
$$\vdash_{\mathrm{PA}} Set(a, s) \rightarrow a \not\varepsilon\, s. \quad (4)$$

12.5.3 Set membership. The set membership predicate $x \in a$ has the following basic property

$$\vdash_{\mathrm{PA}} Set(s) \rightarrow a \in s \leftrightarrow a \,\varepsilon\, s \quad (1)$$

and it is defined by list recursion on s as a primitive recursive predicate:

$a \in b, s \leftarrow a = b$
$a \in b, s \leftarrow a > b \land a \in s.$

Property (1) is proved by a straightforward list induction on s.

12.5.4 Set insertion. The function $\{a\} \cup s$ inserts a into the set s. The function satisfies

$$\vdash_{\mathrm{PA}} Set(s) \rightarrow Set(\{a\} \cup s) \quad (1)$$
$$\vdash_{\mathrm{PA}} Set(s) \rightarrow b \in \{a\} \cup s \leftrightarrow b = a \lor b \in s \quad (2)$$

and it is defined by list recursion on s as a primitive recursive function:

$\{a\} \cup 0 = a, 0$
$\{a\} \cup (b, s) = a, b, s \leftarrow a < b$
$\{a\} \cup (b, s) = b, s \leftarrow a = b$
$\{a\} \cup (b, s) = b, \{a\} \cup s \leftarrow a > b.$

First note that

$$\vdash_{\mathrm{PA}} b \,\varepsilon\, \{a\} \cup s \leftrightarrow b = a \lor b \,\varepsilon\, s. \quad (3)$$

Property (3) is proved by list induction on s. The base case is straightforward. In the inductive case when $s = c, s_1$ we consider three cases. If $a < c$ then we have

$$b \,\varepsilon\, \{a\} \cup (c, s_1) \overset{\text{def}}{\Leftrightarrow} b \,\varepsilon\, a, c, s_1 \Leftrightarrow b = a \lor b \,\varepsilon\, c, s_1 .$$

If $a = c$ then we have

$$b \,\varepsilon\, \{c\} \cup (c, s_1) \overset{\text{def}}{\Leftrightarrow} b \,\varepsilon\, c, s_1 \Leftrightarrow b = c \lor b \,\varepsilon\, c, s_1 .$$

If $a > c$ then we have

$$\begin{aligned} b \,\varepsilon\, \{a\} \cup (c, s_1) \overset{\text{def}}{\Leftrightarrow} b \,\varepsilon\, c, \{a\} \cup s_1 \Leftrightarrow b = c \lor b \,\varepsilon\, \{a\} \cup s_1 \overset{\text{IH}}{\Leftrightarrow} \\ \Leftrightarrow b = c \lor b = a \lor b \,\varepsilon\, s_1 \Leftrightarrow b = a \lor b \,\varepsilon\, c, s_1 . \end{aligned}$$

As a simple consequence of (3) we get

$$b \prec \{a\} \cup s \leftrightarrow b \prec a, s. \tag{4}$$

Property (1) is proved by list induction on s. The base case is straightforward. In the inductive case, when $s = b, s_1$, assume $Set(b, s_1)$ and consider three cases. If $a < b$ then we have

$$Set(\{a\} \cup (b, s_1)) \overset{\text{def}}{\Leftrightarrow} Set(a, b, s_1) \overset{12.5.2(2)}{\Leftrightarrow} Set(b, s_1) \land a \prec b, s_1 .$$

The last follows from assumptions by 12.5.2(3). If $a > b$ then we have

$$\begin{aligned} &Set(\{a\} \cup (b, s_1)) \overset{\text{def}}{\Leftrightarrow} Set(b, \{a\} \cup s_1) \overset{12.5.2(2)}{\Leftrightarrow} Set(\{a\} \cup s_1) \land b \prec \{a\} \cup s_1 \overset{(4)}{\Leftrightarrow} \\ &Set(\{a\} \cup s_1) \land b \prec a, s_1 \overset{12.5.1(2)}{\Leftrightarrow} Set(\{a\} \cup s_1) \land b < a \land b \prec s_1 \end{aligned}$$

The last follows from IH and 12.5.2(2). The case when $a = b$ is trivial.

Property (2) is a straighforward consequence of 12.5.3(1), (1), and (3).

12.5.5 Set deletion. The function $s \setminus \{a\}$ deletes a from the set s. The function satisfies

$$\vdash_{\text{PA}} Set(s) \to Set(s \setminus \{a\}) \tag{1}$$

$$\vdash_{\text{PA}} Set(s) \to b \in s \setminus \{a\} \leftrightarrow b \in s \land b \neq a \tag{2}$$

and it is defined by list recursion on s as a primitive recursive function:

$$\begin{aligned} &0 \setminus \{a\} = 0 \\ &(b, s) \setminus \{a\} = b, s \setminus \{a\} \leftarrow b < a \\ &(b, s) \setminus \{a\} = s \leftarrow b = a \\ &(b, s) \setminus \{a\} = b, s \leftarrow b > a. \end{aligned}$$

First note that

$$\vdash_{\mathrm{PA}} Set(s) \to b \mathrel{\varepsilon} s \setminus \{a\} \leftrightarrow b \mathrel{\varepsilon} s \wedge b \neq a. \tag{3}$$

Property (3) is proved by list induction on s. The base case is straightforward. In the inductive case, when $s = c, s_1$, assume $Set(c, s_1)$ and consider three cases. If $c < a$ then we have

$$\begin{aligned}&b \mathrel{\varepsilon} (c, s_1) \setminus \{a\} \overset{\text{def}}{\Leftrightarrow} b \mathrel{\varepsilon} c, s_1 \setminus \{a\} \Leftrightarrow b = c \vee b \mathrel{\varepsilon} s_1 \setminus \{a\} \overset{\text{IH}}{\Leftrightarrow}\\ &b = c \vee b \mathrel{\varepsilon} s_1 \wedge b \neq a \Leftrightarrow b \mathrel{\varepsilon} c, s_1 \wedge b \neq a.\end{aligned}$$

If $c = a$ then, since $a \not\mathrel{\varepsilon} s_1$ by 12.5.2(4), we have

$$b \mathrel{\varepsilon} (a, s_1) \setminus \{a\} \overset{\text{def}}{\Leftrightarrow} b \mathrel{\varepsilon} s_1 \Leftrightarrow b \mathrel{\varepsilon} a, s_1 \wedge b \neq a.$$

If $c > a$ then $a \not\mathrel{\varepsilon} c, s_1$ by 12.5.2(3) and definition of $\prec$. We have

$$b \mathrel{\varepsilon} (c, s_1) \setminus \{a\} \overset{\text{def}}{\Leftrightarrow} b \mathrel{\varepsilon} c, s_1 \Leftrightarrow b \mathrel{\varepsilon} c, s_1 \wedge b \neq a.$$

As a simple consequence of (3) we get

$$Set(s) \wedge b < a \to b \prec s \setminus \{a\} \leftrightarrow b \prec s. \tag{4}$$

Property (1) is proved by list induction on s. The base case is straightforward. In the inductive case, when $s = b, s_1$, assume $Set(b, s_1)$ and consider three cases. If $b > a$ then the property trivially holds by definition. If $b = a$ then the property follows from 12.5.2(2). If $b < a$ then we have

$$\begin{aligned}&Set((b, s_1) \setminus \{a\}) \overset{\text{def}}{\Leftrightarrow} Set(b, s_1 \setminus \{a\}) \overset{12.5.2(2)}{\Leftrightarrow}\\ &Set(s_1 \setminus \{a\}) \wedge b \prec s_1 \setminus \{a\} \overset{(4)}{\Leftrightarrow} Set(s_1 \setminus \{a\}) \wedge b \prec s_1\end{aligned}$$

The last follows from IH and 12.5.2(2).

Property (2) is a straighforward consequence of 12.5.3(1), (1), and (3).

Polynomials

12.5.6 Polynomials. We will consider polynomials in one variable X with coefficients in $\mathbb{N}$. We say that a number p codes a polynomial $P(X)$:

$$P(X) \equiv \sum_{i=0}^{\infty} a_i \cdot X^i$$

if for every number i we have $(p)_i = a_i$.

The predicate $p \sim q$ holds if the numbers p and q code the same polynomial, ie

$$\vdash_{\mathrm{PAx}} p \sim q \leftrightarrow \forall i\,(p)_i = (q)_i .$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} p \sim p \tag{1}$$
$$\vdash_{\mathrm{PA}} p \sim q \to q \sim p \tag{2}$$
$$\vdash_{\mathrm{PA}} p \sim q \land q \sim r \to p \sim r \tag{3}$$
$$\vdash_{\mathrm{PA}} p \sim q \to a, p \sim a, q \tag{4}$$
$$\vdash_{\mathrm{PA}} a, p \sim b, q \leftrightarrow a = b \land p \sim q \tag{5}$$
$$\vdash_{\mathrm{PA}} a, p \sim 0 \leftrightarrow a = 0 \land p \sim 0. \tag{6}$$

The *denotation* function $p(x)$ takes the code p of a polynomial $P(X)$ and an assignment x and returns the value of $P(X)$ when the variable X takes x as its value. The function $p(x)$ is defined by list recursion on p as a primitive recursive function:

$$0(x) = 0$$
$$(a, p)(x) = a + x \cdot p(x).$$

The denotation function satisfies

$$p \sim q \leftrightarrow \forall x\, p(x) = q(x). \tag{7}$$

In the sequel we identify polynomials with their codes.

12.5.7 Addition of polynomials. The function $p \boldsymbol{+} q$ returns the addition of the polynomials p and q. The function satisfies

$$\vdash_{\mathrm{PA}} (p \boldsymbol{+} q)(x) = p(x) + q(x) \tag{1}$$
$$\vdash_{\mathrm{PA}} p \sim q \land r \sim s \to p \boldsymbol{+} r \sim q \boldsymbol{+} s \tag{2}$$

and it is defined by list recursion with substitution in parameter as a primitive recursive function:

$$0 \boldsymbol{+} q = q$$
$$(a, p) \boldsymbol{+} 0 = a, p$$
$$(a, p) \boldsymbol{+} (b, q) = a + b, p \boldsymbol{+} q.$$

Property $\forall q(1)$ is proved by list induction on p. In the base case we have

$$(0 \boldsymbol{+} q)(x) \stackrel{\mathrm{def}}{=} q(x) = 0 + q(x) = 0(x) + q(x).$$

In the inductive case when $p = a, p_1$ we consider two cases. If $q = 0$ then

$$((a, p_1) \boldsymbol{+} 0)(x) \stackrel{\mathrm{def}}{=} (a, p_1)(x) = (a, p_1)(x) + 0 = (a, p_1)(x) + 0(x).$$

If $q = b, q_1$ then we have

$$\begin{aligned} ((a, p_1) \boldsymbol{+} (b, q_1))(x) &\stackrel{\mathrm{def}}{=} ((a + b), p_1 \boldsymbol{+} q_1)(x) = (a + b) + x \cdot (p_1 \boldsymbol{+} q_1)(x) \stackrel{\mathrm{IH}}{=} \\ &= (a + b) + x \cdot (p_1(x) + q_1(x)) = (a + x \cdot p_1(x)) + (b + x \cdot q_1(x)) = \\ &= (a, p_1)(x) + (b, q_1)(x). \end{aligned}$$

12.5.8 Multiplication of polynomials by constants. The function $\overline{a} \times p$ computes the multiplication of the polynomial p by the constant a. The function satisfies

$$\vdash_{\mathrm{PA}} (\overline{a} \times p)(x) = a \cdot p(x) \tag{1}$$

$$\vdash_{\mathrm{PA}} p \sim q \rightarrow \overline{a} \times p \sim \overline{a} \times q \tag{2}$$

and it is defined by list recursion as a primitive recursive function:

$\overline{a} \times 0 = 0$
$\overline{a} \times (b, p) = a \cdot b, \overline{a} \times p.$

Both properties are proved by a straighforward list induction.

12.5.9 Multiplication of polynomials. The function $p \times q$ returns the multiplication of the polynomials p and q. The function satisfies

$$\vdash_{\mathrm{PA}} (p \times q)(x) = p(x) \cdot q(x) \tag{1}$$

$$\vdash_{\mathrm{PA}} p \sim q \wedge r \sim s \rightarrow p \times r \sim q \times s \tag{2}$$

and it is defined by list recursion as a primitive recursive function:

$0 \times q = 0$
$(a, p) \times q = \overline{a} \times q + (0, p \times q).$

Property (1) is proved by list induction on p. In the base case we have

$$(0 \times q)(x) \overset{\text{def}}{=} 0(x) = 0 = 0 \cdot q(x) = 0(x) \cdot q(x).$$

In the base case when $p = a, p_1$ we have

$$((a, p_1) \times q)(x) \overset{\text{def}}{=} (\overline{a} \times q + (0, p_1 \times q))(x) \overset{12.5.7(1)}{=}$$
$$= (\overline{a} \times q)(x) + (0, p_1 \times q)(x) = (\overline{a} \times q)(x) + x \cdot (p_1 \times q)(x) \overset{12.5.8(1)}{=}$$
$$= a \cdot q(x) + x \cdot (p_1 \times q)(x) \overset{\text{IH}}{=} a \cdot q(x) + x \cdot (p_1(x) \cdot q(x)) =$$
$$= (a + x \cdot p_1(x)) \cdot q(x) = (a, p_1)(x) \cdot q(x).$$

12.6 Exercises

12.6.1 Exercise. Prove

$$\vdash_{\mathrm{PA}} x \,\varepsilon\, y \leftrightarrow \exists z_1 \exists z_2\, y = z_1 \oplus (x, z_2). \tag{1}$$

12.6.2 Exercise. Prove

$$\vdash_{\mathrm{PA}} \mathit{Map}(x \oplus y) = \mathit{Map}(x) \oplus \mathit{Map}(y).$$

12.6.3 Exercise. Prove

$$\vdash_{\text{PA}} k \leq m \land m \leq n \to [k\,..\,m] \oplus [m+1\,..\,n] = [k\,..\,n].$$

12.6.4 Exercise. Prove

$$\vdash_{\text{PA}} \mathit{Combine}(\mathit{Ieven}(x), \mathit{Iodd}(x)) = x.$$

12.6.5 Exercise. Prove

$$\vdash_{\text{PA}} \mathit{Take}(L(x), x \oplus y) = x \tag{1}$$
$$\vdash_{\text{PA}} \mathit{Drop}(L(x), x \oplus y) = y \tag{2}$$
$$\vdash_{\text{PA}} n \leq L(x) \to x = \mathit{Take}(n,x) \oplus \mathit{Drop}(n,x) \tag{3}$$
$$\vdash_{\text{PA}} m+n \leq L(x) \to \mathit{Drop}(m+n,x) = \mathit{Drop}(n, \mathit{Drop}(m,x)). \tag{4}$$

12.6.6 Exercise. Prove

$$\vdash_{\text{PA}} x \neq 0 \land y \neq 0 \to \mathit{Minl}(x \oplus y) = \min(\mathit{Minl}(x), \mathit{Minl}(y))$$
$$\vdash_{\text{PA}} x \neq 0 \land y \neq 0 \to \mathit{Maxl}(x \oplus y) = \max(\mathit{Maxl}(x), \mathit{Maxl}(y)).$$

12.6.7 Exercise. Consider the function $s_1 \cup s_2$ defined by

$$\begin{aligned}
&0 \cup s_2 = s_2\\
&(a_1, s_1) \cup 0 = a_1, s_1\\
&(a_1, s_1) \cup (a_2, s_2) = a_1, s_1 \cup (a_2, s_2) \leftarrow a_1 < a_2\\
&(a_1, s_1) \cup (a_2, s_2) = a_1, s_1 \cup s_2 \leftarrow a_1 = a_2\\
&(a_1, s_1) \cup (a_2, s_2) = a_2, (a_1, s_1) \cup s_2 \leftarrow a_1 > a_2.
\end{aligned}$$

Prove

$$\vdash_{\text{PA}} \mathit{Set}(s_1) \land \mathit{Set}(s_2) \to \mathit{Set}(s_1 \cup s_2)$$
$$\vdash_{\text{PA}} \mathit{Set}(s_1) \land \mathit{Set}(s_2) \to a \in s_1 \cup s_2 \leftrightarrow a \in s_1 \lor a \in s_2.$$

12.6.8 Exercise. Consider the function $s_1 \setminus s_2$ defined by

$$\begin{aligned}
&0 \setminus s_2 = 0\\
&(a_1, s_1) \setminus 0 = a_1, s_1\\
&(a_1, s_1) \setminus (a_2, s_2) = a_1, s_1 \setminus (a_2, s_2) \leftarrow a_1 < a_2\\
&(a_1, s_1) \setminus (a_2, s_2) = s_1 \setminus s_2 \leftarrow a_1 = a_2\\
&(a_1, s_1) \setminus (a_2, s_2) = (a_1, s_1) \setminus s_2 \leftarrow a_1 > a_2.
\end{aligned}$$

Prove

$$\vdash_{\text{PA}} \mathit{Set}(s_1) \land \mathit{Set}(s_2) \to \mathit{Set}(s_1 \setminus s_2)$$
$$\vdash_{\text{PA}} \mathit{Set}(s_1) \land \mathit{Set}(s_2) \to a \in s_1 \setminus s_2 \leftrightarrow a \in s_1 \land a \notin s_2.$$

13. Programs Operating on Trees

13.1 Binary Trees

13.1.1 Arithmetization of labeled binary trees. We arithmetize *binary trees with labels in* $\mathbb{N}$ by two constructors:

$$E = 0,0$$
$$Nd(x,l,r) = 1,x,l,r.$$

The predicate $Bt(t)$ holding of codes of binary trees with labels in $\mathbb{N}$ is defined by course of values recursion as a primitive recursive predicate:

$$Bt(E)$$
$$Bt\,Nd(x,l,r) \leftarrow Bt(l) \land Bt(r).$$

We identify labeled binary trees with their codes and from now on we will say the *binary tree* t instead of the *code of the binary tree* t.

13.1.2 Case analysis on binary trees. We have the following principle of *case analysis on binary trees*:

$$\vdash_{\mathrm{PA}} Bt(t) \to t = E \lor \exists x \exists l \exists r\, t = Nd(x,l,r) \tag{1}$$

which is proved by a straightforward pair case analysis.

13.1.3 Structural induction on binary trees. The formula of *structural induction on the binary tree* t *for* $\phi[t]$ is the following one:

$$\phi[E] \land \forall x \forall l \forall r (\phi[l] \land \phi[r] \to \phi[Nd(x,l,r)]) \to Bt(t) \to \phi[t].$$

In the sequel we will often say shortly the *Bt-induction on* t instead of the structural induction on the binary tree t.

13.1.4 Theorem. *We have*

$$\vdash_{PA} \phi[E] \land \forall x \forall l \forall r (\phi[l] \land \phi[r] \to \phi[Nd(x,l,r)]) \to Bt(t) \to \phi[t].$$

Proof. The property is proved by complete induction on t. Take any t and under the assumptions of the claim consider two cases by 13.1.2(1). The case when $t = E$ is trivial. If $t = Nd(x,l,r)$ for some x,l,r then $\phi[l]$ and $\phi[r]$ by IH since $l < Nd(x,l,r)$ and $r < Nd(x,l,r)$. From this and assumptions we get $\phi[Nd(x,l,r)]$. $\square$

13.1.5 Structural recursion on binary trees. Initial clauses for clausal definitions with *structural recursion on binary trees* are of a form

$$f(\vec{y}, t, \vec{z}) = \alpha_1[\vec{y}, \vec{z}] \leftarrow t = E$$
$$f(\vec{y}, t, \vec{z}) = \alpha_2[\dot{\lambda}\vec{y}t\vec{z}.f(\vec{y}, l, \vec{z}), \dot{\lambda}\vec{y}t\vec{z}.f(\vec{y}, r, \vec{z}); \vec{y}, \vec{z}, x, l, r] \leftarrow t = Nd(x, l, r).$$

In the sequel we will often say shortly the *Bt-recursion on t* instead of the structural recursion on the binary tree t.

13.1.6 Membership in binary trees. The predicate $x \in_b t$ holds if x is a label of the binary tree t. The predicate is defined by Bt-recursion on t as a primitive recursive predicate:

$$x \in_b Nd(y, l, r) \leftarrow x = y$$
$$x \in_b Nd(y, l, r) \leftarrow x \neq y \land x \in_b l$$
$$x \in_b Nd(y, l, r) \leftarrow x \neq y \land x \notin_b l \land x \in_b r.$$

The predicate has the following easy to prove properties:

$$\vdash_{\text{PA}} x \notin_b E \tag{1}$$
$$\vdash_{\text{PA}} x \in_b Nd(y, l, r) \leftrightarrow x = y \lor x \in_b l \lor x \in_b r. \tag{2}$$

13.1.7 Size and depth of binary trees. The *size* function $|t|_b$ counts the number of labels in the binary tree t. The function is defined by Bt-recursion as a primitive recursive function:

$$|E|_b = 0$$
$$|Nd(x, l, r)|_b = |l|_b + |r|_b + 1.$$

The *depth* function $Dp(t)$ yields the length of the longest path from the root to a leaf in the binary tree t. The function is defined by Bt-recursion as a primitive recursive function:

$$Dp(E) = 0$$
$$Dp\,Nd(x, l, r) = \max(Dp(l), Dp(r)) + 1.$$

The functions satisfy

$$\vdash_{\text{PA}} Bt(t) \to |t|_b = 0 \leftrightarrow t = E \tag{1}$$
$$\vdash_{\text{PA}} Bt(t) \to Dp(t) = 0 \leftrightarrow t = E \tag{2}$$
$$\vdash_{\text{PA}} Bt(t) \to Dp(t) \leq |t|_b < 2^{Dp(t)}. \tag{3}$$

Properties (1) and (2) are straightforward. Property (3) is proved structural induction on the binary tree t. The base case is straightforward. In the inductive case when $t = Nd(x, l, r)$ we have

$$Dp\,Nd(x, l, r) \stackrel{\text{def}}{=} \max(Dp(l), Dp(r)) + 1 \stackrel{\text{IH}}{\leq} \max(|l|_b, |r|_b) + 1 =$$
$$= \max(|l|_b + 1, |r|_b + 1) \stackrel{\text{IH}}{\leq} \max(2^{Dp(l)}, 2^{Dp(r)}) = 2^{\max(Dp(l), Dp(r))} <$$
$$< 2^{\max(Dp(l), Dp(r))+1} \stackrel{\text{def}}{=} 2^{Dp\,Nd(x, l, r)}.$$

13.1.8 Reflection function. The *reflection* function $\mathit{Reflect}(t)$ yields the mirror image of the binary tree t by recursively exchanging left and right subtrees. The function is defined by Bt-recursion as a primitive recursive function:

$$\mathit{Reflect}(E) = E$$
$$\mathit{Reflect}\, \mathit{Nd}(x,l,r) = \mathit{Nd}(x, \mathit{Reflect}(r), \mathit{Reflect}(l)).$$

The function satisfies

$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow Bt\, \mathit{Reflect}(t) \tag{1}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow x \in_b \mathit{Reflect}(t) \leftrightarrow x \in_b t \tag{2}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow |\mathit{Reflect}(t)|_b = |t|_b \tag{3}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \mathit{Dp}\, \mathit{Reflect}(t) = \mathit{Dp}(t) \tag{4}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \mathit{Reflect}\, \mathit{Reflect}(t) = t \tag{5}$$
$$\vdash_{\mathrm{PA}} Bt(t_1) \wedge Bt(t_2) \wedge \mathit{Reflect}(t_1) = \mathit{Reflect}(t_2) \rightarrow t_1 = t_2 \tag{6}$$
$$\vdash_{\mathrm{PA}} Bt(t_1) \rightarrow \exists t_2\, \mathit{Reflect}(t_2) = t_1. \tag{7}$$

Property (1) is proved by a straightforward Bt-induction. Property (2) is proved by Bt-induction. The base is straightforward and in the inductive case when $t = \mathit{Nd}(y,l,r)$ we have

$$x \in_b \mathit{Reflect}\, \mathit{Nd}(y,l,r) \overset{\text{def}}{\Leftrightarrow} x \in_b \mathit{Nd}(y, \mathit{Reflect}(r), \mathit{Reflect}(l)) \overset{13.1.6(2)}{\Leftrightarrow}$$
$$x = y \vee x \in_b \mathit{Reflect}(r) \vee x \in_b \mathit{Reflect}(l) \overset{\text{IH}}{\Leftrightarrow} x = y \vee x \in_b r \vee x \in_b l \overset{13.1.6(2)}{\Leftrightarrow}$$
$$x \in_b \mathit{Nd}(y,l,r).$$

Properties (3) and (4) are proved by a straightforward Bt-induction. Property (5) is proved by Bt-induction. The base is straightforward and in the inductive case we have

$$\mathit{Reflect}\, \mathit{Reflect}\, \mathit{Nd}(x,l,r) \overset{\text{def}}{=} \mathit{Reflect}\, \mathit{Nd}(x, \mathit{Reflect}(r), \mathit{Reflect}(l)) \overset{\text{def}}{=}$$
$$= \mathit{Nd}(x, \mathit{Reflect}\, \mathit{Reflect}(l), \mathit{Reflect}\, \mathit{Reflect}(r)) \overset{\text{IH}}{=} \mathit{Nd}(x,l,r).$$

Properties (6) and (7) follows from (5).

13.1.9 Traversals of binary trees. The functions $\mathit{Preorder}(t)$, $\mathit{Inorder}(t)$, and $\mathit{Postorder}(t)$ collect the labels of a binary tree t into a list in the order corresponding respectively to the preorder, inorder, and postorder traversal of the binary tree t. The functions are defined by Bt-recursion as primitive recursive functions:

$$\mathit{Preorder}(E) = 0$$
$$\mathit{Preorder}\, \mathit{Nd}(x,l,r) = (x,0) \oplus \mathit{Preorder}(l) \oplus \mathit{Preorder}(r)$$

$$Inorder(E) = 0$$
$$Inorder\,Nd(x,l,r) = Inorder(l) \oplus (x,0) \oplus Inorder(r)$$

$$Postorder(E) = 0$$
$$Postorder\,Nd(x,l,r) = Postorder(l) \oplus Postorder(r) \oplus (x,0).$$

The following are the basic properties of the traversal functions:

$$\vdash_{\mathrm{PA}} Bt(t) \to L\,Preorder(t) = |t|_b \tag{1}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to x \mathrel{\varepsilon} Preorder(t) \leftrightarrow x \in_b t \tag{2}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to L\,Inorder(t) = |t|_b \tag{3}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to x \mathrel{\varepsilon} Inorder(t) \leftrightarrow x \in_b t \tag{4}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to L\,Postorder(t) = |t|_b \tag{5}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to x \mathrel{\varepsilon} Postorder(t) \leftrightarrow x \in_b t. \tag{6}$$

Property (1) is proved by Bt-induction. The base case is straighforward and in the inductive case we have

$$L\,Preorder\,Nd(x,l,r) \stackrel{\text{def}}{=} L((x,0) \oplus Preorder(l) \oplus Preorder(t)) \stackrel{12.1.9(8)}{=}$$
$$= L\,Preorder(l) + L\,Preorder(r) + 1 \stackrel{\text{IH}}{=} |l|_b + |r|_b + 1 = |Nd(x,l,r)|_b.$$

Property (2) is proved by Bt-induction on t. The base case is straighforward and in the inductive case when $t = Nd(y,l,r)$ we have

$$x \mathrel{\varepsilon} Preorder\,Nd(y,l,r) \stackrel{\text{def}}{\Leftrightarrow} x \mathrel{\varepsilon} (y,0) \oplus Preorder(l) \oplus Preorder(t) \Leftrightarrow$$
$$x = y \lor x \mathrel{\varepsilon} Preorder(l) \lor x \mathrel{\varepsilon} Preorder(r) \stackrel{\text{IH}}{\Leftrightarrow} x = y \lor x \in_b l \lor x \in_b r \stackrel{13.1.6(2)}{\Leftrightarrow}$$
$$x \in_b Nd(y,l,r).$$

The remaining properties are proved similarly.

The relationship between the preorder and postorder traversals is captured by the following properties:

$$\vdash_{\mathrm{PA}} Bt(t) \to Preorder(t) = Rev\,Postorder\,Reflect(t) \tag{7}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to Postorder(t) = Rev\,Preorder\,Reflect(t). \tag{8}$$

Property (7) is proved by Bt-induction. The base case is straightforward and in the inductive case we have

$$Rev\,Postorder\,Reflect\,Nd(x,l,r) =$$
$$= Rev\,Postorder\,Nd(x, Reflect(r), Reflect(l)) \stackrel{\text{def}}{=}$$
$$= Rev(Postorder\,Reflect(r) \oplus Postorder\,Reflect(l) \oplus (x,0)) \stackrel{12.1.13(2)}{=}$$
$$= (x,0) \oplus Rev\,Postorder\,Reflect(l) \oplus Rev\,Postorder\,Reflect(r) \stackrel{\text{IH}}{=}$$
$$= (x,0) \oplus Preorder(l) \oplus Preorder(r) \stackrel{\text{def}}{=} Preorder\,Nd(x,l,r).$$

Property (8) is proved similarly.

13.1.10 Fast programs for tree traversals. We can save the repeated concatenation in the definitions of the tree traversal functions by keeping the labels in an accumulator. For instance, in case of preorder traversal, we define a binary *accumulator* function $f(t,a)$ by nested Bt-recursion on t:

$$\begin{aligned}&f(E,a) = a\\ &f(Nd(x,l,r),a) = x, f(l, f(r,a))\end{aligned}$$

and then take the following property as an alternative definition of preorder traversal:

$$\vdash_{\mathrm{PA}} \; Bt(t) \rightarrow \mathit{Preorder}(t) = f(t,0). \tag{1}$$

In order to see this we need the following property of f:

$$\vdash_{\mathrm{PA}} \; Bt(t) \rightarrow \forall a\, f(t,a) = \mathit{Preorder}(t) \oplus a \tag{2}$$

which is proved Bt-induction. The base case is straightforward. In the inductive case when $t = Nd(x,l,r)$ take any a and we have

$$\begin{aligned}f(Nd(x,l,r),a) &\stackrel{\text{def}}{=} x, f(l, f(r,a)) \stackrel{\text{IH}}{=} x, f(l, \mathit{Preorder}(r) \oplus a) \stackrel{\text{IH}}{=}\\ &= x, \mathit{Preorder}(l) \oplus \mathit{Preorder}(r) \oplus a = \mathit{Preorder}\; Nd(x,l,r) \oplus a.\end{aligned}$$

13.1.11 Tail recursive tree traversals. We can find a tail recursive implementation of preorder traversal (and similarly for inorder and postorder traversals) with the help of the binary function $f(s,a)$ defined by

$$\begin{aligned}&f(0,a) = a\\ &f((E,s),a) = f(s,a)\\ &f((Nd(x,l,r),s),a) = f((r,l,\mathit{Label}(x),s),a)\\ &f((\mathit{Label}(x),s),a) = f(s,x,a),\end{aligned}$$

where $\mathit{Label}(x) = 2, x$ is an auxiliary constructor. Note that this is a definition by course of values recursion with measure $m(s,a)$:

$$\begin{aligned}&m_1(E) = 1\\ &m_1\; Nd(x,l,r) = m_1(l) + m_1(r) + 2\\ &m_1\; \mathit{Label}(x) = 1\end{aligned}$$

$$\begin{aligned}&m(0,a) = 0\\ &m((t,s),a) = m_1(t) + m(s,a).\end{aligned}$$

We can express the relation between *Preorder* and f by

$$\vdash_{\mathrm{PA}} \; Bt(t) \rightarrow \mathit{Preorder}(t) = f((t,0),0). \tag{1}$$

First note that the function f satisfies:

$$\vdash_{\mathrm{PA}} \; Bt(t) \rightarrow \forall s \forall a\, f((t,s),a) = f(s, \mathit{Preorder}(t) \oplus a). \tag{2}$$

Property (2) is proved by Bt-induction. In the base case take any s and a. We have

$$f((E,s),a) \stackrel{\text{def}}{=} f(s,a) = f(s, 0 \oplus a) \stackrel{\text{def}}{=} f(s, \mathit{Preorder}(E) \oplus a).$$

In the inductive case when $t = \mathit{Nd}(x,l,r)$ take any s and a. We have

$$\begin{aligned} & f((\mathit{Nd}(x,l,r),s),a) \stackrel{\text{def}}{=} f((r,l,\mathit{Label}(x),s),a) \stackrel{\text{IH}}{=} \\ & \quad = f((l,\mathit{Label}(x),s),\mathit{Preorder}(r) \oplus a) \stackrel{\text{IH}}{=} \\ & \quad = f((\mathit{Label}(x),s),\mathit{Preorder}(l) \oplus \mathit{Preorder}(r) \oplus a) \stackrel{\text{def}}{=} \\ & \quad = f(s,x,\mathit{Preorder}(l) \oplus \mathit{Preorder}(r) \oplus a) = \\ & \quad = f(s,\mathit{Preorder}\ \mathit{Nd}(x,l,r) \oplus a). \end{aligned}$$

We are now in position to prove (1). Assume $Bt(t)$. We have

$$f((t,0),0) \stackrel{(2)}{=} f(0,\mathit{Preorder}(t) \oplus 0) = f(0,\mathit{Preorder}(t)) \stackrel{\text{def}}{=} \mathit{Preorder}(t).$$

13.1.12 Subtree relation. The predicate $t_1 \trianglelefteq_b t_2$ holds if the binary tree t_1 is a subtree of the binary tree t_2. The predicate is defined by Bt-recursion on t_2 as a primitive recursive predicate:

$t_1 \trianglelefteq_b t_2 \leftarrow t_1 = t_2$
$t_1 \trianglelefteq_b t_2 \leftarrow t_1 \neq t_2 \land t_2 = \mathit{Nd}(x_2,l_2,r_2) \land t_1 \trianglelefteq_b l_2$
$t_1 \trianglelefteq_b t_2 \leftarrow t_1 \neq t_2 \land t_2 = \mathit{Nd}(x_2,l_2,r_2) \land t_1 \ntrianglelefteq_b l_2 \land t_1 \trianglelefteq_b r_2.$

The predicate has the following easy to prove properties:

$$\vdash_{\text{PA}} t \trianglelefteq_b E \leftrightarrow t = E \tag{1}$$
$$\vdash_{\text{PA}} t \trianglelefteq_b \mathit{Nd}(x,l,r) \leftrightarrow t = \mathit{Nd}(x,l,r) \lor t \trianglelefteq_b l \lor t \trianglelefteq_b r. \tag{2}$$

13.1.13 Isomorphic binary trees. The predicate $t_1 \simeq_b t_2$ holds if the binary trees t_1 and t_2 are isomorphic. The predicate is defined by Bt-recursion on t_1 with substitution in parameter t_2 as a primitive recursive predicate:

$E \simeq_b E$
$\mathit{Nd}(x_1,l_1,r_1) \simeq_b \mathit{Nd}(x_2,l_2,r_2) \leftarrow l_1 \simeq_b l_2 \land r_1 \simeq_b r_2.$

The predicate satisfies

$$\vdash_{\text{PA}} Bt(t) \to t \simeq_b t \tag{1}$$
$$\vdash_{\text{PA}} Bt(t_1) \land Bt(t_2) \land t_1 \simeq_b t_2 \to t_2 \simeq_b t_1 \tag{2}$$
$$\vdash_{\text{PA}} Bt(t_1) \land Bt(t_2) \land Bt(t_3) \land t_1 \simeq_b t_2 \land t_2 \simeq_b t_3 \to t_1 \simeq_b t_3 \tag{3}$$
$$\vdash_{\text{PA}} Bt(t_1) \land Bt(t_2) \land t_1 \simeq_b t_2 \to |t_1|_b = |t_2|_b \tag{4}$$
$$\vdash_{\text{PA}} Bt(t_1) \land Bt(t_2) \land t_1 \simeq_b t_2 \to \mathit{Dp}(t_1) = \mathit{Dp}(t_2) \tag{5}$$
$$\vdash_{\text{PA}} Bt(t_1) \land Bt(t_2) \to \mathit{Reflect}(t_1) \simeq_b \mathit{Reflect}(t_2) \leftrightarrow t_1 \simeq_b t_2. \tag{6}$$

UNFINISHED

13.1.14 Counting the labels in binary trees. The function $\#_b(x,t)$ counts the number of occurrences of the label x in the binary tree t. The function is defined by Bt-recursion on t as a primitive recursive function:

$$\begin{aligned}
&\#_b(x,E) = 0\\
&\#_b(x,Nd(y,l,r)) = \#_b(x,l) + \#_b(x,r) + 1 \leftarrow x = y\\
&\#_b(x,Nd(y,l,r)) = \#_b(x,l) + \#_b(x,r) \leftarrow x \neq y.
\end{aligned}$$

The function satisfies:

$$\vdash_{\mathrm{PA}} \#_b(x,Nd(y,l,r)) = \#_b(x,l) + \#_b(x,r) + (x =_* y) \tag{1}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,t) > 0 \leftrightarrow x \in_b t \tag{2}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,t) \leq |t|_b \tag{3}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,t) = |t|_b \leftrightarrow \forall y(y \in_b t \rightarrow y = x) \tag{4}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,\mathit{Reflect}(t)) = \#_b(x,t) \tag{5}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,t) = \#(x,\mathit{Preorder}(t)) \tag{6}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,t) = \#(x,\mathit{Inorder}(t)) \tag{7}$$
$$\vdash_{\mathrm{PA}} Bt(t) \rightarrow \#_b(x,t) = \#(x,\mathit{Postorder}(t)) \tag{8}$$
$$\vdash_{\mathrm{PA}} Bt(t_1) \wedge Bt(t_2) \wedge t_1 \trianglelefteq_b t_2 \rightarrow \#_b(x,t_1) \leq \#_b(x,t_2). \tag{9}$$

Property (1) is straightforward. Property (4) is proved by Bt-induction on t as follows. **UNFINISHED**

Property (9) is proved by Bt-induction on t_2. The remaining properties are proved by a straightforward Bt-induction on t.

13.2 Binary Search Trees

13.2.1 Tree comparision predicates. The predicate $x \prec t$ holds if x is a strict lower bound of the labels of the binary tree t, i.e.

$$\vdash_{\mathrm{PAx}} x \prec t \leftrightarrow \forall y(y \in_b t \rightarrow x < y).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} x \prec E \tag{1}$$
$$\vdash_{\mathrm{PA}} x \prec Nd(y,l,r) \leftrightarrow x < y \wedge x \prec l \wedge x \prec r \tag{2}$$
$$\vdash_{\mathrm{PA}} x \leq y \wedge y \prec t \rightarrow x \prec t. \tag{3}$$

The predicate $x \succ t$ holds if x is a strict upper bound of the labels of the binary tree t, i.e.

$$\vdash_{\mathrm{PAx}} x \succ t \leftrightarrow \forall y(y \in_b t \rightarrow x > y).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} x \succ E \tag{4}$$
$$\vdash_{\mathrm{PA}} x \succ Nd(y,l,r) \leftrightarrow x > y \land x \succ l \land x \succ r \tag{5}$$
$$\vdash_{\mathrm{PA}} x \geq y \land y \succ t \rightarrow x \succ t. \tag{6}$$

The predicate $t_1 \prec_b t_2$ holds if the labels of the binary tree t_1 are strictly less than the labels of the binary tree t_2, i.e.

$$\vdash_{\mathrm{PAx}} t_1 \prec_b t_2 \leftrightarrow \forall x_1 \forall x_2 (x_1 \in_b t_1 \land x_2 \in_b t_2 \rightarrow x_1 < x_2).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} E \prec_b t_2 \tag{7}$$
$$\vdash_{\mathrm{PA}} Nd(x_1,l_1,r_1) \prec_b t_2 \leftrightarrow x_1 \prec t_2 \land l_1 \prec_b t_2 \land r_1 \prec_b t_2 \tag{8}$$
$$\vdash_{\mathrm{PA}} t_1 \prec_b E \tag{9}$$
$$\vdash_{\mathrm{PA}} t_1 \prec_b Nd(x_2,l_2,r_2) \leftrightarrow x_2 \succ t_1 \land t_1 \prec_b l_2 \land t_1 \prec_b r_2 \tag{10}$$
$$\vdash_{\mathrm{PA}} t_1 \prec_b t_2 \land x \in_b t_1 \rightarrow x \prec t_2 \tag{11}$$
$$\vdash_{\mathrm{PA}} t_1 \prec_b t_2 \land x \in_b t_2 \rightarrow x \succ t_1 \tag{12}$$
$$\vdash_{\mathrm{PA}} x \succ t_1 \land x \prec t_2 \rightarrow t_1 \prec_b t_2. \tag{13}$$

13.2.2 Binary search trees. The predicate $Bst(t)$ holds if t is a binary tree satisfying the following *search condition*:

> for every nonempty subtree of t each label of its left (right) son is strictly less (greater) than its root label.

The predicate is defined by

$$\vdash_{\mathrm{PAx}} Bst(t) \leftrightarrow Bt(t) \land \forall x \forall l \forall r (Nd(x,l,r) \trianglelefteq_b t \rightarrow x \succ l \land x \prec r).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} Bst(E) \tag{1}$$
$$\vdash_{\mathrm{PA}} Bst\, Nd(x,l,r) \leftrightarrow x \succ l \land x \prec r \land Bst(l) \land Bst(r) \tag{2}$$
$$\vdash_{\mathrm{PA}} Bst\, Nd(x,l,r) \land y \leq x \rightarrow y \notin_b r \tag{3}$$
$$\vdash_{\mathrm{PA}} Bst\, Nd(x,l,r) \land y \geq x \rightarrow y \notin_b l. \tag{4}$$
$$\vdash_{\mathrm{PA}} Bst\, Nd(x,l,r) \rightarrow l \prec_b r. \tag{5}$$

13.2.3 Membership in binary search trees. The predicate $x \in t$ holds if x is a label of the binary search tree t. The predicate satisfies

$$\vdash_{\mathrm{PA}} Bst(t) \rightarrow x \in t \leftrightarrow x \in_b t \tag{1}$$

and it is defined by Bt-recursion on t as a primitive recursive predicate:

$x \in Nd(y,l,r) \leftarrow x < y \land x \in l$
$x \in Nd(y,l,r) \leftarrow x = y$
$x \in Nd(y,l,r) \leftarrow x > y \land x \in r.$

Property (1) is proved by Bt-induction on t. The base is straightforward. In the inductive case, when $t = Nd(y,l,r)$, assume $Bst(t)$, and consider three cases. If $x < y$ then we have

$$x \in Nd(y,l,r) \overset{\text{def}}{\Leftrightarrow} x \in l \overset{\text{IH}}{\Leftrightarrow} x \in_b l \overset{13.2.2(3)}{\Leftrightarrow}$$
$$x = y \lor x \in_b l \lor x \in_b r \overset{13.1.6(2)}{\Leftrightarrow} x \in_b Nd(y,l,r).$$

The case when $x = y$ is trivial and the case when $x > y$ is proved similarly.

13.2.4 Insertion in binary search trees. The function $t \cup \{x\}$ takes a binary search tree t and inserts x into it. The function satisfies

$$\vdash_{\mathrm{PA}} Bst(t) \to Bst(t \cup \{x\}) \tag{1}$$
$$\vdash_{\mathrm{PA}} Bst(t) \to y \in t \cup \{x\} \leftrightarrow y \in t \lor y = x \tag{2}$$

and it is defined by Bt-recursion on t as a primitive recursive function:

$$\begin{aligned}
&E \cup \{x\} = Nd(x,E,E)\\
&Nd(y,l,r) \cup \{x\} = Nd(y,l,r \cup \{x\}) \leftarrow y < x\\
&Nd(y,l,r) \cup \{x\} = Nd(y,l,r) \leftarrow y = x\\
&Nd(y,l,r) \cup \{x\} = Nd(y,l \cup \{x\},r) \leftarrow y > x.
\end{aligned}$$

First note that

$$\vdash_{\mathrm{PA}} Bt(t) \to y \in_b t \cup \{x\} \leftrightarrow y \in_b t \lor y = x. \tag{3}$$

Property (3) is proved by Bt-induction on t. The base case is straightforward. In the inductive case, when $t = Nd(z,l,r)$, assume $Bt\,Nd(z,l,r)$ and consider three cases. If $z < x$ then we have

$$y \in_b Nd(z,l,r) \cup \{x\} \overset{\text{def}}{\Leftrightarrow} y \in_b Nd(z,l,r \cup \{x\}) \overset{13.1.6(2)}{\Leftrightarrow}$$
$$y = z \lor y \in_b l \lor y \in_b r \cup \{x\} \overset{\text{IH}}{\Leftrightarrow} y = z \lor y \in_b l \lor y \in_b r \lor y = x \overset{13.1.6(2)}{\Leftrightarrow}$$
$$y \in_b Nd(z,l,r) \lor y = x.$$

The case when $z = x$ is trivial and the case when $z > x$ is proved similarly. As a simple consequence of (3) we get

$$\vdash_{\mathrm{PA}} Bt(t) \to y \prec t \cup \{x\} \leftrightarrow y \prec t \land y < x \tag{4}$$
$$\vdash_{\mathrm{PA}} Bt(t) \to y \succ t \cup \{x\} \leftrightarrow y \succ t \land y > x. \tag{5}$$

Property (1) is proved by Bt-induction on t. The base case is straightforward. In the inductive case when $t = Nd(y,l,r)$ we consider three cases. If $y < x$ then we have

$$Bst(Nd(y,l,r) \cup \{x\}) \overset{\text{def}}{\Leftrightarrow} Bst\,Nd(y,l,r \cup \{x\}) \overset{13.2.2(2)}{\Leftrightarrow}$$
$$y \succ l \land y \prec r \cup \{x\} \land Bst(l) \land Bst(r \cup \{x\}) \overset{(4)}{\Leftrightarrow}$$
$$y \succ l \land y \prec r \land Bst(l) \land Bst(r \cup \{x\}).$$

The last follows from IH and assumptions by 13.2.2(2). The case when $y = x$ is trivial and the case when $y > x$ is proved similarly.

Property (2) is a straighforward consequence of 13.2.3(1), (1), and (3).

13.2.5 Deletion in binary search trees. The function $t \setminus \{x\}$ takes a binary search tree t and a number x and yields a new binary search tree obtained from t by deleting x from it. The function satitisfies

$$\vdash_{\mathrm{PA}} Bst(t) \to Bst(t \setminus \{x\}) \tag{1}$$

$$\vdash_{\mathrm{PA}} Bst(t) \to y \in t \setminus \{x\} \leftrightarrow y \in t \wedge y \neq x \tag{2}$$

and it is defined by Bt-recursion on t as a primitive recursive function:

$$E \sqcup t_2 = t_2$$
$$Nd(x_1, l_1, r_1) \sqcup t_2 = Nd(x_1, l_1, r_1 \sqcup t_2)$$

$$E \setminus \{x\} = E$$
$$Nd(y, l, r) \setminus \{x\} = Nd(y, l, r \setminus \{x\}) \leftarrow y < x$$
$$Nd(y, l, r) \setminus \{x\} = l \sqcup r \leftarrow y = x$$
$$Nd(y, l, r) \setminus \{x\} = Nd(y, l \setminus \{x\}, r) \leftarrow y > x.$$

The auxiliary function $t_1 \sqcup t_2$ satisfies

$$\vdash_{\mathrm{PA}} Bt(t_1) \to x \in_b t_1 \sqcup t_2 \leftrightarrow x \in_b t_1 \vee x \in_b t_2 \tag{3}$$

$$\vdash_{\mathrm{PA}} Bt(t_1) \to x \prec t_1 \sqcup t_2 \leftrightarrow x \prec t_1 \wedge x \prec t_2 \tag{4}$$

$$\vdash_{\mathrm{PA}} Bst(t_1) \wedge Bst(t_2) \wedge t_1 \prec_b t_2 \to Bst(t_1 \sqcup t_2). \tag{5}$$

Property (3) is proved by a straightforward Bt-induction on t_1. Property (4) is a simple consequence of (3). Property (5) is proved by Bt-induction on t_1 with the help of (4).

Note that

$$\vdash_{\mathrm{PA}} Bst(t) \to y \in_b t \setminus \{x\} \leftrightarrow y \in_b t \wedge y \neq x. \tag{6}$$

Property (6) is proved by Bt-induction on t. The base case is straightforward. In the inductive case when $t = Nd(z, l, r)$ we consider three cases. If $z < x$ then we have

$$y \in_b Nd(z, l, r) \setminus \{x\} \overset{\text{def}}{\Leftrightarrow} y \in_b Nd(z, l, r \setminus \{x\}) \overset{13.1.6(2)}{\Leftrightarrow}$$
$$y = z \vee y \in_b l \vee y \in_b r \setminus \{x\} \overset{\text{IH}}{\Leftrightarrow} y = z \vee y \in_b l \vee y \in_b r \wedge y \neq x \overset{(*)}{\Leftrightarrow}$$
$$(y = z \vee y \in_b l \vee y \in_b r) \wedge y \neq x \overset{13.1.6(2)}{\Leftrightarrow} y \in_b Nd(z, l, r) \wedge y \neq x.$$

The step marked by $(*)$ follows by a simple case analysis on $y = x$ and $y \neq x$ by noting that we have $x \notin_b l$ by 13.2.2(3). The case when $z = x$ follows from (3) by similar arguments. The case when $z > x$ is left to the reader.

As a simple consequence of (6) we get

$$\vdash_{\mathrm{PA}} Bst(t) \land y < x \to y \prec t \setminus \{x\} \leftrightarrow y \prec t \tag{7}$$
$$\vdash_{\mathrm{PA}} Bst(t) \land y > x \to y \succ t \setminus \{x\} \leftrightarrow y \succ t. \tag{8}$$

Property (1) is proved by Bt-induction on t. The base case is straightforward. In the inductive case when $t = Nd(y,l,r)$ we consider three cases. If $y < x$ then we have

$$Bst(Nd(y,l,r) \setminus \{x\}) \overset{\text{def}}{\Leftrightarrow} Bst\,Nd(y,l,r \setminus \{x\}) \overset{13.2.2(2)}{\Leftrightarrow}$$
$$y \succ l \land y \prec r \setminus \{x\} \land Bst(l) \land Bst(r \setminus \{x\}) \overset{(7)}{\Leftrightarrow}$$
$$y \succ l \land y \prec r \land Bst(l) \land Bst(r \setminus \{x\}).$$

The last follows from IH and assumptions by 13.2.2(2). If $y = x$ then the claim follows from 13.2.2(5) and (5). The case when $y > x$ is proved similarly.

Property (2) is a straighforward consequence of 13.2.3(1), (1), and (6).

13.3 Perfectly Balanced Binary Trees

13.3.1 Perfectly (size) balanced binary trees. The predicate $Pbt(t)$ holds if t is a binary tree satisfying the following *(size) balanced condition*:

> for every nonempty subtree of t the size of its left son is at most one more than the size of its right son.

The predicate is defined by

$$\vdash_{\mathrm{PAx}} Pbt(t) \leftrightarrow Bt(t) \land \forall x \forall l \forall r (Nd(x,l,r) \trianglelefteq_b t \to |l|_b = |r|_b \lor |l|_b = |r|_b + 1).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} Pbt(E) \tag{1}$$
$$\vdash_{\mathrm{PA}} Pbt\,Nd(x,l,r) \leftrightarrow (|l|_b = |r|_b \lor |l|_b = |r|_b + 1) \land Pbt(l) \land Pbt(r) \tag{2}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \to 2^{Dp(t)} \div 2 \leq |t|_b < 2^{Dp(t)} \tag{3}$$
$$\vdash_{\mathrm{PA}} Pbt(t_1) \land Pbt(t_2) \to t_1 \simeq_b t_2 \leftrightarrow |t_1|_b = |t_2|_b. \tag{4}$$

Properties (1) and (2) are straightforward. The sharp inequality in (3) follows from 13.1.7(3). The non-sharp inequality is proved by Bt-induction on t. Property $\forall t_2(4)$ is proved by Bt-induction on t_1. The base case is straightforward. In the inductive case when $t_1 = Nd(x_1, l_1, r_1)$ take any t_2 and under the assumptions of the claim we have $t_2 = Nd(x_2, l_2, r_2)$ for some x_2, l_2, and r_2. We obtain

$$Nd(x_1,l_1,r_1) \simeq_b Nd(x_2,l_2,r_2) \Leftrightarrow l_1 \simeq_b l_2 \wedge r_1 \simeq_b r_2 \overset{\mathrm{IH}}{\Leftrightarrow}$$
$$|l_1|_b = |l_2|_b \wedge |r_1|_b = |r_2|_b \overset{(*)}{\Leftrightarrow} |l_1|_b + |r_1|_b = |l_2|_b + |r_2|_b \Leftrightarrow$$
$$|Nd(x_1,l_1,r_1)|_b = |Nd(x_2,l_2,r_2)|_b.$$

The step marked by $(*)$ follows from (2).

13.3.2 Fast indexing in perfectly balanced binary trees. The application $t[i]$ yields the i-th label of the perfectly balanced binary tree t. The function is defined by dyadic recursion on i with substitution in parameter as a primitive recursive function:

$$Nd(x,l,r)[0] = x$$
$$Nd(x,l,r)[i\mathbf{1}] = l[i]$$
$$Nd(x,l,r)[i\mathbf{2}] = r[i].$$

13.3.3 Fast modification in perfectly balanced binary trees. The function $t[i := y]$ modifies the perfectly balanced tree t at the index i to obtain a new value y. The function satisfies

$$\vdash_{\mathrm{PA}} Pbt(t) \wedge i < |t|_b \to |t[i := y]|_b = |t|_b \tag{1}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \wedge i < |t|_b \to Pbt(t[i := y]) \tag{2}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \wedge i < |t|_b \to t[i := y][i] = y \tag{3}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \wedge i < |t|_b \wedge j < |t|_b \wedge j \neq i \to t[i := y][j] = t[j] \tag{4}$$

and it is defined by dyadic recursion on i with substitution in parameter t as a primitive recursive function:

$$Nd(x,l,r)[0 := y] = Nd(y,l,r)$$
$$Nd(x,l,r)[i\mathbf{1} := y] = Nd(x,l[i := y],r)$$
$$Nd(x,l,r)[i\mathbf{2} := y] = Nd(x,l,r[i := y]).$$

First note that under the assumptions $Pbt(t)$ and $i < |t|_b$ we have $t = Nd(x,l,r)$ for some x, l, and r, and thus

$$i < |Nd(x,l,r)|_b = |l|_b + |r|_b + 1. \tag{5}$$

Property $\forall t(1)$ is proved by dyadic induction on i. In the base case we have

$$|Nd(x,l,r)[0 := y]|_b \overset{\mathrm{def}}{=} |Nd(y,l,r)|_b = |l|_b + |r|_b + 1 = |Nd(x,l,r)|_b.$$

In the inductive case when $i = j\mathbf{1}$ we have $j < |l|_b$ by 13.3.1(2) and (5). We get

$$|Nd(x,l,r)[j\mathbf{1} := y]|_b \overset{\mathrm{def}}{=} |Nd(x,l[j := y],r)|_b = |l[j := y]|_b + |r|_b + 1 \overset{\mathrm{IH}}{=}$$
$$= |l|_b + |r|_b + 1 = |Nd(x,l,r)|_b.$$

The inductive case when $i = j\mathbf{2}$ has a similar proof.

Property $\forall t(2)$ is proved by dyadic induction on i. The base case is straightforward. In the inductive case when $i = j\mathbf{1}$ we have $j < |l|_b$ by 13.3.1(2) and (5). We get

$$Pbt(Nd(x,l,r)[j\mathbf{1} := y]) \overset{\text{def}}{\Leftrightarrow} Pbt\, Nd(x,l[j := y],r) \overset{13.3.1(2)}{\Leftrightarrow}$$
$$(|l[j := y]|_b = |r|_b \lor |l[j := y]|_b = |r|_b + 1) \land Pbt(l[j := y]) \land Pbt(r) \overset{(1)}{\Leftrightarrow}$$
$$(|l|_b = |r|_b \lor |l|_b = |r|_b + 1) \land Pbt(l[j := y]) \land Pbt(r) \overset{\text{IH}}{\Leftrightarrow}$$
$$(|l|_b = |r|_b \lor |l|_b = |r|_b + 1) \land Pbt(l) \land Pbt(r) \overset{13.3.1(2)}{\Leftrightarrow} Pbt\, Nd(x,l,r).$$

The inductive case when $i = j\mathbf{2}$ has a similar proof.

Property $\forall t(3)$ is proved by dyadic induction on i. In the base case we have

$$Nd(x,l,r)[0 := y][0] \overset{\text{def}}{=} Nd(y,l,r)[0] = y.$$

In the inductive case when $i = j\mathbf{1}$ we have $j < |l|_b$ by 13.3.1(2) and (5). We get

$$Nd(x,l,r)[j\mathbf{1} := y][j\mathbf{1}] \overset{\text{def}}{=} Nd(x,l[j := y],r)[j\mathbf{1}] = l[j := y][j] \overset{\text{IH}}{=} y.$$

The inductive case when $i = j\mathbf{2}$ has a similar proof.

Property $\forall t \forall j(4)$ is proved by dyadic induction on i. In the base case when $i = 0$ take any $j \neq 0$ and consider two subcases. If $j = k\mathbf{1}$ for some k then we have

$$Nd(x,l,r)[0 := y][k\mathbf{1}] \overset{\text{def}}{=} Nd(y,l,r)[k\mathbf{1}] = l[k] = Nd(x,l,r)[k\mathbf{1}].$$

The subcase when $j = k\mathbf{2}$ is similar. In the inductive case when $i = i_1\mathbf{1}$ first note that $i_1 < |l|_b$ by 13.3.1(2) and (1). Now take any $j \neq i_1\mathbf{1}$ such that

$$j < |Nd(x,l,r)|_b = |l|_b + |r|_b + 1 \tag{6}$$

and consider three subcases. If $j = 0$ then we have

$$Nd(x,l,r)[i_1\mathbf{1} := y][0] \overset{\text{def}}{=} Nd(x,l[i_1 := y],r)[0] = x = Nd(x,l,r)[0].$$

If $j = k\mathbf{1}$ for some k then $k \neq i_1$ and $k < |l|_b$ by 13.3.1(2) and (6). We have

$$Nd(x,l,r)[i_1\mathbf{1} := y][k\mathbf{1}] \overset{\text{def}}{=} Nd(x,l[i_1 := y],r)[k\mathbf{1}] = l[i_1 := y][k] \overset{\text{IH}}{=}$$
$$= l[k] = Nd(x,l,r)[k\mathbf{1}].$$

If $j = k\mathbf{2}$ for some k then we have

$$Nd(x,l,r)[i_1\mathbf{1} := y][k\mathbf{2}] \overset{\text{def}}{=} Nd(x,l[i_1 := y],r)[k\mathbf{2}] = r[k] = Nd(x,l,r)[k\mathbf{2}].$$

The inductive case when $i = i_1\mathbf{2}$ has a similar proof.

13.3.4 Filling function. The function $\mathit{Fill}(x,n)$ creates a perfectly balanced tree of size n labelling the nodes by x. The function satisfies

$$\vdash_{\mathrm{PA}} |\mathit{Fill}(x,n)|_b = n \tag{1}$$
$$\vdash_{\mathrm{PA}} \mathit{Pbt}\,\mathit{Fill}(x,n) \tag{2}$$
$$\vdash_{\mathrm{PA}} i < n \to \mathit{Fill}(x,n)[i] = x \tag{3}$$

and it is defined by course of values recursion on n as a primitive recursive function:

$$\begin{aligned}
&\mathit{Fill}(x,0) = E\\
&\mathit{Fill}(x,n\mathbf{1}) = \mathit{Nd}(x,\mathit{Fill}(x,n),\mathit{Fill}(x,n))\\
&\mathit{Fill}(x,n\mathbf{2}) = \mathit{Nd}(x,\mathit{Fill}(x,n+1),\mathit{Fill}(x,n)).
\end{aligned}$$

Properties (1), (2), and $\forall i(3)$ are proved by complete induction on n.

13.3.5 Insertion of a new first label. The function $\mathit{Insfirst}(x,t)$ increases by one the size of the perfectly balanced tree t by inserting x into the first position. The function satisfies

$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to |\mathit{Insfirst}(x,t)|_b = |t|_b + 1 \tag{1}$$
$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to \mathit{Pbt}\,\mathit{Insfirst}(x,t) \tag{2}$$
$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to \mathit{Insfirst}(x,t)[0] = x \tag{3}$$
$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \wedge i < |t|_b \to \mathit{Insfirst}(x,t)[i+1] = t[i] \tag{4}$$

and it is defined by Bt-recursion on t with substitution in parameter x as a primitive recursive function:

$$\begin{aligned}
&\mathit{Insfirst}(x,E) = \mathit{Nd}(x,E,E)\\
&\mathit{Insfirst}(x,\mathit{Nd}(y,l,r)) = \mathit{Nd}(x,\mathit{Insfirst}(y,r),l).
\end{aligned}$$

Property $\forall x(1)$ is proved by Bt-induction on t. In the base case when $t = E$ take any x and we have

$$|\mathit{Insfirst}(x,E)|_b \stackrel{\text{def}}{=} |\mathit{Nd}(x,E,E)|_b = |E|_b + |E|_b + 1 = 1 = |E|_b + 1.$$

In the inductive case when $t = \mathit{Nd}(y,l,r)$ take any x and we have

$$\begin{aligned}
&|\mathit{Insfirst}(x,\mathit{Nd}(y,l,r))|_b \stackrel{\text{def}}{=} |\mathit{Nd}(x,\mathit{Insfirst}(y,r),l)|_b =\\
&\quad = |\mathit{Insfirst}(y,r)|_b + |l|_b + 1 \stackrel{\text{IH}}{=} |r|_b + 1 + |l|_b + 1 = |\mathit{Nd}(y,l,r)|_b + 1.
\end{aligned}$$

Property $\forall x(2)$ is proved by Bt-induction on t. The base case is straightforward. In the inductive case when $t = \mathit{Nd}(y,l,r)$ take any x and we have

$$Pbt\,Insfirst(x, Nd(y,l,r)) \overset{\text{def}}{\Leftrightarrow} Pbt\,Nd(x, Insfirst(y,r), l) \overset{13.3.1(2)}{\Leftrightarrow}$$
$$(|Insfirst(y,r)|_b = |l|_b \lor |Insfirst(y,r)|_b = |l|_b + 1) \land$$
$$\land\, Pbt\,Insfirst(y,r) \land Pbt(l) \overset{(1)}{\Leftrightarrow}$$
$$(|r|_b + 1 = |l|_b \lor |r|_b + 1 = |l|_b + 1) \land Pbt\,Insfirst(y,r) \land Pbt(l) \Leftrightarrow$$
$$(|l|_b = |r|_b \lor |l|_b = |r|_b + 1) \land Pbt(r) \land Pbt(l) \overset{13.3.1(2)}{\Leftrightarrow} Pbt\,Nd(y,l,r).$$

Property (3) is straighforward.

Property $\forall i \forall x(4)$ is proved by Bt-induction on t. In the base case there is nothing to prove. In the inductive case when $t = Nd(y,l,r)$ take any i and x such that

$$i < |Nd(y,l,r)|_b = |l|_b + |r|_b + 1 \tag{5}$$

and consider three cases. If $i = 0$ then we have

$$Insfirst(x, Nd(y,l,r))[0+1] \overset{\text{def}}{=} Nd(x, Insfirst(y,r), l)[1] =$$
$$= Insfirst(y,r)[0] \overset{(3)}{=} y = Nd(y,l,r)[0].$$

If $i = j\mathbf{1}$ for some j then we have

$$Insfirst(x, Nd(y,l,r))[j\mathbf{1}+1] \overset{\text{def}}{=} Nd(x, Insfirst(y,r), l)[j\mathbf{2}] =$$
$$= l[j] = Nd(y,l,r)[j\mathbf{1}].$$

If $i = j\mathbf{2}$ for some j then $j < |r|_b$ by 13.3.1(2) and (5). We have

$$Insfirst(x, Nd(y,l,r))[j\mathbf{2}+1] \overset{\text{def}}{=} Nd(x, Insfirst(y,r), l)[(j+1)\mathbf{1}] =$$
$$= Insfirst(y,r)[j+1] \overset{\text{IH}}{=} r[j] = Nd(y,l,r)[j\mathbf{2}].$$

13.3.6 Deletion of the first label. The function $Delfirst(t)$ decreases by one the size of the nonempty perfectly balanced tree t by removing its first label. The function satisfies

$$\vdash_{\text{PA}} Pbt(t) \land |t|_b > 0 \to |Delfirst(t)|_b = |t|_b \dot{-} 1 \tag{1}$$
$$\vdash_{\text{PA}} Pbt(t) \land |t|_b > 0 \to Pbt\,Delfirst(t) \tag{2}$$
$$\vdash_{\text{PA}} Pbt(t) \land |t|_b > 0 \land i < |t|_b \dot{-} 1 \to Delfirst(t)[i] = t[i+1] \tag{3}$$

and it is defined by Bt-recursion as a primitive recursive function:

$$Delfirst\,Nd(x,l,r) = E \leftarrow l = E$$
$$Delfirst\,Nd(x,l,r) = Nd(x_1, r, Delfirst(l)) \leftarrow l = Nd(x_1, l_1, r_1).$$

Property (1) is proved by Bt-induction on t. In the base case there is nothing to prove. In the inductive case when $t = Nd(x,l,r)$ we consider two cases. If $l = E$ then $r = E$ by 13.3.1(2) and we have

$$|Delfirst\ Nd(x,E,E)|_b \stackrel{\text{def}}{=} |E|_b = 0 = 1 \dot{-} 1 = |Nd(x,E,E)|_b \dot{-} 1.$$

If $l = Nd(x_1, l_1, r_1)$ for some x_1, l_1, and r_1 then we have

$$|Delfirst\ Nd(x,l,r)|_b \stackrel{\text{def}}{=} |Nd(x_1, r, Delfirst(l))|_b = |r|_b + |Delfirst(l)|_b + 1 \stackrel{\text{IH}}{=}$$
$$= |r|_b + |l|_b \dot{-} 1 + 1 = |Nd(x,l,r)|_b \dot{-} 1.$$

Property (2) is proved by Bt-induction on t. In the base case there is nothing to prove. In the inductive case when $t = Nd(x,l,r)$ we consider two cases. If $l = E$ then $r = E$ by 13.3.1(2) and the property (2) holds trivially. If $l = Nd(x_1, l_1, r_1)$ for some x_1, l_1, and r_1 then we have

$$Pbt\ Delfirst\ Nd(x,l,r) \stackrel{\text{def}}{\Leftrightarrow} Pbt\ Nd(x_1, r, Delfirst(l)) \stackrel{13.3.1(2)}{\Leftrightarrow}$$
$$(|r|_b = |Delfirst(l)|_b \lor |r|_b = |Delfirst(l)|_b + 1) \land Pbt(r) \land Pbt\ Delfirst(l) \stackrel{(1)}{\Leftrightarrow}$$
$$(|r|_b = |l|_b \dot{-} 1 \lor |r|_b = |l|_b \dot{-} 1 + 1) \land Pbt(r) \land Pbt\ Delfirst(l) \stackrel{\text{IH}}{\Leftrightarrow}$$
$$(|l|_b = |r|_b \lor |l|_b = |r|_b + 1) \land Pbt(r) \land Pbt(l) \stackrel{13.3.1(2)}{\Leftrightarrow} Pbt\ Nd(x,l,r).$$

Property $\forall i(3)$ is proved by Bt-induction on t. In the base case there is nothing to prove. In the inductive case when $t = Nd(x,l,r)$ take any i such that

$$i < |Nd(x,l,r)|_b \dot{-} 1 = |l|_b + |r|_b \tag{4}$$

and consider two cases. If $l = E$ then $r = E$ by 13.3.1(2) and we have a contradiction by (4). So suppose that $l = Nd(x_1, l_1, r_1)$ for some x_1, l_1, and r_1. We consider three subcases. If $i = 0$ then

$$(Delfirst\ Nd(x,l,r))[0] \stackrel{\text{def}}{=} Nd(x_1, r, Delfirst(l))[0] = x_1 = Nd(x,l,r)[0+1].$$

If $i = j\mathbf{1}$ for some j then we have

$$(Delfirst\ Nd(x,l,r))[j\mathbf{1}] \stackrel{\text{def}}{=} Nd(x_1, r, Delfirst(l))[j\mathbf{1}] = r[j] =$$
$$= Nd(x,l,r)[j\mathbf{2}] = Nd(x,l,r)[j\mathbf{1}+1].$$

If $i = j\mathbf{2}$ for some j then $j < |l|_b$ by 13.3.1(2) and (4). We have

$$(Delfirst\ Nd(x,l,r))[j\mathbf{2}] \stackrel{\text{def}}{=} Nd(x_1, r, Delfirst(l))[j\mathbf{2}] = Delfirst(l)[j] \stackrel{\text{IH}}{=}$$
$$= l[j+1] = Nd(x,l,r)[(j+1)\mathbf{1}] = Nd(x,l,r)[j\mathbf{2}+1].$$

13.3.7 Insertion of a new last label. The function $Inslast(x,n,t)$ increases by one the size of the perfectly balanced tree t, where $|t|_b = n$, by inserting x into a new last position. The function satisfies

$$\vdash_{\mathrm{PA}} Pbt(t) \to |Inslast(x, |t|_b, t)|_b = |t|_b + 1 \tag{1}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \to Pbt\, Inslast(x, |t|_b, t) \tag{2}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \land i < |t|_b \to Inslast(x, |t|_b, t)[i] = t[i] \tag{3}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \to Inslast(x, |t|_b, t)[|t|_b] = x \tag{4}$$

and it is defined by dyadic recursion on n with substitution in parameter t as a primitive recursive function:

$Inslast(x, 0, t) = Nd(x, E, E)$
$Inslast(x, n\mathbf{1}, Nd(y, l, r)) = Nd(y, Inslast(x, n, l), r)$
$Inslast(x, n\mathbf{2}, Nd(y, l, r)) = Nd(y, l, Inslast(x, n, r))$.

Properties (1), (2), $\forall i(3)$, and (4) are proved by Bt-induction on t.

13.3.8 Deletion of the last label. The function $Dellast(n, t)$ decreases by one the size of the nonempty perfectly balanced tree t, where $|t|_b = n + 1$, by removing its last label. The function satisfies

$$\vdash_{\mathrm{PA}} Pbt(t) \land |t|_b > 0 \to |Dellast(|t|_b \dot{-} 1, t)|_b = |t|_b \dot{-} 1 \tag{1}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \land |t|_b > 0 \to Pbt\, Dellast(|t|_b \dot{-} 1, t) \tag{2}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \land |t|_b > 0 \land i < |t|_b \dot{-} 1 \to Dellast(|t|_b \dot{-} 1, t)[i] = t[i] \tag{3}$$

and it is defined by dyadic recursion on n with substitution in parameter t as a primitive recursive function:

$Dellast(0, t) = E$
$Dellast(n\mathbf{1}, Nd(x, l, r)) = Nd(x, Dellast(n, l), r)$
$Dellast(n\mathbf{2}, Nd(x, l, r)) = Nd(x, l, Dellast(n, r))$.

Properties (1), (2), and $\forall i(3)$ are proved by Bt-induction on t.

13.3.9 Converting lists into perfectly balanced binary trees. The function $Ln2pbt(x)$ takes a list and yields a perfectly balanced tree with members of the list as its labels. The function satisfies

$$\vdash_{\mathrm{PA}} |Ln2pbt(x)|_b = L(x) \tag{1}$$
$$\vdash_{\mathrm{PA}} Pbt\, Ln2pbt(x) \tag{2}$$
$$\vdash_{\mathrm{PA}} i < L(x) \to Ln2pbt(x)[i] = (x)_i \tag{3}$$

and it is defined by course of values recursion with measure $L(x)$ as a primitive recursive function:

$Split(0) = 0, 0$
$Split(u, 0) = (u, 0), 0$
$Split(u, v, w) = (u, y), v, z \leftarrow Split(w) = y, z$

$Ln2pbt(0) = E$
$Ln2pbt(v, w) = Nd(v, Ln2pbt(y), Ln2pbt(z)) \leftarrow Split(w) = y, z$.

The auxilliary function *Split* satisfies:

$$\vdash_{\text{PA}} \exists y \exists z\, \mathit{Split}(x) = y, z \tag{4}$$

$$\begin{aligned}&\vdash_{\text{PA}} \mathit{Split}(x) = y, z \to \\ &\quad L(x) = L(y) + L(z) \wedge (L(y) = L(z) \vee L(y) = L(z) + 1)\end{aligned} \tag{5}$$

$$\vdash_{\text{PA}} \mathit{Split}(x) = y, z \wedge 2 \cdot i < L(x) \to (x)_{2 \cdot i} = (y)_i \tag{6}$$

$$\vdash_{\text{PA}} \mathit{Split}(x) = y, z \wedge 2 \cdot i + 1 < L(x) \to (x)_{2 \cdot i+1} = (z)_i. \tag{7}$$

Properties (4), $\forall y \forall z(5)$, $\forall y \forall z \forall i(6)$, and $\forall y \forall z \forall i(7)$ are proved by measure induction with measure $L(x)$.

Property (1) is proved by meausure induction with measure $L(x)$. So take any x and consider two cases. If $x = 0$ then we have

$$|\mathit{Ln2pbt}(0)|_b \overset{\text{def}}{=} |E|_b = 0 = L(0).$$

If $x = v, w$ for some v and w then by (4) there exist y and z such that $\mathit{Split}(w) = y, z$. Note also that $L(y) \leq L(w)$ and $L(z) \leq L(w)$ by (5). We have

$$|\mathit{Ln2pbt}(v, w)|_b \overset{\text{def}}{=} |\mathit{Nd}(v, \mathit{Ln2pbt}(y), \mathit{Ln2pbt}(z))|_b =$$

$$= |\mathit{Ln2pbt}(y)|_b + |\mathit{Ln2pbt}(z)|_b + 1 \overset{\text{IH}}{=} L(y) + L(z) + 1 \overset{(5)}{=} L(w) + 1 = L(v, w).$$

Property (2) is proved by measure induction with measure $L(x)$. So take any x and consider two cases. The case when $x = 0$ is straightforward. So suppose that $x = v, w$ for some v and w. By (4) there exist y and z such that $\mathit{Split}(w) = y, z$. Note also that $L(y) \leq L(w)$ and $L(z) \leq L(w)$ by (5). We have

$$\begin{aligned}&\mathit{Pbt}\, \mathit{Ln2pbt}(v, w) \overset{\text{def}}{\Leftrightarrow} \mathit{Pbt}\, \mathit{Nd}(v, \mathit{Ln2pbt}(y), \mathit{Ln2pbt}(z)) \overset{13.3.1(2)}{\Leftrightarrow} \\ &(|\mathit{Ln2pbt}(y)|_b = |\mathit{Ln2pbt}(z)|_b \vee |\mathit{Ln2pbt}(y)|_b = |\mathit{Ln2pbt}(z)|_b + 1) \wedge \\ &\quad \wedge \mathit{Pbt}\, \mathit{Ln2pbt}(y) \wedge \mathit{Pbt}\, \mathit{Ln2pbt}(z) \overset{(1)}{\Leftrightarrow} \\ &(L(y) = L(z) \vee L(y) = L(z) + 1) \wedge \mathit{Pbt}\, \mathit{Ln2pbt}(y) \wedge \mathit{Pbt}\, \mathit{Ln2pbt}(z).\end{aligned}$$

The last follows from IH and (5).

Property $\forall i(3)$ is proved by measure induction with measure $L(x)$. Take any x and i such that $i < L(x)$. Then $x = v, w$ for some v and w and thus $i < L(v, w) = L(w) + 1$. By (4) there exist y and z such that $\mathit{Split}(w) = y, z$. We consider three cases. If $i = 0$ then we have

$$\mathit{Ln2pbt}(v, w)[0] \overset{\text{def}}{=} \mathit{Nd}(v, \mathit{Ln2pbt}(y), \mathit{Ln2pbt}(z))[0] = v = (v, w)[0].$$

If $i = j\mathbf{1}$ for some j then $j < L(y)$ and $L(y) \leq L(w)$ by (5). We have

$$\mathit{Ln2pbt}(v, w)[j\mathbf{1}] \overset{\text{def}}{=} \mathit{Nd}(v, \mathit{Ln2pbt}(y), \mathit{Ln2pbt}(z))[j\mathbf{1}] =$$

$$= \mathit{Ln2pbt}(y)[j] \overset{\text{IH}}{=} y[j] \overset{(6)}{=} w[2 \cdot j] = (v, w)[j\mathbf{1}].$$

The case when $i = j\mathbf{2}$ is similar.

13.3.10 Converting perfectly balanced binary trees into lists. The function $Pbt2ln(t)$ takes a perfectly balanced tree and yields a list with labels of the tree as its members. The function satisfies

$$\vdash_{\mathrm{PA}} Pbt(t) \to L\,Pbt2ln(t) = |t|_b \tag{1}$$
$$\vdash_{\mathrm{PA}} Pbt(t) \land i < |t|_b \to (Pbt2ln(t))_i = t[i] \tag{2}$$

and it is defined by Bt-recursion as a primitive recursive function:

$$Pbt2ln(E) = 0$$
$$Pbt2ln\,Nd(x,l,r) = x, Combine(Pbt2ln(l), Pbt2ln(r)).$$

The auxiliary function *Combine* is defined in Par. 12.2.6.

Properties (1) and $\forall i(2)$ are proved by Bt-induction on t.

13.4 Applications of Trees

Heaps and Priority Queues

13.4.1 Tree comparision predicates. The predicate $x \succeq t$ holds if x is an upper bound of the labels of the binary tree t, i.e.

$$\vdash_{\mathrm{PAx}} x \succeq t \leftrightarrow \forall y(y \in_b t \to x \geq y).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} x \succeq E \tag{1}$$
$$\vdash_{\mathrm{PA}} x \succeq Nd(y,l,r) \leftrightarrow x > y \land x \succeq l \land x \succeq r \tag{2}$$
$$\vdash_{\mathrm{PA}} x \geq y \land y \succeq t \to x \succeq t. \tag{3}$$

13.4.2 Heaps. The predicate $Heap(t)$ holds if t is a perfectly balanced binary tree satisfying the following *heap condition*:

> for every nonempty subtree of t each label of its left (right) son is less than its root label.

The predicate is defined by

$$\vdash_{\mathrm{PAx}} Heap(t) \leftrightarrow Pbt(t) \land \forall x \forall l \forall r(Nd(x,l,r) \trianglelefteq_b t \to x \succeq l \land x \succeq r).$$

The predicate satisfies

$$\vdash_{\mathrm{PA}} Heap(E) \tag{1}$$
$$\begin{aligned} &\vdash_{\mathrm{PA}} Heap\,Nd(x,l,r) \leftrightarrow \\ &\quad (|l|_b = |r|_b \lor |l|_b = |r|_b + 1) \land x \succeq l \land x \succeq r \land Heap(l) \land Heap(r). \end{aligned} \tag{2}$$

13.4.3 Priority queues.

$$\vdash_{\mathrm{PAx}} Queue(q) \leftrightarrow \exists n \exists t(q = n,t \land Heap(t) \land |t|_b = n).$$

$$\vdash_{\mathrm{PAx}} E_q = 0, E$$
$$\vdash_{\mathrm{PAx}} x \in_q q \leftrightarrow x \in_b T(q)$$
$$\vdash_{\mathrm{PAx}} |q|_q = |T(q)|_b$$
$$\vdash_{\mathrm{PAx}} \#_q(x,q) = \#_b(x,T(q)).$$

13.4.4 Insertion in priority queues. The function $\mathit{Upheap}(n,t,x)$ takes a heap t of the size n and inserts x into it. The function satisfies

$$\vdash_{\mathrm{PA}} \mathit{Heap}(t) \to |\,\mathit{Upheap}(|t|_b, t, x)|_b = |t|_b + 1 \tag{1}$$
$$\vdash_{\mathrm{PA}} \mathit{Heap}(t) \to \mathit{Heap}\ \mathit{Upheap}(|t|_b, t, x) \tag{2}$$
$$\vdash_{\mathrm{PA}} \mathit{Heap}(t) \to \#_b\big(x, \mathit{Upheap}(|t|_b, t, x)\big) = \#_b(x,t) + 1 \tag{3}$$
$$\vdash_{\mathrm{PA}} \mathit{Heap}(t) \land y \neq x \to \#_b\big(y, \mathit{Upheap}(|t|_b, t, x)\big) = \#_b(y,t) \tag{4}$$

and it is defined by dyadic recursion on n with substitution in parameters as a primitive recursive function:

$$\begin{aligned}
&\mathit{Upheap}(0,E,x) = \mathit{Nd}(x,E,E)\\
&\mathit{Upheap}(n\mathbf{1}, \mathit{Nd}(y,l,r), x) = \mathit{Nd}(y, \mathit{Upheap}(n,l,x), r) \leftarrow x \leq y\\
&\mathit{Upheap}(n\mathbf{1}, \mathit{Nd}(y,l,r), x) = \mathit{Nd}(x, \mathit{Upheap}(n,l,y), r) \leftarrow x > y\\
&\mathit{Upheap}(n\mathbf{2}, \mathit{Nd}(y,l,r), x) = \mathit{Nd}(y, l, \mathit{Upheap}(n,r,x)) \leftarrow x \leq y\\
&\mathit{Upheap}(n\mathbf{2}, \mathit{Nd}(y,l,r), x) = \mathit{Nd}(x, l, \mathit{Upheap}(n,r,y)) \leftarrow x > y.
\end{aligned}$$

The function $\mathit{Enqueue}(q,x)$ takes a priority queue q and inserts x into it. The function satisfies

$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \to |\mathit{Enqueue}(q,x)|_q = |q|_q + 1 \tag{5}$$
$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \to \mathit{Queue}\ \mathit{Enqueue}(q,x) \tag{6}$$
$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \to \#_q\big(x, \mathit{Enqueue}(q,x)\big) = \#_q(x,q) + 1 \tag{7}$$
$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \land y \neq x \to \#_q\big(y, \mathit{Enqueue}(q,x)\big) = \#_q(y,q) \tag{8}$$

and it is defined explicitly as a primitive recursive function:

$$\mathit{Enqueue}((n,t),x) = n+1, \mathit{Upheap}(n,t,x).$$

Property (1) follows from

$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to |\,\mathit{Upheap}(|t|_b, t, x)|_b = |t|_b + 1, \tag{9}$$

which is proved by Bt-induction on t with the induction formula $\forall x(9)$. The base case is straightforward. In the inductive case when $t = \mathit{Nd}(y,l,r)$ take any x and consider two cases. If $|l|_b = |r|_b$ then $|\mathit{Nd}(y,l,r)|_b = |l|_b\mathbf{1}$. We consider two subcases. If $x \leq y$ then we have

$$\begin{aligned}
&|\,\mathit{Upheap}(|l|_b\mathbf{1}, \mathit{Nd}(y,l,r), x)|_b \overset{\text{def}}{=} |\mathit{Nd}(y, \mathit{Upheap}(|l|_b, l, x), r)|_b =\\
&\quad = |\,\mathit{Upheap}(|l|_b, l, x)|_b + |r|_b + 1 \overset{\text{IH}}{=} |l|_b + 1 + |r|_b + 1 = |\mathit{Nd}(y,l,r)|_b + 1.
\end{aligned}$$

If $x > y$ then we have

$$\begin{aligned}
&|\,\mathit{Upheap}(|l|_b\mathbf{1}, \mathit{Nd}(y,l,r), x)|_b \overset{\text{def}}{=} |\mathit{Nd}(x, \mathit{Upheap}(|l|_b, l, y), r)|_b =\\
&\quad = |\,\mathit{Upheap}(|l|_b, l, y)|_b + |r|_b + 1 \overset{\text{IH}}{=} |l|_b + 1 + |r|_b + 1 = |\mathit{Nd}(y,l,r)|_b + 1.
\end{aligned}$$

The case when $|l|_b = |r|_b + 1$ is similar.

Now note that

$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to y \in_b \mathit{Upheap}(|t|_b, t, x) \leftrightarrow y \in_b t \vee y = x. \tag{10}$$

Property $\forall x(10)$ is proved by Bt-induction on t and is left to the reader. As a simple consequence of (10) we get

$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to y \succeq \mathit{Upheap}(|t|_b, t, x) \leftrightarrow y \succeq t \wedge y \geq x. \tag{11}$$

Property $\forall x(2)$ is proved by Bt-induction on t. The base case is straightforward. In the inductive case when $t = \mathit{Nd}(y, l, r)$ take any x and consider two cases. If $|l|_b = |r|_b$ then $|\mathit{Nd}(y, l, r)|_b = |l|_b\mathbf{1}$. We consider two subcases. If $x \leq y$ then we have

$$\begin{aligned}
&\mathit{Heap}\ \mathit{Upheap}(|l|_b\mathbf{1}, \mathit{Nd}(y, l, r), x) \overset{\text{def}}{\Leftrightarrow} \mathit{Heap}\ \mathit{Nd}(y, \mathit{Upheap}(|l|_b, l, x), r) \overset{13.4.2(2)}{\Leftrightarrow}\\
&(|\mathit{Upheap}(|l|_b, l, x)|_b = |r|_b \vee |\mathit{Upheap}(|l|_b, l, x)|_b = |r|_b + 1) \wedge\\
&\quad y \succeq \mathit{Upheap}(|l|_b, l, x) \wedge y \succeq r \wedge \mathit{Heap}\ \mathit{Upheap}(|l|_b, l, x) \wedge \mathit{Heap}(r) \overset{(1),(11)}{\Leftrightarrow}\\
&(|l|_b + 1 = |r|_b \vee |l|_b + 1 = |r|_b + 1) \wedge\\
&\quad y \succeq l \wedge y \succeq r \wedge \mathit{Heap}\ \mathit{Upheap}(|l|_b, l, x) \wedge \mathit{Heap}(r).
\end{aligned}$$

The last follows from IH and assumptions. If $x > y$ then we have

$$\begin{aligned}
&\mathit{Heap}\ \mathit{Upheap}(|l|_b\mathbf{1}, \mathit{Nd}(y, l, r), x) \overset{\text{def}}{\Leftrightarrow} \mathit{Heap}\ \mathit{Nd}(x, \mathit{Upheap}(|l|_b, l, y), r) \overset{13.4.2(2)}{\Leftrightarrow}\\
&(|\mathit{Upheap}(|l|_b, l, y)|_b = |r|_b \vee |\mathit{Upheap}(|l|_b, l, y)|_b = |r|_b + 1) \wedge\\
&\quad x \succeq \mathit{Upheap}(|l|_b, l, y) \wedge x \succeq r \wedge \mathit{Heap}\ \mathit{Upheap}(|l|_b, l, y) \wedge \mathit{Heap}(r) \overset{(1),(11)}{\Leftrightarrow}\\
&(|l|_b + 1 = |r|_b \vee |l|_b + 1 = |r|_b + 1) \wedge\\
&\quad x \succeq l \wedge x \succeq r \wedge \mathit{Heap}\ \mathit{Upheap}(|l|_b, l, y) \wedge \mathit{Heap}(r).
\end{aligned}$$

The last follows from IH and assumptions by 13.4.1(3). The case when $|l|_b = |r|_b + 1$ is similar.

Properties (3) and (4) follows from

$$\vdash_{\mathrm{PA}} \mathit{Pbt}(t) \to \#_b\big(y, \mathit{Upheap}(|t|_b, t, x)\big) = \#_b(y, t) + (y =_* x), \tag{12}$$

which is proved by Bt-induction on t with the induction formula $\forall x(12)$. The base case is straightforward. In the inductive case when $t = \mathit{Nd}(z, l, r)$ take any x and consider two cases. If $|l|_b = |r|_b$ then $|\mathit{Nd}(y, l, r)|_b = |l|_b\mathbf{1}$. We consider two subcases. If $x \leq z$ then we have

$$\begin{aligned}
&\#_b\big(y, \mathit{Upheap}(|l|_b\mathbf{1}, \mathit{Nd}(z, l, r), x)\big) \overset{\text{def}}{=}\\
&\quad = \#_b\big(y, \mathit{Nd}(z, \mathit{Upheap}(|l|_b, l, x), r)\big) \overset{13.1.14(1)}{=}
\end{aligned}$$

$$= \#_b\big(y, \mathit{Upheap}(|l|_b, l, x)\big) + \#_b(y,r) + (y =_* z) \overset{\mathrm{IH}}{=}$$
$$= \#_b(y,l) + (y =_* x) + \#_b(y,r) + (y =_* z) \overset{13.1.14(1)}{=}$$
$$= \#_b(y, \mathit{Nd}(z,l,r)) + (y =_* x).$$

If $x > z$ then we have

$$\#_b\big(y, \mathit{Upheap}(|l|_b\mathbf{1}, \mathit{Nd}(z,l,r), x)\big) \overset{\mathrm{def}}{=}$$
$$= \#_b\big(y, \mathit{Nd}(x, \mathit{Upheap}(|l|_b, l, z), r)\big) \overset{13.1.14(1)}{=}$$
$$= \#_b\big(y, \mathit{Upheap}(|l|_b, l, z)\big) + \#_b(y,r) + (y =_* x) \overset{\mathrm{IH}}{=}$$
$$= \#_b(y,l) + (y =_* z) + \#_b(y,r) + (y =_* x) \overset{13.1.14(1)}{=}$$
$$= \#_b(y, \mathit{Nd}(z,l,r)) + (y =_* x).$$

The case when $|l|_b = |r|_b + 1$ is similar.

13.4.5 Deletion in priority queues.

$$\vdash_{\mathrm{PA}} \mathit{Heap}(t) \land t \neq E \to |\mathit{Downheap}(t,x)|_b = |t|_b \tag{1}$$
$$\vdash_{\mathrm{PA}} \mathit{Heap}(t) \land t \neq E \to \mathit{Heap}\ \mathit{Downheap}(t,x) \tag{2}$$

$$\begin{aligned}
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(x,l,r) \leftarrow l = E\\
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(y_1, \mathit{Nd}(x,l_1,r_1), r) \leftarrow\\
&\quad l \neq E \land r = E \land l = \mathit{Nd}(y_1,l_1,r_1) \land x \leq y_1\\
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(x,l,r) \leftarrow\\
&\quad l \neq E \land r = E \land l = \mathit{Nd}(y_1,l_1,r_1) \land x > y_1\\
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(y_2, l, \mathit{Downheap}(r,x)) \leftarrow\\
&\quad l \neq E \land r \neq E \land \mathit{Root}(l) = y_1 \land \mathit{Root}(r) = y_2 \land y_1 \leq y_2 \land x \leq y_2\\
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(x,l,r) \leftarrow\\
&\quad l \neq E \land r \neq E \land \mathit{Root}(l) = y_1 \land \mathit{Root}(r) = y_2 \land y_1 \leq y_2 \land x > y_2\\
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(y_1, \mathit{Downheap}(l,x), r) \leftarrow\\
&\quad l \neq E \land r \neq E \land \mathit{Root}(l) = y_1 \land \mathit{Root}(r) = y_2 \land y_1 > y_2 \land x \leq y_1\\
&\mathit{Downheap}(\mathit{Nd}(y,l,r),x) = \mathit{Nd}(x,l,r) \leftarrow\\
&\quad l \neq E \land r \neq E \land \mathit{Root}(l) = y_1 \land \mathit{Root}(r) = y_2 \land y_1 > y_2 \land x > y_1.
\end{aligned}$$

$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \land q \neq E_q \to |\mathit{Dequeue}(q)|_q + 1 = |q|_q \tag{3}$$
$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \land q \neq E_q \to \mathit{Queue}\ \mathit{Dequeue}(q) \tag{4}$$
$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \land q \neq E_q \to \#_q\big(\mathit{Largest}(q), \mathit{Dequeue}(q,x)\big) = \#_q(x,q) + 1 \tag{5}$$
$$\vdash_{\mathrm{PA}} \mathit{Queue}(q) \land q \neq E_q \land y \neq \mathit{Largest}(q) \to \#_q\big(y, \mathit{Dequeue}(q,x)\big) = \#_q(y,q) \tag{6}$$

$$\begin{aligned}
&\mathit{Dequeue}(1,t) = E\\
&\mathit{Dequeue}(n+1,t) = \mathit{Downheap}(n, \mathit{Dellast}(n,t), t[n]) \leftarrow n > 0.
\end{aligned}$$

$$\begin{aligned} &\models_{\text{PA}} Bt(t) \wedge t \neq E \wedge y \neq Root(t) \rightarrow \\ &\quad y \in_b Downheap(t,x) \leftrightarrow y \in_b t \vee y = x \end{aligned} \tag{7}$$

$$\models_{\text{PA}} Bt(t) \wedge t \neq E \wedge y \succeq t \rightarrow y \succeq Downheap(t,x) \leftrightarrow y \geq x \tag{8}$$

13.4.6 Heap sort.

$$\models_{\text{PA}} Hsort(x) \sim x \tag{1}$$

$$\models_{\text{PA}} Ord\ Hsort(x). \tag{2}$$

13.5 Exercises

13.5.1 Exercise. Prove

$$\vdash_{\mathrm{PA}} Bt(t) \to \mathit{Inorder}(t) = \mathit{Rev}\ \mathit{Inorder}\ \mathit{Reflect}(t)$$

13.5.2 Exercise. Save the concatenation in the definition of the function $\mathit{Inorder}(t)$ with the help of an accumulator function and verify your implementation.

13.5.3 Exercise. Save the concatenation in the definition of the function $\mathit{Postorder}(t)$ with the help of an accumulator function and verify your implementation.

13.5.4 Exercise. Find a tail recursive implementation of the function $\mathit{Inorder}(t)$ and verify your implementation.

13.5.5 Exercise. Find a tail recursive derivation of the function $\mathit{Postorder}(t)$ and verify your implementation.

13.5.6 Exercise. Define a function $\mathit{Subtrees}(t)$ satisfying

$$\vdash_{\mathrm{PA}} Bt(t) \to t_1 \mathrel{\varepsilon} \mathit{Subtrees}(t) \leftrightarrow t_1 \trianglelefteq_b t.$$

Prove that the function has the required property.

13.5.7 Exersice. Consider the following implementation of the deletion function $t \setminus \{x\}$:

$$\begin{aligned}
&\mathit{Split}\ Nd(y,l,r) = y,l \leftarrow r = E\\
&\mathit{Split}\ Nd(y,l,r) = y,l \leftarrow r \neq E \land \mathit{Split}(r) = x,t
\end{aligned}$$

$$\begin{aligned}
&t_1 \sqcup t_2 = t_2 \leftarrow t_1 = E\\
&t_1 \sqcup t_2 = Nd(x,t,t_2) \leftarrow t_1 \neq E \land \mathit{Split}(t_1) = x,t
\end{aligned}$$

$$\begin{aligned}
&E \setminus \{x\} = E\\
&Nd(y,l,r) \setminus \{x\} = Nd(y,l,r \setminus \{x\}) \leftarrow y < x\\
&Nd(y,l,r) \setminus \{x\} = l \sqcup r \leftarrow y = x\\
&Nd(y,l,r) \setminus \{x\} = Nd(y,l \setminus \{x\},r) \leftarrow y > x.
\end{aligned}$$

Prove

$$\begin{aligned}
&\vdash_{\mathrm{PA}} Bst(t) \to Bst(t \setminus \{x\})\\
&\vdash_{\mathrm{PA}} Bst(t) \to y \in t \setminus \{x\} \leftrightarrow y \in t \land y \neq x.
\end{aligned}$$

Hint. First note that the auxiliary function *Split* satisfies

$\vdash_{\mathrm{PA}} Bt(t_1) \wedge t_1 \neq E \rightarrow Split(t_1) \neq 0$
$\vdash_{\mathrm{PA}} Bt(t_1) \wedge t_1 \neq E \wedge Split(t_1) = x_2, t_2 \rightarrow y \in_b t_1 \leftrightarrow y = x_2 \vee y \in_b t_2$
$\vdash_{\mathrm{PA}} Bt(t_1) \wedge t_1 \neq E \wedge Split(t_1) = x_2, t_2 \rightarrow y \prec t_1 \leftrightarrow y < x_2 \wedge y \prec t_2$
$\vdash_{\mathrm{PA}} Bst(t_1) \wedge t_1 \neq E \wedge Split(t_1) = x_2, t_2 \rightarrow x_2 \succ t_2 \wedge Bst(t_2).$

14. Programs Operating on Symbolic Expressions

14.0.8 Sublists. The predicate $x \subset y$ holds if every element of the list x occurs also in the the list y, i.e.

$$\vdash_{\mathrm{PAx}} x \subset y \to \forall z(z \,\varepsilon\, x \to z \,\varepsilon\, y).$$

The predicate satisfies:

$$\vdash_{\mathrm{PA}} 0 \subset y \tag{1}$$

$$\vdash_{\mathrm{PA}} v, w \subset y \leftrightarrow v \,\varepsilon\, y \wedge w \subset y \tag{2}$$

$$\vdash_{\mathrm{PA}} x_1 \oplus x_2 \subset y \leftrightarrow x_1 \subset y \wedge x_2 \subset y. \tag{3}$$

14.1 Numeric Terms

14.1.1 Numeric terms. Numeric terms are formed from variables x_i, constants n by the numeric operators $+$ (addition) and $\cdot$ (multiplication).

14.1.2 Arithmetization of numeric terms. We arithmetize numeric terms with the help of four constructors:

$\mathbf{x}_i = 0, i$
$\overline{n} = 1, n$
$t_1 \mathbin{\pmb{+}} t_2 = 2, t_1, t_2$
$t_1 \mathbin{\pmb{\times}} t_2 = 3, t_1, t_2.$

We assign to each numeric term τ a number $\ulcorner\tau\urcorner$ called the code of τ. The mapping is defined inductively on the structure of numeric terms as follows:

$$\ulcorner x_i \urcorner = \mathbf{x}_i \tag{1}$$
$$\ulcorner n \urcorner = \overline{n} \tag{2}$$
$$\ulcorner \tau_1 + \tau_2 \urcorner = \ulcorner \tau_1 \urcorner \mathbin{\pmb{+}} \ulcorner \tau_2 \urcorner \tag{3}$$
$$\ulcorner \tau_1 \cdot \tau_2 \urcorner = \ulcorner \tau_1 \urcorner \mathbin{\pmb{\times}} \ulcorner \tau_2 \urcorner. \tag{4}$$

The predicate $\mathit{Term}(t)$ holding of the codes of numeric terms is defined by course of values recursion as a primitive recursive predicate:

$\mathit{Term}(\mathbf{x}_i)$
$\mathit{Term}(\overline{n})$
$\mathit{Term}(t_1 \mathbin{\pmb{+}} t_2) \leftarrow \mathit{Term}(t_1) \wedge \mathit{Term}(t_2)$
$\mathit{Term}(t_1 \mathbin{\pmb{\times}} t_2) \leftarrow \mathit{Term}(t_1) \wedge \mathit{Term}(t_2).$

We identify numeric terms with their codes and from now on we will say the *numeric term* t instead of the *code of the numeric term* t.

14.1.3 Case analysis on numeric terms. We have the following principle of *case analysis on numeric terms*:

$$\begin{aligned} \vdash_{\mathrm{PA}}\ & \mathit{Term}(t) \rightarrow \\ & \exists i\, t = \mathbf{x}_i \vee \exists n\, t = \overline{n} \vee \exists t_1 \exists t_2\, t = t_1 \mathbin{\pmb{+}} t_2 \vee \exists t_1 \exists t_2\, t = t_1 \mathbin{\pmb{\times}} t_2 \end{aligned} \tag{1}$$

which is proved by a straightforward pair case analysis.

14.1.4 Structural induction on numeric terms. The formula of *structural induction on the numeric term t for* $\phi[t]$ is the following one:

$$\begin{aligned} & \forall i\, \phi[\mathbf{x}_i] \wedge \forall n\, \phi[\overline{n}] \wedge \forall t_1 \forall t_2 (\phi[t_1] \wedge \phi[t_2] \rightarrow \phi[t_1 \mathbin{\pmb{+}} t_2]) \wedge \\ & \forall t_1 \forall t_2 (\phi[t_1] \wedge \phi[t_2] \rightarrow \phi[t_1 \mathbin{\pmb{\times}} t_2]) \rightarrow \mathit{Term}(t) \rightarrow \phi[t]. \end{aligned}$$

In the sequel we will often say shortly the *Term-induction on t* instead of the structural induction on the numeric term t.

14.1.5 Theorem. *We have*

$$\vdash_{\scriptscriptstyle PA} \forall i\, \phi[\mathbf{x}_i] \land \forall n\, \phi[\overline{n}] \land \forall t_1 \forall t_2 (\phi[t_1] \land \phi[t_2] \to \phi[t_1 \mathbin{\boldsymbol{+}} t_2]) \land$$
$$\forall t_1 \forall t_2 (\phi[t_1] \land \phi[t_2] \to \phi[t_1 \mathbin{\boldsymbol{\times}} t_2]) \to \mathit{Term}(t) \to \phi[t].$$

Proof. The property is proved by complete induction on t. Take any t and under the assumptions of the claim consider the following cases by 14.1.3(1). The case when $t = \mathbf{x}_i$ or $t = \overline{n}$ is trivial. The case when $t = t_1 \mathbin{\boldsymbol{+}} t_2$ for some t_1, t_2 we have $\phi[t_1]$ and $\phi[t_2]$ by IH since $t_1 < t_1 \mathbin{\boldsymbol{+}} t_2$ and $t_2 < t_1 \mathbin{\boldsymbol{+}} t_2$. From this and assumptions we get $\phi[t_1 \mathbin{\boldsymbol{+}} t_2]$. The case when $t = t_1 \mathbin{\boldsymbol{\times}} t_2$ for some t_1, t_2 is similar. □

14.1.6 Structural recursion on numeric terms. Initial clauses for clausal definitions with *structural recursion on numeric terms* are of a form

$$f(\vec{y}, t, \vec{z}) = \alpha_1[\vec{y}, \vec{z}, i] \leftarrow t = \mathbf{x}_i$$
$$f(\vec{y}, t, \vec{z}) = \alpha_2[\vec{y}, \vec{z}, n] \leftarrow t = \overline{n}$$
$$f(\vec{y}, t, \vec{z}) = \alpha_3[\dot{\lambda} \vec{y} t \vec{z}. f(\vec{y}, t_i, \vec{z}); \vec{y}, \vec{z}, t_1, t_2] \leftarrow t = t_1 \mathbin{\boldsymbol{+}} t_2$$
$$f(\vec{y}, t, \vec{z}) = \alpha_4[\dot{\lambda} \vec{y} t \vec{z}. f(\vec{y}, t_i, \vec{z}); \vec{y}, \vec{z}, t_1, t_2] \leftarrow t = t_1 \mathbin{\boldsymbol{\times}} t_2.$$

In the sequel we will often say shortly the *Term-recursion on* t instead of the structural recursion on the numeric term t.

14.1.7 Free variables. The function $FV(t)$ takes a numeric term and returns a list of indices of free variables of the term. The function is defined by *Term*-recursion as a primitive recursive function:

$$FV(\mathbf{x}_i) = i, 0$$
$$FV(\overline{n}) = 0$$
$$FV(t_1 \mathbin{\boldsymbol{+}} t_2) = FV(t_1) \oplus FV(t_2)$$
$$FV(t_1 \mathbin{\boldsymbol{\times}} t_2) = FV(t_1) \oplus FV(t_2).$$

14.1.8 Denotation of numeric terms. The denotation function $[\![t]\!]_v$ takes the code t of a numeric term τ and the assignment v which is a list assigning the value $(v)_i$ to the variable x_i and yields the value of the term τ. The function is defined by *Term*-recursion on t as a primitive recursive function:

$$[\![\mathbf{x}_i]\!]_v = (v)_i$$
$$[\![\overline{n}]\!]_v = n$$
$$[\![t_1 \mathbin{\boldsymbol{+}} t_2]\!]_v = [\![t_1]\!]_v + [\![t_2]\!]_v$$
$$[\![t_1 \mathbin{\boldsymbol{\times}} t_2]\!]_v = [\![t_1]\!]_v \cdot [\![t_2]\!]_v.$$

14.1.9 Coincidence of assignments. The ternary predicate $v_1 \equiv v_2\,[is]$ holds if the assignments v_1 and v_2 coincide on every variable whose index is in the list is, i.e.

$$\vdash_{\scriptscriptstyle \mathrm{PA}\times} v_1 \equiv v_2\,[is] \leftrightarrow \forall i (i \mathrel{\varepsilon} is \to (v_1)_i = (v_2)_i).$$

The following holds

$$\vdash_{\mathrm{PA}} \ \mathit{Term}(t) \land FV(t) \subset \mathit{is} \land v_1 \equiv v_2\,[\mathit{is}] \to [\![t]\!]_{v_1} = [\![t]\!]_{v_2}. \tag{1}$$

Property (1) is proved by *Term*-induction on t. For instance, if $t = \mathbf{x}_i$ then

$$[\![\mathbf{x}_i]\!]_{v_1} = (v_1)_i \stackrel{\text{def}}{=} (v_2)_i = [\![\mathbf{x}_i]\!]_{v_2}.$$

If $t = t_1 \mathbin{\textbf{+}} t_2$ then $FV(t_1) \subset \mathit{is}$ and $FV(t_2) \subset \mathit{is}$ by 14.0.8(3) and we obtain

$$[\![t_1 \mathbin{\textbf{+}} t_2]\!]_{v_1} = [\![t_1]\!]_{v_1} + [\![t_2]\!]_{v_1} \stackrel{\text{IH}}{=} [\![t_1]\!]_{v_2} + [\![t_2]\!]_{v_2} = [\![t_1 \mathbin{\textbf{+}} t_2]\!]_{v_2}.$$

The remaining cases are similar.

14.1.10 Postfix machine. Our next task is the proof of correctness of a simple postfix machine for evaluating numeric terms. The machine is represented by the function $\mathit{Run}(p, v, s)$, where p is a list of instructions (program), v is an assignment (environment), and s is a list of values (I/O stack).

Instructions are defined with the help of four constructors:

$LOAD(i) = 0, i$
$PUSH(n) = 1, n$
$ADD = 2, 0$
$MULT = 3, 0.$

The predicate $\mathit{Instr}(i)$ holds if i is an instruction of the postfix machine. The predicate is primitive recursive with the following explicit clausal definition:

$\mathit{Instr}\, LOAD(i)$
$\mathit{Instr}\, PUSH(n)$
$\mathit{Instr}(ADD)$
$\mathit{Instr}(MULT).$

The predicate $\mathit{Program}(p)$ holds if p is a list of instructions. The predicate is defined by list recursion as a primitive recursive predicate:

$\mathit{Program}(0)$
$\mathit{Program}(i, p) \leftarrow \mathit{Instr}(i) \land \mathit{Program}(p).$

Numeric terms are compiled into programs by the function $\mathit{Cmp}(t)$. The function is defined by *Term*-recursion as a primitive recursive function:

$\mathit{Cmp}(\mathbf{x}_i) = LOAD(i), 0$
$\mathit{Cmp}(\overline{n}) = PUSH(n), 0$
$\mathit{Cmp}(t_1 \mathbin{\textbf{+}} t_2) = \mathit{Cmp}(t_1) \oplus \mathit{Cmp}(t_2) \oplus (ADD, 0)$
$\mathit{Cmp}(t_1 \mathbin{\boldsymbol{\times}} t_2) = \mathit{Cmp}(t_1) \oplus \mathit{Cmp}(t_2) \oplus (MULT, 0).$

The function $\mathit{Run}(p, v, s)$ representing the postfix machine is defined by list recursion on p with substitution in parameter s as a primitive recursive function:

$Run(0, v, t, s) = t$
$Run((LOAD(i), p), v, s) = Run(p, v, (v)_i, s)$
$Run((PUSH(n), p), v, s) = Run(p, v, n, s)$
$Run((ADD, p), v, t_2, t_1, s) = Run(p, v, t_1 + t_2, s)$
$Run((MULT, p), v, t_2, t_1, s) = Run(p, v, t_1 \cdot t_2, s).$

Finally, programs of the postfix machine are evaluated by

$$\models_{\mathrm{PAx}} Eval(p, v) = Run(p, v, 0).$$

The following property expresses the correctness of the evaluation function:

$$\models_{\mathrm{PA}} Term(t) \to Eval(Cmp(t), v) = [\![t]\!]_v. \tag{1}$$

To see this we first prove the basic property of the function *Run*:

$$\models_{\mathrm{PA}} Term(t) \to Run(Cmp(t) \oplus p, v, s) = Run(p, v, [\![t]\!]_v, s). \tag{2}$$

Property $\forall p \forall s(2)$ is proved by *Term*-induction on t. In the case when $t = \mathbf{x}_i$ take any p, s and we have

$$Run(Cmp(\mathbf{x}_i) \oplus p, v, s) \stackrel{\mathrm{def}}{=} Run((LOAD(i), p), v, s) \stackrel{\mathrm{def}}{=}$$
$$= Run(p, v, (v)_i, s) = Run(p, v, [\![\mathbf{x}_i]\!]_v, s).$$

In the case when $t = \overline{n}$ take any p, s and we have

$$Run(Cmp(\overline{n}) \oplus p, v, s) \stackrel{\mathrm{def}}{=} Run((PUSH(n), p), v, s) \stackrel{\mathrm{def}}{=}$$
$$= Run(p, v, n, s) = Run(p, v, [\![\overline{n}]\!]_v, s).$$

In the case when $t = t_1 \mathbin{\pmb{+}} t_2$ take any p, s and we have

$$Run(Cmp(t_1 \mathbin{\pmb{+}} t_2) \oplus p, v, s) \stackrel{\mathrm{def}}{=}$$
$$= Run((Cmp(t_1) \oplus Cmp(t_2) \oplus (ADD, p)), v, s) \stackrel{\mathrm{IH}}{=}$$
$$= Run((Cmp(t_2) \oplus (ADD, p)), v, [\![t_1]\!]_v, s) \stackrel{\mathrm{IH}}{=}$$
$$= Run((ADD, p), v, [\![t_2]\!]_v, [\![t_1]\!]_v, s) \stackrel{\mathrm{def}}{=}$$
$$= Run(p, v, [\![t_1]\!]_v + [\![t_2]\!]_v, s) = Run(p, v, [\![t_1 \mathbin{\pmb{+}} t_2]\!]_v, s).$$

The case when $t = t_1 \mathbin{\pmb{\times}} t_2$ has a similar proof.

We are now in position to prove (1). Assume $Term(t)$ and we have

$$Eval(Cmp(t), v) \stackrel{\mathrm{def}}{=} Run(Cmp(t), v, 0) \stackrel{(2)}{=} Run(0, v, [\![t]\!]_v, 0) \stackrel{\mathrm{def}}{=} [\![t]\!]_v.$$

14.2 Pair Terms

14.2.1 Pair terms. Pair terms are formed from variables x_i, the constant 0 by the operators H (head), T (tail), x, y (pairing), and the ternary case discrimination function D.

14.2.2 Arithmetization of pair terms. We arithmetize pair terms with the help of the following constructors:

$\mathbf{x}_i = 0, i$
$\mathbf{0} = 1, 0$
$\mathbf{H}(t) = 2, t$
$\mathbf{T}(t) = 3, t$
$t_1 \mathbf{,} t_2 = 4, t_1, t_2$
$\mathbf{D}(t_1, t_2, t_3) = 5, t_1, t_2, t_3.$

We assign to each pair term τ a number $\ulcorner\tau\urcorner$ called the code of τ. The mapping is defined inductively on the structure of pair terms:

$$\ulcorner x_i \urcorner = \mathbf{x}_i \tag{1}$$
$$\ulcorner 0 \urcorner = \mathbf{0} \tag{2}$$
$$\ulcorner H(\tau) \urcorner = \mathbf{H}(\ulcorner\tau\urcorner) \tag{3}$$
$$\ulcorner T(\tau) \urcorner = \mathbf{T}(\ulcorner\tau\urcorner) \tag{4}$$
$$\ulcorner \tau_1, \tau_2 \urcorner = \ulcorner\tau_1\urcorner \mathbf{,} \ulcorner\tau_2\urcorner \tag{5}$$
$$\ulcorner D(\tau_1, \tau_2, \tau_3) \urcorner = \mathbf{D}(\ulcorner\tau_1\urcorner, \ulcorner\tau_2\urcorner, \ulcorner\tau_3\urcorner). \tag{6}$$

The predicate $\mathit{Term}(t)$ holding of the codes of pair terms is defined by course of values recursion as a primitive recursive predicate:

$\mathit{Term}(\mathbf{x}_i)$
$\mathit{Term}(\mathbf{0})$
$\mathit{Term}\,\mathbf{H}(t) \leftarrow \mathit{Term}(t)$
$\mathit{Term}\,\mathbf{T}(t) \leftarrow \mathit{Term}(t)$
$\mathit{Term}(t_1 \mathbf{,} t_2) \leftarrow \mathit{Term}(t_1) \wedge \mathit{Term}(t_2)$
$\mathit{Term}\,\mathbf{D}(t_1, t_2, t_3) \leftarrow \mathit{Term}(t_1) \wedge \mathit{Term}(t_2) \wedge \mathit{Term}(t_3).$

We identify pair terms with their codes and from now on we will say the *pair term t* instead of the *code of the pair term t*.

14.2.3 Case analysis on pair terms. We have the following principle of *case analysis on pair terms*:

$$\begin{aligned} \vdash_{\mathrm{PA}} \; & \mathit{Term}(t) \rightarrow \\ & \exists i\, t = \mathbf{x}_i \vee t = \mathbf{0} \vee \exists t_1\, t = \mathbf{H}(t_1) \vee \exists t_1\, t = \mathbf{T}(t_1) \vee \\ & \exists t_1 \exists t_2\, t = t_1 \mathbf{,} t_2 \vee \exists t_1 \exists t_2 \exists t_3\, t = \mathbf{D}(t_1, t_2, t_3) \end{aligned} \tag{1}$$

which is proved by a straightforward pair case analysis.

14.2.4 Structural induction on pair terms. The formula of *structural induction on the pair term t for $\phi[t]$* is the following one:

$$\begin{aligned}&\forall i\, \phi[\mathbf{x}_i] \land \phi[\mathbf{0}] \land \forall t(\phi[t] \to \phi[\mathbf{H}(t)]) \land \forall t(\phi[t] \to \phi[\mathbf{T}(t)]) \land\\ &\forall t_1 \forall t_2(\phi[t_1] \land \phi[t_2] \to \phi[t_1 \mathbf{,} t_2]) \land\\ &\forall t_1 \forall t_2 \forall t_3(\phi[t_1] \land \phi[t_2] \land \phi[t_3] \to \phi[\mathbf{D}(t_1, t_2, t_3)]) \to\\ &\mathit{Term}(t) \to \phi[t].\end{aligned}$$

In the sequel we will often say shortly the *Term-induction on t* instead of the structural induction on the pair term t.

14.2.5 Theorem. *We have*

$$\begin{aligned}\vdash_{PA}\ &\forall i\, \phi[\mathbf{x}_i] \land \phi[\mathbf{0}] \land \forall t(\phi[t] \to \phi[\mathbf{H}(t)]) \land \forall t(\phi[t] \to \phi[\mathbf{T}(t)]) \land\\ &\forall t_1 \forall t_2(\phi[t_1] \land \phi[t_2] \to \phi[t_1 \mathbf{,} t_2]) \land\\ &\forall t_1 \forall t_2 \forall t_3(\phi[t_1] \land \phi[t_2] \land \phi[t_3] \to \phi[\mathbf{D}(t_1, t_2, t_3)]) \to\\ &\mathit{Term}(t) \to \phi[t].\end{aligned}$$

Proof. The property is proved by complete induction on t. Take any t and under the assumptions of the claim consider the following cases by 14.2.3(1). The case when $t = \mathbf{x}_i$ or $t = \mathbf{0}$ is trivial. The case when $t = t_1 \mathbf{,} t_2$ for some t_1, t_2 we have $\phi[t_1]$ and $\phi[t_2]$ by IH since $t_1 < t_1 \mathbf{,} t_2$ and $t_2 < t_1 \mathbf{,} t_2$. From this and assumptions we get $\phi[t_1 \mathbf{,} t_2]$. The remaining cases are similar. □

14.2.6 Structural recursion on pair terms. Initial clauses for clausal definitions with *structural recursion on pair terms* are of a form

$$\begin{aligned}&f(\vec{y}, t, \vec{z}) = \alpha_1[\vec{y}, \vec{z}, i] \leftarrow t = \mathbf{x}_i\\ &f(\vec{y}, t, \vec{z}) = \alpha_2[\vec{y}, \vec{z}] \leftarrow t = \mathbf{0}\\ &f(\vec{y}, t, \vec{z}) = \alpha_3[\dot{\lambda}\vec{y}t\vec{z}.f(\vec{y}, t_1, \vec{z}); \vec{y}, \vec{z}, t_1] \leftarrow t = \mathbf{H}(t_1)\\ &f(\vec{y}, t, \vec{z}) = \alpha_4[\dot{\lambda}\vec{y}t\vec{z}.f(\vec{y}, t_1, \vec{z}); \vec{y}, \vec{z}, t_1] \leftarrow t = \mathbf{T}(t_1)\\ &f(\vec{y}, t, \vec{z}) = \alpha_5[\dot{\lambda}\vec{y}t\vec{z}.f(\vec{y}, t_i, \vec{z}); \vec{y}, \vec{z}, t_1, t_2] \leftarrow t = t_1 \mathbf{,} t_2\\ &f(\vec{y}, t, \vec{z}) = \alpha_6[\dot{\lambda}\vec{y}t\vec{z}.f(\vec{y}, t_i, \vec{z}); \vec{y}, \vec{z}, t_1, t_2, t_3] \leftarrow t = \mathbf{D}(t_1, t_2, t_3).\end{aligned}$$

In the sequel we will often say shortly the *Term-recursion on t* instead of the structural recursion on the pair term t.

14.2.7 Free variables. The function $FV(t)$ takes a pair term and returns a list of indices of free variables of the term. The function is defined by *Term*-recursion as a primitive recursive function:

$$\begin{aligned}&FV(\mathbf{x}_i) = i, 0\\ &FV(\mathbf{0}) = 0\\ &FV\, \mathbf{H}(t) = FV(t)\\ &FV\, \mathbf{T}(t) = FV(t)\\ &FV(t_1 \mathbf{,} t_2) = FV(t_1) \oplus FV(t_2)\\ &FV\, \mathbf{D}(t_1, t_2, t_3) = FV(t_1) \oplus FV(t_2) \oplus FV(t_3).\end{aligned}$$

14.2.8 Denotation of pair terms. The denotation function $[\![t]\!]_v$ takes the code t of a pair term τ and the assignment v which is a list assigning the value $(v)_i$ to the variable x_i and yields the value of the term τ. The function is defined by *Term*-recursion on t as a primitive recursive function:

$$
\begin{aligned}
&[\![\mathbf{x}_i]\!]_v = (v)_i \\
&[\![\mathbf{0}]\!]_v = 0 \\
&[\![\mathbf{H}(t)]\!]_v = H([\![t]\!]_v) \\
&[\![\mathbf{T}(t)]\!]_v = T([\![t]\!]_v) \\
&[\![t_1 \,\mathbf{,}\, t_2]\!]_v = [\![t_1]\!]_v, [\![t_2]\!]_v \\
&[\![\mathbf{D}(t_1, t_2, t_3)]\!]_v = D([\![t_1]\!]_v, [\![t_2]\!]_v, [\![t_3]\!]_v).
\end{aligned}
$$

14.2.9 Coincidence of assignments. Consider the predicate $v_1 \equiv v_2\,[is]$ from Par. 14.1.9. The following holds

$$\vdash_{\mathrm{PA}} \mathit{Term}(t) \land FV(t) \subset is \land v_1 \equiv v_2\,[is] \to [\![t]\!]_{v_1} = [\![t]\!]_{v_2}. \tag{1}$$

Property (1) is proved by *Term*-induction on t (see the proof of 14.1.9(1)).

14.2.10 Postfix machine. Our next task is the proof of correctness of a simple postfix machine for evaluating pair terms. The machine is represented by the function $\mathit{Run}(p, v, s)$, where p is a list of instructions (program), v is an assignment (environment), and s is a list of values (I/O stack).

Instructions are defined with the help of the following constructors:

$$
\begin{aligned}
&\mathit{LOAD}(i) = 0, i \\
&\mathit{PUSHZ} = 1, 0 \\
&\mathit{HEAD} = 2, 0 \\
&\mathit{TAIL} = 3, 0 \\
&\mathit{PAIR} = 4, 0 \\
&\mathit{JUMPZ} = 5, 0 \\
&\mathit{JUMP} = 6, 0.
\end{aligned}
$$

The predicate $\mathit{Instr}(i)$ holds if i is an instruction of the postfix machine. The predicate is primitive recursive with the following explicit clausal definition:

$$
\begin{aligned}
&\mathit{Instr}\,\mathit{LOAD}(i) \\
&\mathit{Instr}(\mathit{PUSHZ}) \\
&\mathit{Instr}(\mathit{HEAD}) \\
&\mathit{Instr}(\mathit{TAIL}) \\
&\mathit{Instr}(\mathit{PAIR}) \\
&\mathit{Instr}(\mathit{JUMPZ}) \\
&\mathit{Instr}(\mathit{JUMP}).
\end{aligned}
$$

The predicate $\mathit{Program}(p)$ holds if p is a list of instructions. The predicate is defined by list recursion as a primitive recursive predicate:

$$
\begin{aligned}
&\mathit{Program}(0) \\
&\mathit{Program}(i, p) \leftarrow \mathit{Instr}(i) \land \mathit{Program}(p).
\end{aligned}
$$

Pair terms are compiled into programs by the function $Cmp(t)$. The function is defined by *Term*-recursion as a primitive recursive function:

$$
\begin{aligned}
&Cmp(\mathbf{x}_i) = LOAD(i), 0\\
&Cmp(\mathbf{0}) = PUSHZ, 0\\
&Cmp\,\mathbf{H}(t) = Cmp(t) \oplus (HEAD, 0)\\
&Cmp\,\mathbf{T}(t) = Cmp(t) \oplus (TAIL, 0)\\
&Cmp(t_1 \mathbf{,} t_2) = Cmp(t_1) \oplus Cmp(t_2) \oplus (PAIR, 0)\\
&Cmp\,\mathbf{D}(t_1, t_2, t_3) = p_1 \oplus p_2 \oplus p_3 \leftarrow\\
&\quad Cmp(t_1) = p_1 \wedge JUMPZ(L\,Cmp(t_2) + 1), Cmp(t_2) = p_2 \wedge\\
&\quad JUMP\;L\,Cmp(t_3), Cmp(t_3) = p_3.
\end{aligned}
$$

The function $Run(p, v, s)$ representing the postfix machine is defined by course of values recursion with measure $L(p)$ with substitution in parameter s as a primitive recursive function:

$$
\begin{aligned}
&Run(0, v, t, s) = t\\
&Run((LOAD(i), p), v, s) = Run(p, v, (v)_i, s)\\
&Run((PUSHZ, p), v, s) = Run(p, v, 0, s)\\
&Run((HEAD, p), v, t, s) = Run(p, v, H(t), s)\\
&Run((TAIL, p), v, t, s) = Run(p, v, T(t), s)\\
&Run((PAIR, p), v, t_2, t_1, s) = Run(p, v, (t_1, t_2), s)\\
&Run((JUMPZ(n), p), v, t, s) = Run(Drop(n, p), v, s) \leftarrow t = 0\\
&Run((JUMPZ(n), p), v, t, s) = Run(p, v, s) \leftarrow t \neq 0\\
&Run((JUMP(n), p), v, s) = Run(Drop(n, p), v, s).
\end{aligned}
$$

Finally, programs of the postfix machine are evaluated by

$$\vdash_{\mathrm{PAx}} Eval(p, v) = Run(p, v, 0).$$

The following property expresses the correctness of the evaluation function:

$$\vdash_{\mathrm{PA}} Term(t) \to Eval(Cmp(t), v) = [\![t]\!]_v. \tag{1}$$

To see this we first prove the property of the function *Run*:

$$\vdash_{\mathrm{PA}} Term(t) \to Run(Cmp(t) \oplus p, v, s) = Run(p, v, [\![t]\!]_v, s). \tag{2}$$

Property $\forall p \forall s(2)$ is proved by *Term*-induction on t. In the case when $t = \mathbf{D}(t_1, t_2, t_3)$ take any p, s and we have

$$
\begin{aligned}
&Run(Cmp\,\mathbf{D}(t_1, t_2, t_3) \oplus p, v, s) \stackrel{\text{def}}{=}\\
&\quad = Run\big(Cmp(t_1) \oplus (JUMPZ(L\,Cmp(t_2) + 1), Cmp(t_2)) \oplus\\
&\qquad\qquad \oplus (JUMP\;L\,Cmp(t_3), Cmp(t_3)) \oplus p, v, s\big) \stackrel{\text{IH}}{=}\\
&\quad = Run\big(JUMPZ(L\,Cmp(t_2) + 1), Cmp(t_2) \oplus\\
&\qquad\qquad \oplus (JUMP\;L\,Cmp(t_3), Cmp(t_3)) \oplus p, v, [\![t_1]\!]_v, s\big).
\end{aligned} \tag{3}
$$

We consider two subcases. If $[\![t_1]\!]_v = 0$ then we have

$$\begin{aligned}
&\mathit{Run}(\mathit{Cmp}\,\mathbf{D}(t_1,t_2,t_3)\oplus p,v,s) \overset{(3),\mathrm{def}}{=} \\
&\quad = \mathit{Run}\big(\mathit{Drop}(L\ \mathit{Cmp}(t_2)+1, \\
&\qquad\qquad\qquad \mathit{Cmp}(t_2)\oplus(\mathit{JUMP}\ L\ \mathit{Cmp}(t_3),\mathit{Cmp}(t_3))\oplus p,v,s\big) \overset{12.6.5(2)}{=} \\
&\quad = \mathit{Run}(\mathit{Cmp}(t_3)\oplus p,v,s) \overset{\mathrm{IH}}{=} \mathit{Run}(p,v,[\![t_3]\!]_v,s) = \\
&\quad = \mathit{Run}(p,v,D([\![t_1]\!]_v,[\![t_2]\!]_v,[\![t_3]\!]_v),s) = \mathit{Run}(p,v,[\![\mathbf{D}(t_1,t_2,t_3)]\!]_v,s).
\end{aligned}$$

If $[\![t_1]\!]_v \neq 0$ then we have

$$\begin{aligned}
&\mathit{Run}(\mathit{Cmp}\,\mathbf{D}(t_1,t_2,t_3)\oplus p,v,s) \overset{(3),\mathrm{def}}{=} \\
&\quad = \mathit{Run}(\mathit{Cmp}(t_2)\oplus(\mathit{JUMP}\ L\ \mathit{Cmp}(t_3),\mathit{Cmp}(t_3))\oplus p,v,s) \overset{\mathrm{IH}}{=} \\
&\quad = \mathit{Run}(\mathit{JUMP}\ L\ \mathit{Cmp}(t_3),\mathit{Cmp}(t_3)\oplus p,v,[\![t_2]\!]_v,s) \overset{\mathrm{def}}{=} \\
&\quad = \mathit{Run}(\mathit{Drop}(\mathit{JUMP}\ L\ \mathit{Cmp}(t_3),\mathit{Cmp}(t_3)\oplus p),v,[\![t_2]\!]_v,s) \overset{12.6.5(2)}{=} \\
&\quad = \mathit{Run}(p,v,[\![t_2]\!]_v,s) = \mathit{Run}(p,v,D([\![t_1]\!]_v,[\![t_2]\!]_v,[\![t_3]\!]_v),s) = \\
&\quad = \mathit{Run}(p,v,[\![\mathbf{D}(t_1,t_2,t_3)]\!]_v,s).
\end{aligned}$$

The remaining cases are left to the reader (see the proof of 14.1.10(2)).

We are now in position to prove (1). Assume $\mathit{Term}(t)$ and we have

$$\mathit{Eval}(\mathit{Cmp}(t),v) \overset{\mathrm{def}}{=} \mathit{Run}(\mathit{Cmp}(t),v,0) \overset{(2)}{=} \mathit{Run}(0,v,[\![t]\!]_v,0) \overset{\mathrm{def}}{=} [\![t]\!]_v.$$

14.3 Propositional Logic

14.3.1 Propositional formulas. Propositional formulas are formed from propositional constants $\top$ (true) and $\bot$ (falsehood), propositional variables p_i by the propositional connectives $\neg\phi$ (negation), $\phi_1 \wedge \phi_2$ (conjunction), $\phi_1 \vee \phi_2$ (disjunction), $\phi_1 \to \phi_2$ (implication), and $\phi_1 \leftrightarrow \phi_2$ (equivalence).

14.3.2 Arithmetization of propositional formulas. We arithmetize propositional formulas with the help of the following constructors:

$\mathbf{T} = 0, 0$
$\mathbf{\bot} = 1, 0$
$\mathbf{p}_i = 2, i$
$\boldsymbol{\neg} a = 3, a$
$a \boldsymbol{\wedge} b = 4, a, b$
$a \boldsymbol{\vee} b = 5, a, b$
$a \boldsymbol{\to} b = 6, a, b$
$a \boldsymbol{\leftrightarrow} b = 7, a, b.$

We assign to each propositional formula ϕ a number $\ulcorner\phi\urcorner$ called the code of ϕ. The mapping is defined inductively on the structure of propositional formulas:

$$\ulcorner\top\urcorner = \mathbf{T} \tag{1}$$
$$\ulcorner\bot\urcorner = \mathbf{\bot} \tag{2}$$
$$\ulcorner p_i\urcorner = \mathbf{p}_i \tag{3}$$
$$\ulcorner\neg\phi\urcorner = (\boldsymbol{\neg}\ulcorner\phi\urcorner) \tag{4}$$
$$\ulcorner\phi_1 \wedge \phi_2\urcorner = (\ulcorner\phi_1\urcorner \boldsymbol{\wedge} \ulcorner\phi_2\urcorner) \tag{5}$$
$$\ulcorner\phi_1 \vee \phi_2\urcorner = (\ulcorner\phi_1\urcorner \boldsymbol{\vee} \ulcorner\phi_2\urcorner) \tag{6}$$
$$\ulcorner\phi_1 \to \phi_2\urcorner = (\ulcorner\phi_1\urcorner \boldsymbol{\to} \ulcorner\phi_2\urcorner) \tag{7}$$
$$\ulcorner\phi_1 \leftrightarrow \phi_2\urcorner = (\ulcorner\phi_1\urcorner \boldsymbol{\leftrightarrow} \ulcorner\phi_2\urcorner). \tag{8}$$

The predicate $Form(a)$ holding of the codes of propositional formulas is defined by course of values recursion as a primitive recursive predicate:

$Form(\mathbf{T})$
$Form(\mathbf{\bot})$
$Form(\mathbf{p}_i)$
$Form(\boldsymbol{\neg} a) \leftarrow Form(a)$
$Form(a \boldsymbol{\wedge} b) \leftarrow Form(a) \wedge Form(b)$
$Form(a \boldsymbol{\vee} b) \leftarrow Form(a) \wedge Form(b)$
$Form(a \boldsymbol{\to} b) \leftarrow Form(a) \wedge Form(b)$
$Form(a \boldsymbol{\leftrightarrow} b) \leftarrow Form(a) \wedge Form(b).$

We identify propositional formulas with their codes and from now on we will say the *propositional formula* a instead of the *code of the propositional formula* a.

The predicate $Lform(as)$ holds if as is a list of propositional formulas. The predicate is defined by list recursion as a primitive recursive predicate:

$$
\begin{aligned}
&Lform(0)\\
&Lform(a, as) \leftarrow Form(a) \land Lform(as).
\end{aligned}
$$

14.3.3 Case analysis on propositional formulas. We have the following principle of *case analysis on propositional formulas*:

$$
\begin{aligned}
\vdash_{\mathrm{PA}}\ & Form(a) \rightarrow\\
& a = \mathbf{T} \lor a = \mathbf{\bot} \lor \exists i\, a = \mathbf{p}_i \lor \exists b\, a = (\mathbf{\neg} b) \lor \exists b \exists c\, a = (b \mathbin{\pmb{\land}} c) \lor \\
& \exists b \exists c\, a = (b \mathbin{\pmb{\lor}} c) \lor \exists b \exists c\, a = (b \mathbin{\pmb{\rightarrow}} c) \lor \exists b \exists c\, a = (b \mathbin{\pmb{\leftrightarrow}} c),
\end{aligned}
\tag{1}
$$

which is proved by a straightforward pair case analysis.

14.3.4 Structural induction on propositional formulas. The formula of *structural induction on the propositional formula a for* $\phi[a]$ is the following one:

$$
\begin{aligned}
&\phi[\mathbf{T}] \land \phi[\mathbf{\bot}] \land \forall i\, \phi[\mathbf{p}_i] \land \forall a(\phi[a] \rightarrow \phi[\mathbf{\neg} a]) \land \forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\land}} b]) \land \\
&\forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\lor}} b]) \land \forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\rightarrow}} b]) \land \\
&\forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\leftrightarrow}} b]) \rightarrow Form(a) \rightarrow \phi[a].
\end{aligned}
$$

In the sequel we will often say shortly the *Form-induction on a* instead of the structural induction on the propositional formula a.

14.3.5 Theorem. *We have*

$$
\begin{aligned}
\vdash_{PA}\ &\phi[\mathbf{T}] \land \phi[\mathbf{\bot}] \land \forall i\, \phi[\mathbf{p}_i] \land \forall a(\phi[a] \rightarrow \phi[\mathbf{\neg} a]) \land \forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\land}} b]) \land \\
&\forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\lor}} b]) \land \forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\rightarrow}} b]) \land \\
&\forall a \forall b(\phi[a] \land \phi[b] \rightarrow \phi[a \mathbin{\pmb{\leftrightarrow}} b]) \rightarrow Form(a) \rightarrow \phi[a].
\end{aligned}
$$

Proof. The property is proved by complete induction on a. Take any a and under the assumptions of the claim consider the cases according to 14.3.3(1). If $a = (b \mathbin{\pmb{\land}} b)$ for some b, c then we have $\phi[b]$ and $\phi[c]$ by IH since $b < b \mathbin{\pmb{\land}} c$ and $c < b \mathbin{\pmb{\land}} c$. From this and assumptions we get $\phi[b \mathbin{\pmb{\land}} c]$. The remaining cases are similar. ☐

14.3.6 Structural recursion on propositional formulas. Initial clauses for clausal definitions with *structural recursion on propositional formulas* are of a form

$$
\begin{aligned}
&f(\vec{y}, a, \vec{z}) = \alpha_1[\vec{y}, \vec{z}] \leftarrow a = \mathbf{T}\\
&f(\vec{y}, a, \vec{z}) = \alpha_2[\vec{y}, \vec{z}] \leftarrow a = \mathbf{\bot}\\
&f(\vec{y}, a, \vec{z}) = \alpha_3[\vec{y}, \vec{z}, i] \leftarrow a = \mathbf{p}_i\\
&f(\vec{y}, a, \vec{z}) = \alpha_4[\dot{\lambda} \vec{y} a \vec{z}. f(\vec{y}, b, \vec{z}); \vec{y}, \vec{z}, b] \leftarrow a = (\mathbf{\neg} b)
\end{aligned}
$$

$f(\vec{y},a,\vec{z}) = \alpha_5[\dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},b,\vec{z}), \dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},c,\vec{z}); \vec{y},\vec{z},b,c] \leftarrow a = (b \wedge c)$
$f(\vec{y},a,\vec{z}) = \alpha_6[\dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},b,\vec{z}), \dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},c,\vec{z}); \vec{y},\vec{z},b,c] \leftarrow a = (b \vee c)$
$f(\vec{y},a,\vec{z}) = \alpha_7[\dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},b,\vec{z}), \dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},c,\vec{z}); \vec{y},\vec{z},b,c] \leftarrow a = (b \rightarrow c)$
$f(\vec{y},a,\vec{z}) = \alpha_8[\dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},b,\vec{z}), \dot{\lambda}\vec{y}a\vec{z}.f(\vec{y},c,\vec{z}); \vec{y},\vec{z},b,c] \leftarrow a = (b \leftrightarrow c).$

In the sequel we will often say shortly the *Form-recursion on a* instead of the structural recursion on the propositional formula a.

14.3.7 Propositional size. The function $|a|_p$ counts the number of propositional connectives and propositional variables in the propositional formula a. The function is defined by *Form*-recursion as a primitive recursive function:

$|\top|_p = 1$
$|\bot|_p = 1$
$|\mathbf{p}_i|_p = 1$
$|\neg a|_p = |a|_p + 1$
$|a \wedge b|_p = |a|_p + |b|_p + 1$
$|a \vee b|_p = |a|_p + |b|_p + 1$
$|a \rightarrow b|_p = |a|_p + |b|_p + 1$
$|a \leftrightarrow b|_p = |a|_p + |b|_p + 1.$

The function $\|as\|_p$ computes the sum of the propositional sizes of formulas of the list as. The function is defined by list recursion as a primitive recursive function:

$\|0\|_p = 0$
$\|a, as\|_p = |a|_p + \|as\|_p.$

14.3.8 Propositional variables. The predicate $Lpvar(as)$ holds if as is a list of propositional variables, i.e.

$$\vdash_{\mathrm{PA}\times} Lpvar(as) \leftrightarrow \forall a(a \mathrel{\varepsilon} as \rightarrow \exists i\, a = \mathbf{p}_i).$$

The predicate satisfies the following easy to prove properties:

$$\vdash_{\mathrm{PA}} Lpvar(0) \tag{1}$$
$$\vdash_{\mathrm{PA}} Lpvar(a, as) \leftrightarrow \exists i\, a = \mathbf{p}_i \wedge Lpvar(as). \tag{2}$$

The function $PV(a)$ takes a propositional formula and returns a list of indices of propositional variables of the formula. The function is defined by *Form*-recursion as a primitive recursive function:

$PV(\top) = 0$
$PV(\bot) = 0$
$PV(\mathbf{p}_i) = i, 0$
$PV(\neg a) = PV(a)$
$PV(a \wedge b) = PV(a) \oplus PV(b)$
$PV(a \vee b) = PV(a) \oplus PV(b)$

$PV(a \rightarrow b) = PV(a) \oplus PV(b)$
$PV(a \leftrightarrow b) = PV(a) \oplus PV(b)$.

The function $PVL(as)$ returns the list union of indices of the propositional variables of the list of formulas as. The function is defined by list recursion as a primitive recursive function:

$PVL(0) = 0$
$PVL(a, as) = PV(a) \oplus PVL(as)$.

14.3.9 Truth predicate. The predicate $v \models_p a$ holds if the propositional formula a is true in the propositional valuation v. The predicate is defined by *Form*-recursion on a as a primitive recursive predicate:

$v \models_p \mathbf{T}$
$v \models_p \mathbf{p}_i \leftarrow i \,\varepsilon\, v$
$v \models_p (\neg a) \leftarrow v \not\models_p a$
$v \models_p (a \wedge b) \leftarrow v \models_p a \wedge v \models_p b$
$v \models_p (a \vee b) \leftarrow v \models_p a$
$v \models_p (a \vee b) \leftarrow v \not\models_p a \wedge v \models_p b$
$v \models_p (a \rightarrow b) \leftarrow v \not\models_p a$
$v \models_p (a \rightarrow b) \leftarrow v \models_p a \wedge v \models_p b$
$v \models_p (a \leftrightarrow b) \leftarrow v \models_p a \wedge v \models_p b$
$v \models_p (a \leftrightarrow b) \leftarrow v \not\models_p a \wedge v \not\models_p b$.

The predicate has the following easy to prove properties:

$$\vdash_{\text{PA}} v \models_p \mathbf{T} \tag{1}$$
$$\vdash_{\text{PA}} v \not\models_p \bot \tag{2}$$
$$\vdash_{\text{PA}} v \models_p \mathbf{p}_i \leftrightarrow i \,\varepsilon\, v \tag{3}$$
$$\vdash_{\text{PA}} v \models_p (\neg a) \leftrightarrow v \not\models_p a \tag{4}$$
$$\vdash_{\text{PA}} v \models_p (a \wedge b) \leftrightarrow v \models_p a \wedge v \models_p b \tag{5}$$
$$\vdash_{\text{PA}} v \models_p (a \vee b) \leftrightarrow v \models_p a \vee v \models_p b \tag{6}$$
$$\vdash_{\text{PA}} v \models_p (a \rightarrow b) \leftrightarrow v \models_p a \rightarrow v \models_p b \tag{7}$$
$$\vdash_{\text{PA}} v \models_p (a \leftrightarrow b) \leftrightarrow v \models_p a \leftrightarrow v \models_p b. \tag{8}$$

14.3.10 Coincidence of propositional valuations. The ternary predicate $v_1 \equiv v_2\,[is]$ holds if the propositional valuations v_1 and v_2 coincide on every propositional variable whose index is in the list is, i.e.

$$\vdash_{\text{PAx}} v_1 \equiv v_2\,[is] \leftrightarrow \forall i (i \,\varepsilon\, a \rightarrow i \,\varepsilon\, v_1 \leftrightarrow i \,\varepsilon\, v_2).$$

The following holds

$$\vdash_{\text{PA}} \mathit{Form}(a) \wedge PV(a) \subset is \wedge v_1 \equiv v_2\,[is] \rightarrow v_1 \models_p a \leftrightarrow v_2 \models_p a. \tag{1}$$

Property (1) is proved by *Form*-induction on a. For instance, if $a = \mathbf{p}_i$ then

$$v_1 \models_p \mathbf{p}_i \overset{14.3.9(3)}{\Leftrightarrow} i \,\varepsilon\, v_1 \overset{\text{def}}{\Leftrightarrow} i \,\varepsilon\, v_2 \overset{14.3.9(3)}{\Leftrightarrow} v_2 \models_p \mathbf{p}_i.$$

If $a = (b \mathbin{\pmb{\wedge}} c)$ then $PV(b) \subset is$ and $PV(c) \subset is$ by 14.0.8(3) and we obtain

$$\begin{aligned} &v_1 \models_p (b \mathbin{\pmb{\wedge}} c) \overset{14.3.9(5)}{\Leftrightarrow} v_1 \models_p b \wedge v_1 \models_p c \overset{\text{IH}}{\Leftrightarrow} \\ &v_2 \models_p b \wedge v_2 \models_p c \overset{14.3.9(5)}{\Leftrightarrow} v_2 \models_p (b \mathbin{\pmb{\wedge}} c). \end{aligned}$$

The remaining cases are similar.

14.3.11 Tautologies. A propositional formula a is said to be a tautology, which is written as $\models_p a$, if it is true in any propositional valuation. The predicate $\models_p a$ has the following explicit definition:

$$\vdash_{\text{PAx}} \models_p a \leftrightarrow \forall v\, v \models_p a.$$

14.3.12 Generalized connectives. The generalized conjunction $\bigwedge(as)$ is defined by list recursion as a primitive recursive function:

$$\begin{aligned} &\bigwedge(0) = \mathbf{T} \\ &\bigwedge(a, as) = a \mathbin{\pmb{\wedge}} \bigwedge(as). \end{aligned}$$

We have

$$\vdash_{\text{PA}} Lform(as) \to Form \bigwedge(as) \tag{1}$$

$$\vdash_{\text{PA}} v \models_p \bigwedge(as) \leftrightarrow \forall a(a \,\varepsilon\, as \to v \models_p a) \tag{2}$$

$$\vdash_{\text{PA}} v \models_p \bigwedge(as \oplus bs) \leftrightarrow v \models_p \bigwedge(as) \wedge v \models_p \bigwedge(bs). \tag{3}$$

Properties are proved by straightforward list induction.

The generalized disjunction $\bigvee(as)$ is defined by list recursion as a primitive recursive function:

$$\begin{aligned} &\bigvee(0) = \pmb{\perp} \\ &\bigvee(a, as) = a \mathbin{\pmb{\vee}} \bigvee(as). \end{aligned}$$

We have

$$\vdash_{\text{PA}} Lform(as) \to Form \bigvee(as) \tag{4}$$

$$\vdash_{\text{PA}} v \models_p \bigvee(as) \leftrightarrow \exists a(a \,\varepsilon\, as \wedge v \models_p a) \tag{5}$$

$$\vdash_{\text{PA}} v \models_p \bigvee(as \oplus bs) \leftrightarrow v \models_p \bigvee(as) \vee v \models_p \bigvee(bs). \tag{6}$$

Properties are proved by straightforward list induction.

14.3.13 Propositional sequents. A propositional sequent is an ordered pair

$$\langle as, bs\rangle \tag{1}$$

where as and bs are lists of propositional formulas. The list as is called the antecedent of the sequent (1); the list bs its succedent. The meaning of the sequent (1) is the formula

$$\bigwedge(as) \rightarrow \bigvee(bs)\ . \tag{2}$$

The sequent (1) is said to be a tautology, which is written as $as \models_p bs$, if the corresponding formula (2) is. The predicate $as \models_p bs$ has the following explicit definition:

$$\vdash_{\text{PAx}}\ as \models_p bs \leftrightarrow\ \models_p (\bigwedge(as) \rightarrow \bigvee(bs)).$$

Propositional sequents which antecedents and succedents consist only of propositional variables are called atomic propositional sequents.

14.3.14 Basic properties of propositional sequents. We have

$$\begin{aligned}
&\vdash_{\text{PA}}\ \models_p a \leftrightarrow 0 \models_p a, 0 && (1)\\
&\vdash_{\text{PA}}\ as_1 \oplus (a, as_2) \models_p bs \leftrightarrow a, as_1 \oplus as_2 \models_p bs && (2)\\
&\vdash_{\text{PA}}\ as \models_p bs_1 \oplus (b, bs_2) \leftrightarrow as \models_p b, bs_1 \oplus bs_2 && (3)\\
&\vdash_{\text{PA}}\ \mathbf{T}, as \models_p bs \leftrightarrow as \models_p bs && (4)\\
&\vdash_{\text{PA}}\ as \models_p \mathbf{T}, bs && (5)\\
&\vdash_{\text{PA}}\ \bot, as \models_p bs && (6)\\
&\vdash_{\text{PA}}\ as \models_p \bot, bs \leftrightarrow as \models_p bs && (7)\\
&\vdash_{\text{PA}}\ \mathbf{p}_i, as \models_p \mathbf{p}_i, bs && (8)\\
&\vdash_{\text{PA}}\ \neg a, as \models_p bs \leftrightarrow as \models_p a, bs && (9)\\
&\vdash_{\text{PA}}\ as \models_p \neg a, bs \leftrightarrow a, as \models_p bs && (10)\\
&\vdash_{\text{PA}}\ a \wedge b, as \models_p bs \leftrightarrow a, b, as \models_p bs && (11)\\
&\vdash_{\text{PA}}\ as \models_p a \wedge b, bs \leftrightarrow as \models_p a, bs \wedge as \models_p b, bs && (12)\\
&\vdash_{\text{PA}}\ a \vee b, as \models_p bs \leftrightarrow a, as \models_p bs \wedge b, as \models_p bs && (13)\\
&\vdash_{\text{PA}}\ as \models_p a \vee b, bs \leftrightarrow as \models_p a, b, bs && (14)\\
&\vdash_{\text{PA}}\ a \rightarrow b, as \models_p bs \leftrightarrow as \models_p a, bs \wedge b, as \models_p bs && (15)\\
&\vdash_{\text{PA}}\ as \models_p a \rightarrow b, bs \leftrightarrow a, as \models_p b, bs && (16)\\
&\vdash_{\text{PA}}\ a \leftrightarrow b, as \models_p bs \leftrightarrow as \models_p a, b, bs \wedge a, b, as \models_p bs && (17)\\
&\vdash_{\text{PA}}\ as \models_p a \leftrightarrow b, bs \leftrightarrow a, as \models_p b, bs \wedge b, as \models_p a, bs. && (18)
\end{aligned}$$

For instance, the property (9) is proved as follows:

$$\neg a, as \models_p bs \overset{\text{def}}{\Leftrightarrow} \forall v\, v \models_p \big(\neg a \land \bigwedge(as) \to \bigvee(bs)\big) \overset{14.3.9(7)}{\Leftrightarrow}$$
$$\forall v\Big(v \models_p \big(\neg a \land \bigwedge(as)\big) \to v \models_p \bigvee(bs)\Big) \overset{14.3.9(5)}{\Leftrightarrow}$$
$$\forall v\big(v \models_p (\neg a) \land v \models_p \bigwedge(as) \to v \models_p \bigvee(bs)\big) \overset{14.3.9(4)}{\Leftrightarrow}$$
$$\forall v\big(v \not\models_p a \land v \models_p \bigwedge(as) \to v \models_p \bigvee(bs)\big) \Leftrightarrow$$
$$\forall v\big(v \models_p \bigwedge(as) \to v \models_p a \lor v \models_p \bigvee(bs)\big) \overset{14.3.9(6)}{\Leftrightarrow}$$
$$\forall v\Big(v \models_p \bigwedge(as) \to v \models_p \big(a \lor \bigvee(bs)\big)\Big) \overset{14.3.9(7)}{\Leftrightarrow}$$
$$\forall v\, v \models_p \big(\bigwedge(as) \to a \lor \bigvee(bs)\big) \overset{\text{def}}{\Leftrightarrow} as \models_p a, bs.$$

The remaining properties are proved similarly.

14.3.15 Main lemma for atomic propositional sequents. We have

$$\vdash_{\text{PA}} Lpvar(as) \land Lpvar(bs) \to as \models_p bs \leftrightarrow \exists i(\mathbf{p}_i \mathrel{\varepsilon} as \land \mathbf{p}_i \mathrel{\varepsilon} bs). \tag{1}$$

First note that the following holds

$$\vdash_{\text{PA}} Lpvar(as) \to PVL(as) \models_p \mathbf{p}_i \leftrightarrow \mathbf{p}_i \mathrel{\varepsilon} as \tag{2}$$
$$\vdash_{\text{PA}} Lpvar(as) \to PVL(as) \models_p \bigwedge(as) \tag{3}$$
$$\begin{aligned}&\vdash_{\text{PA}} Lpvar(as) \land Lpvar(bs) \to \\ &\qquad PVL(as) \models_p \bigvee(bs) \leftrightarrow \exists i(\mathbf{p}_i \mathrel{\varepsilon} as \land \mathbf{p}_i \mathrel{\varepsilon} bs).\end{aligned} \tag{4}$$

Property (2) is proved by list induction on as. The base case is straightforward. In the inductive case, when $as = b, bs$, we obtain from assumptions and 14.3.8(2) that $b = \mathbf{p}_j$ for some j. Thus

$$PVL(\mathbf{p}_j, bs) \models_p \mathbf{p}_i \Leftrightarrow PV(\mathbf{p}_j) \oplus PVL(bs) \models_p \mathbf{p}_i \Leftrightarrow j, PVL(bs) \models_p \mathbf{p}_i \Leftrightarrow$$
$$i \mathrel{\varepsilon} j, PVL(bs) \Leftrightarrow i = j \lor i \mathrel{\varepsilon} PVL(bs) \Leftrightarrow \mathbf{p}_i = \mathbf{p}_j \lor PVL(bs) \models_p \mathbf{p}_i \overset{\text{IH}}{\Leftrightarrow}$$
$$\mathbf{p}_i = \mathbf{p}_j \lor \mathbf{p}_i \mathrel{\varepsilon} bs \Leftrightarrow \mathbf{p}_i \mathrel{\varepsilon} \mathbf{p}_j, bs.$$

Property (3) follows from

$$PVL(as) \models_p \bigwedge(as) \overset{14.3.12(2)}{\Leftrightarrow} \forall a(a \mathrel{\varepsilon} as \to PVL(as) \models_p a) \Leftrightarrow$$
$$\forall i(\mathbf{p}_i \mathrel{\varepsilon} as \to PVL(as) \models_p \mathbf{p}_i) \overset{(2)}{\Leftrightarrow} \forall i(\mathbf{p}_i \mathrel{\varepsilon} as \to \mathbf{p}_i \mathrel{\varepsilon} as).$$

The last holds trivially. Property (4) is proved similarly.

In the proof of the $(\to)$-direction of (1) we get $PVL(as) \models_p \bigwedge(as) \to \bigvee(bs)$ from assumptions and thus $PVL(as) \models_p \bigvee(bs)$ by (3). The claim now follows from (4). The $(\leftarrow)$-direction is proved as follows. From assumptions and

12.6.1(1) we obtain that $as = as_1 \oplus (\mathbf{p}_i, as_2)$ and $bs = bs_1 \oplus (\mathbf{p}_i, bs_2)$ for some i, as_1, as_2, bs_1, and bs_2. The claim now follows from 14.3.14(8) since we have

$$as_1 \oplus (\mathbf{p}_i, as_2) \models_p bs_1 \oplus (\mathbf{p}_i, bs_2) \overset{14.3.14(2)(3)}{\Leftrightarrow} \mathbf{p}_i, as_1 \oplus as_2 \models_p \mathbf{p}_i, bs_1 \oplus bs_2.$$

14.3.16 Tautology checker for atomic propositional sequents. Consider the predicate $Closes(as, bs)$ defined by list recursion on as as a primitive recursive predicate:

$$\begin{aligned}
&Closes((a, as), bs) \leftarrow a \,\varepsilon\, bs \\
&Closes((a, as), bs) \leftarrow a \not\varepsilon\, bs \land Closes(as, bs).
\end{aligned}$$

We have

$$\vdash_{\mathrm{PA}} Closes(as, bs) \leftrightarrow \exists c(c \,\varepsilon\, as \land c \,\varepsilon\, bs) \tag{1}$$

$$\vdash_{\mathrm{PA}} Lpvar(as) \land Lpvar(bs) \to Closes(as, bs) \leftrightarrow as \models_p bs. \tag{2}$$

Property (1) is proved by list induction on as. Property (2) follows from (1) and 14.3.15(1).

14.3.17 Auxiliary predicate. The predicate $as \oplus bs \vdash_p cs \oplus ds$ satisfies

$$\begin{aligned}
&\vdash_{\mathrm{PA}} Lform(as) \land Lpvar(bs) \land Lform(cs) \land Lpvar(ds) \to \\
&\qquad as \oplus bs \vdash_p cs \oplus ds \leftrightarrow as \oplus bs \models_p cs \oplus ds
\end{aligned} \tag{1}$$

and it is defined by course of values recursion with measure $\|as\|_p + \|cs\|_p$ with substitution in parameters as a primitive recursive predicate:

$$\begin{aligned}
&0 \oplus bs \vdash_p 0 \oplus ds \leftarrow Closes(bs, ds) \\
&0 \oplus bs \vdash_p (\top, cs) \oplus ds \\
&0 \oplus bs \vdash_p (\bot, cs) \oplus ds \leftarrow 0 \oplus bs \vdash_p cs \oplus ds \\
&0 \oplus bs \vdash_p (\mathbf{p}_i, cs) \oplus ds \leftarrow 0 \oplus bs \vdash_p cs \oplus (\mathbf{p}_i, ds) \\
&0 \oplus bs \vdash_p (\neg a, cs) \oplus ds \leftarrow (a, 0) \oplus bs \vdash_p cs \oplus ds \\
&0 \oplus bs \vdash_p (a \land b, cs) \oplus ds \leftarrow 0 \oplus bs \vdash_p (a, cs) \oplus ds \land 0 \oplus bs \vdash_p (b, cs) \oplus ds \\
&0 \oplus bs \vdash_p (a \lor b, cs) \oplus ds \leftarrow 0 \oplus bs \vdash_p (a, b, cs) \oplus ds \\
&0 \oplus bs \vdash_p (a \to b, cs) \oplus ds \leftarrow (a, 0) \oplus bs \vdash_p (b, cs) \oplus ds \\
&0 \oplus bs \vdash_p (a \leftrightarrow b, cs) \oplus ds \leftarrow \\
&\quad (a, 0) \oplus bs \vdash_p (b, cs) \oplus ds \land (b, 0) \oplus bs \vdash_p (a, cs) \oplus ds \\
&(\top, as) \oplus bs \vdash_p cs \oplus ds \leftarrow as \oplus bs \vdash_p cs \oplus ds \\
&(\bot, as) \oplus bs \vdash_p cs \oplus ds \\
&(\mathbf{p}_i, as) \oplus bs \vdash_p cs \oplus ds \leftarrow as \oplus (\mathbf{p}_i, bs) \vdash_p cs \oplus ds \\
&(\neg a, as) \oplus bs \vdash_p cs \oplus ds \leftarrow as \oplus bs \vdash_p (a, cs) \oplus ds \\
&(a \land b, as) \oplus bs \vdash_p cs \oplus ds \leftarrow (a, b, as) \oplus bs \vdash_p cs \oplus ds \\
&(a \lor b, as) \oplus bs \vdash_p cs \oplus ds \leftarrow \\
&\quad (a, as) \oplus bs \vdash_p cs \oplus ds \land (b, as) \oplus bs \vdash_p cs \oplus ds \\
&(a \to b, as) \oplus bs \vdash_p cs \oplus ds \leftarrow
\end{aligned}$$

$$as \oplus bs \vdash_p (a, cs) \oplus ds \land (b, as) \oplus bs \vdash_p cs \oplus ds$$
$$(a \leftrightarrow b, as) \oplus bs \vdash_p cs \oplus ds \leftarrow$$
$$as \oplus bs \vdash_p (a, b, cs) \oplus ds \land (a, b, as) \oplus bs \vdash_p cs \oplus ds.$$

Property $\forall bs \forall ds(1)$ is proved by induction with measure $\|as\|_p + \|cs\|_p$. So take any as, bs, cs, and ds, and under the assumptions of the claim consider two cases.

If $as = 0$ then we consider two subcases. If $cs = 0$ then we have

$$0 \oplus bs \vdash_p 0 \oplus ds \overset{\text{def}}{\Leftrightarrow} Closes(bs, ds) \overset{14.3.16(2)}{\Leftrightarrow} bs \models_p ds \Leftrightarrow 0 \oplus bs \models_p 0 \oplus ds.$$

If $cs = a, cs_1$ for some a and cs_1 then we do the case analysis on the structure of the propositional formula a. If $a = \top$ then the claim follows from 14.3.14(5). If $a = \bot$ then we have

$$0 \oplus bs \vdash_p (\bot, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow} 0 \oplus bs \vdash_p cs_1 \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$0 \oplus bs \models_p cs_1 \oplus ds \overset{14.3.14(7)}{\Leftrightarrow} 0 \oplus bs \models_p (\bot, cs_1) \oplus ds.$$

If $a = \mathbf{p}_i$ then we have

$$0 \oplus bs \vdash_p (\mathbf{p}_i, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow} 0 \oplus bs \vdash_p cs_1 \oplus (\mathbf{p}_i, ds) \overset{\text{IH}}{\Leftrightarrow}$$
$$0 \oplus bs \models_p cs_1 \oplus (\mathbf{p}_i, ds) \overset{14.3.14(3)}{\Leftrightarrow} 0 \oplus bs \models_p (\mathbf{p}_i, cs_1) \oplus ds.$$

If $a = (\neg b)$ for some b then we have

$$0 \oplus bs \vdash_p (\neg b, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow} (b, 0) \oplus bs \vdash_p cs_1 \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$(b, 0) \oplus bs \models_p cs_1 \oplus ds \overset{14.3.14(10)}{\Leftrightarrow} 0 \oplus bs \models_p (\neg b, cs_1) \oplus ds.$$

If $a = (b \land c)$ for some b and c then we have

$$0 \oplus bs \vdash_p (b \land c, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow}$$
$$0 \oplus bs \vdash_p (b, cs_1) \oplus ds \land 0 \oplus bs \vdash_p (c, cs_1) \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$0 \oplus bs \models_p (b, cs_1) \oplus ds \land 0 \oplus bs \models_p (c, cs_1) \oplus ds \overset{14.3.14(12)}{\Leftrightarrow}$$
$$0 \oplus bs \models_p (b \land c, cs_1) \oplus ds.$$

If $a = (b \lor c)$ for some b and c then we have

$$0 \oplus bs \vdash_p (b \lor c, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow} 0 \oplus bs \vdash_p (b, c, cs_1) \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$0 \oplus bs \models_p (b, c, cs_1) \oplus ds \overset{14.3.14(14)}{\Leftrightarrow} 0 \oplus bs \models_p (b \lor c, cs_1) \oplus ds.$$

If $a = (b \rightarrow c)$ for some b and c then we have

$$0 \oplus bs \vdash_p (b \to c, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow} (b,0) \oplus bs \vdash_p (c, cs_1) \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$(b,0) \oplus bs \models_p (c, cs_1) \oplus ds \overset{14.3.14(16)}{\Leftrightarrow} 0 \oplus bs \models_p (b \to c, cs_1) \oplus ds.$$

If $a = (b \leftrightarrow c)$ for some b and c then we have

$$0 \oplus bs \vdash_p (b \leftrightarrow c, cs_1) \oplus ds \overset{\text{def}}{\Leftrightarrow}$$
$$(b,0) \oplus bs \vdash_p (c, cs_1) \oplus ds \wedge (c,0) \oplus bs \vdash_p (b, cs_1) \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$(b,0) \oplus bs \models_p (c, cs_1) \oplus ds \wedge (c,0) \oplus bs \models_p (b, cs_1) \oplus ds \overset{14.3.14(18)}{\Leftrightarrow}$$
$$0 \oplus bs \models_p (b \leftrightarrow c, cs_1) \oplus ds.$$

If $as = a, as_1$ for some a and as_1 then we do the case analysis on the structure of the propositional formula a. If $a = \mathbf{T}$ then we have

$$(\mathbf{T}, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow} as_1 \oplus bs \vdash_p cs \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$as_1 \oplus bs \models_p cs \oplus ds \overset{14.3.14(4)}{\Leftrightarrow} (\mathbf{T}, as_1) \oplus bs \models_p cs \oplus ds.$$

If $a = \bot$ then the claim follows from 14.3.14(6). If $a = \mathbf{p}_i$ then we have

$$(\mathbf{p}_i, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow} as_1 \oplus (\mathbf{p}_i, bs) \vdash_p cs \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$as_1 \oplus (\mathbf{p}_i, bs) \models_p cs \oplus ds \overset{14.3.14(2)}{\Leftrightarrow} (\mathbf{p}_i, as_1) \oplus bs \models_p cs \oplus ds.$$

If $a = (\neg b)$ for some b then we have

$$(\neg b, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow} as_1 \oplus bs \vdash_p (b, cs) \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$as_1 \oplus bs \models_p (b, cs) \oplus ds \overset{14.3.14(9)}{\Leftrightarrow} (\neg b, as_1) \oplus bs \models_p cs \oplus ds.$$

If $a = (b \wedge c)$ for some b and c then we have

$$(b \wedge c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow} (b, c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$(b, c, as_1) \oplus bs \models_p cs \oplus ds \overset{14.3.14(11)}{\Leftrightarrow} (b \wedge c, as_1) \oplus bs \models_p cs \oplus ds.$$

If $a = (b \vee c)$ for some b and c then we have

$$(b \vee c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow}$$
$$(b, as_1) \oplus bs \vdash_p cs \oplus ds \wedge (c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{IH}}{\Leftrightarrow}$$
$$(b, as_1) \oplus bs \models_p cs \oplus ds \wedge (c, as_1) \oplus bs \models_p cs \oplus ds \overset{14.3.14(13)}{\Leftrightarrow}$$
$$(b \vee c, as_1) \oplus bs \models_p cs \oplus ds.$$

If $a = (b \to c)$ for some b and c then we have

$$
\begin{aligned}
&(b \to c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow} \\
&as_1 \oplus bs \vdash_p (b, cs) \oplus ds \land (c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{IH}}{\Leftrightarrow} \\
&as_1 \oplus bs \models_p (b, cs) \oplus ds \land (c, as_1) \oplus bs \models_p cs \oplus ds \overset{14.3.14(15)}{\Leftrightarrow} \\
&(b \to c, as_1) \oplus bs \models_p cs \oplus ds.
\end{aligned}
$$

If $a = (b \leftrightarrow c)$ for some b and c then we have

$$
\begin{aligned}
&(b \leftrightarrow c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{def}}{\Leftrightarrow} \\
&as_1 \oplus bs \vdash_p (b, c, cs) \oplus ds \land (b, c, as_1) \oplus bs \vdash_p cs \oplus ds \overset{\text{IH}}{\Leftrightarrow} \\
&as_1 \oplus bs \models_p (b, c, cs) \oplus ds \land (b, c, as_1) \oplus bs \models_p cs \oplus ds \overset{14.3.14(17)}{\Leftrightarrow} \\
&(b \leftrightarrow c, as_1) \oplus bs \models_p cs \oplus ds.
\end{aligned}
$$

14.3.18 Tautology checker for propositional sequents. Consider the predicate $as \vdash_p bs$ defined explicitly as a primitive recursive predicate:

$$\models_{\mathrm{PAx}} \; as \vdash_p bs \leftrightarrow as \oplus 0 \vdash_p bs \oplus 0.$$

We have

$$\models_{\mathrm{PA}} \; \mathit{Lform}(as) \land \mathit{Lform}(bs) \to as \vdash_p bs \leftrightarrow as \models_p bs. \tag{1}$$

Property (1) follows from 14.3.17(1).

14.3.19 Tautology checker. Consider the predicate $\vdash_p a$ defined explicitly as a primitive recursive predicate:

$$\models_{\mathrm{PAx}} \; \vdash_p a \leftrightarrow 0 \vdash_p a, 0.$$

We have

$$\models_{\mathrm{PA}} \; \mathit{Form}(a) \to \vdash_p a \leftrightarrow \models_p a. \tag{1}$$

Property (1) follows from 14.3.14(1) and 14.3.18(1).

14.4 Exercises

14.4.1 Exercise. Additive numeric terms are formed from variables and constants by applications of addition. The predicate $Term(t)$ holding of the codes of additive numeric terms is defined by course of values recursion as a primitive recursive predicate:

$$
\begin{aligned}
&Term(\mathbf{x}_i)\\
&Term(\overline{n})\\
&Term(t_1 \mathbin{\pmb{+}} t_2) \leftarrow Term(t_1) \wedge Term(t_2).
\end{aligned}
$$

The denotation function $[\![t]\!]_v$ for additive numeric terms is defined by *Term*-recursion on t as a primitive recursive function:

$$
\begin{aligned}
&[\![\mathbf{x}_i]\!]_v = (v)_i\\
&[\![\overline{n}]\!]_v = n\\
&[\![t_1 \mathbin{\pmb{+}} t_2]\!]_v = [\![t_1]\!]_v + [\![t_2]\!]_v.
\end{aligned}
$$

The predicate $Lassoc(t)$ holds if the additive numeric term t is left associative w.r.t. addition. The predicate is defined by *Term*-induction as a primitive recursive predicate:

$$
\begin{aligned}
&Lassoc(\mathbf{x}_i)\\
&Lassoc(\overline{n})\\
&Lassoc(t_1 \mathbin{\pmb{+}} \mathbf{x}_i) \leftarrow Lassoc(t_1)\\
&Lassoc(t_1 \mathbin{\pmb{+}} \overline{n}) \leftarrow Lassoc(t_1).
\end{aligned}
$$

Consider the primitive recursive function $f(t)$ defined by course of values recursion with measure $m(t)$:

$$
\begin{aligned}
&f(\mathbf{x}_i) = \mathbf{x}_i\\
&f(\overline{n}) = \overline{n}\\
&f(t_1 \mathbin{\pmb{+}} \mathbf{x}_i) = f(t_1) \mathbin{\pmb{+}} \mathbf{x}_i\\
&f(t_1 \mathbin{\pmb{+}} \overline{n}) = f(t_1) \mathbin{\pmb{+}} \overline{n}\\
&f(t_1 \mathbin{\pmb{+}} (t_2 \mathbin{\pmb{+}} t_3)) = f(t_1 \mathbin{\pmb{+}} t_2 \mathbin{\pmb{+}} t_3),
\end{aligned}
$$

where

$$
\begin{aligned}
&m(\mathbf{x}_i) = 1\\
&m(\overline{n}) = 1\\
&m(t_1 \mathbin{\pmb{+}} t_2) = m(t_1) + 2 \cdot m(t_2) + 1.
\end{aligned}
$$

Prove

$$
\begin{aligned}
&\vdash_{\mathrm{PA}} Term(t) \to Term\, f(t)\\
&\vdash_{\mathrm{PA}} Term(t) \to Lassoc\, f(t)\\
&\vdash_{\mathrm{PA}} Term(t) \to [\![f(t)]\!]_v = [\![t]\!]_v.
\end{aligned}
$$

14.4.2 Exercise. Numeric terms in one variable are formed from the variable x and constants by applications of addition and multiplication. The predicate $\mathit{Term}(t)$ holding of the codes of numeric terms in one variable is defined by course of values recursion as a primitive recursive predicate:

$$\begin{aligned}
&\mathit{Term}(\mathbf{x})\\
&\mathit{Term}(\overline{n})\\
&\mathit{Term}(t_1 \mathbin{\pmb{+}} t_2) \leftarrow \mathit{Term}(t_1) \wedge \mathit{Term}(t_2)\\
&\mathit{Term}(t_1 \mathbin{\pmb{\times}} t_2) \leftarrow \mathit{Term}(t_1) \wedge \mathit{Term}(t_2).
\end{aligned}$$

The denotation function $[\![t]\!]_x$ for numeric terms in one variables is defined by Term-recursion on t as a primitive recursive function:

$$\begin{aligned}
&[\![\mathbf{x}]\!]_x = x\\
&[\![\overline{n}]\!]_x = n\\
&[\![t_1 \mathbin{\pmb{+}} t_2]\!]_x = [\![t_1]\!]_x + [\![t_2]\!]_x\\
&[\![t_1 \mathbin{\pmb{\times}} t_2]\!]_x = [\![t_1]\!]_x \cdot [\![t_2]\!]_x.
\end{aligned}$$

Define the function $f(t)$ translating a numeric term t in one variable into an equivalent polynomial, i.e.

$$\vdash_{\mathrm{PA}} \mathit{Term}(t) \rightarrow f(t)(x) = [\![t]\!]_x.$$

Prove that the function has the required property.

15. Programs Operating on Arrays

15.1 Basic operations on arrays

15.1.1 Arrays.

Array predicate. The binary predicate $\mathit{Array}(n, a)$ holds if a is an array of the length n.

Array indexing. The array indexing function $a[i]$ subscribes the array a at the index i.

Array modification. The array modification function $a[i := x]$ modifies the array a at the index i to obtain the new value x. The function has the following properties:

$$\mathit{Array}(n, a) \wedge i < n \to \mathit{Array}(n, a[i := x]) \tag{1}$$
$$\mathit{Array}(n, a) \wedge i < n \to a[i := x][i] = x \tag{2}$$
$$\mathit{Array}(n, a) \wedge i < n \to \forall j(j < n \wedge j \neq i \to a[i := x][j] = a[j]) \ . \tag{3}$$

New array. The function $\mathit{New}(n)$ creates a new array of the length n. The function has the following property:

$$\mathit{Array}(n, \mathit{New}(n)) \ . \tag{4}$$

15.1.2 Exercise. Define a function $\mathit{Fill}(x, n)$ satisfying

$$\mathit{Array}(n, \mathit{Fill}(x, n)) \tag{1}$$
$$i < n \to \mathit{Fill}(x, n)[i] = x \ . \tag{2}$$

Prove that the function has the required properties.

Hint. Define $\mathit{Fill}(x, n)$ as follows

$$\begin{aligned}
&\mathit{Fill}_1(x, 0, a) = a \\
&\mathit{Fill}_1(x, i + 1, a) = \mathit{Fill}_1(x, i, a[i := x]) \\
&\mathit{Fill}(x, n) = \mathit{Fill}_1(x, n, \mathit{New}(n)) \quad ,
\end{aligned}$$

where the function $\mathit{Fill}_1(x, i, a)$ is defined by primitive recursion on i with substitution in parameter a. Prove first the following properties of the auxiliary function:

$$Array(n,a) \wedge i \le n \to Array(n, Fill_1(x,i,a)) \tag{3}$$

$$\begin{aligned} &Array(n,a) \wedge i \le n \wedge j < n \to \\ &\qquad (j < i \to Fill_1(x,i,a)[j] = x) \wedge (j \ge i \to Fill_1(x,i,a)[j] = a[j]) \ . \end{aligned} \tag{4}$$

15.1.3 Position. The predicate $Pos(x,i,n,a)$ holds if $i < n$ and x is the value of the array a at the index i, ie

$$Pos(x,i,n,a) \leftrightarrow i < n \wedge a[i] = x \ .$$

The predicate has the following properties:

$$\neg Pos(x,i,0,a) \tag{1}$$
$$Pos(x,i,n+1,a) \leftrightarrow i = n \wedge a[i] = x \vee Pos(x,i,n,a) \ . \tag{2}$$

15.1.4 Array membership. The predicate $Ina(x,n,a)$ holds if there is a number $i < n$ such that x is the value of the array a at the index i, ie

$$Ina(x,n,a) \leftrightarrow \exists i (i < n \wedge a[i] = x) \ .$$

The predicate has the following properties:

$$Ina(x,n,a) \leftrightarrow \exists i \, Pos(x,i,n,a) \tag{1}$$
$$\neg Ina(x,0,a) \tag{2}$$
$$Ina(x,n+1,a) \leftrightarrow a[n] = x \vee Ina(x,n,a) \ . \tag{3}$$

15.1.5 Exercise. Define a function $Search(x,n,a)$ satisfying

$$Search(x,n,a) = 0,i \to Pos(x,i,n,a) \tag{1}$$
$$Ina(x,n,a) \to \exists i \, Search(x,n,a) = 0,i \ . \tag{2}$$

Prove that the function has the required properties.

Hint. Define $Search(x,n,a)$ by primitive recursion on n as follows

$$\begin{aligned} &Search(x,0,a) = 0 \\ &Search(x,n+1,a) = 0,n \leftarrow a[n] = x \\ &Search(x,n+1,a) = Search(x,n,a) \leftarrow a[n] \ne x \end{aligned}$$

and prove the properties by the corresponding induction principle.

15.1.6 Position *(2nd form)***.** The predicate $Pos_2(x,i,m,n,a)$ holds if $m \le i < n$ and x is the value of the array a at the index i, ie

$$Pos_2(x,i,m,n,a) \leftrightarrow m \le i < n \wedge a[i] = x \ .$$

The predicate has the following properties:

$$Pos(x,i,n,a) \leftrightarrow Pos_2(x,i,0,n,a) \tag{1}$$
$$m \le i < n \wedge a[i] = x \rightarrow Pos_2(x,i,m,n,a) \tag{2}$$
$$m \ge n \rightarrow \neg Pos_2(x,i,m,n,a) \tag{3}$$
$$Pos_2(x,i,m,n,a) \wedge k \le m \rightarrow Pos_2(x,i,k,n,a) \tag{4}$$
$$Pos_2(x,i,m,n,a) \wedge n \le k \rightarrow Pos_2(x,i,m,k,a)\ . \tag{5}$$

15.1.7 Ordered arrays. The predicate $Orda(n,a)$ holds if the first n elements of the array a are ordered in the increasing order, ie

$$Orda(n,a) \leftrightarrow \forall i \forall j (i < n \wedge j < n \wedge i < j \rightarrow a[i] < a[j])\ .$$

The predicate has the following properties:

$$Orda(0,a) \tag{1}$$
$$Orda(n,a) \wedge m \le n \rightarrow Orda(m,a)\ . \tag{2}$$

15.1.8 Exercise *(binary search)*. Define a function $Bsearch(x,n,a)$ with the complexity $O(\log(n))$ satisfying

$$Orda(n,a) \rightarrow Bsearch(x,n,a) = 0,i \leftrightarrow Pos(x,i,n,a)\ . \tag{1}$$

Prove that the function has the required property.

Solution. We define $Bsearch(x,n,a)$ as follows

$$\begin{aligned}
&Bsearch_1(x,m,n,a) = 0 \leftarrow m \ge n\\
&Bsearch_1(x,m,n,a) = Bsearch_1(x,k+1,n,a) \leftarrow\\
&\quad m < n \wedge (m+n) \div 2 = k \wedge a[k] < x\\
&Bsearch_1(x,m,n,a) = 0,k \leftarrow\\
&\quad m < n \wedge (m+n) \div 2 = k \wedge a[k] = x\\
&Bsearch_1(x,m,n,a) = Bsearch_1(x,m,k,a) \leftarrow\\
&\quad m < n \wedge (m+n) \div 2 = k \wedge a[k] > x\\
&Bsearch(x,n,a) = Bsearch_1(x,0,n,a)\quad ,
\end{aligned}$$

where the auxiliary function $Bsearch_1(x,m,n,a)$ is defined by recursion with measure $n \dot{-} m$. The function $Bsearch_1(x,m,n,a)$ satisfies:

$$Bsearch_1(x,m,n,a) = 0,i \rightarrow Pos_2(x,i,m,n,a) \tag{2}$$
$$Orda(n,a) \wedge Pos_2(x,i,m,n,a) \rightarrow Bsearch_1(x,m,n,a) = 0,i\ . \tag{3}$$

Note that the property (1) follows from (2) and (3) by 15.1.6(1).

We prove (2) by course of values induction on m and n w.r.t. measure $n \dot{-} m$. Take any m and n such that

$$Bsearch_1(x,m,n,a) = 0,i \tag{4}$$

holds and assume

$$\forall m_1 \forall n_1 (n_1 \dot{-} m_1 < n \dot{-} m \rightarrow$$
$$Bsearch_1(x, m_1, n_1, a) = 0, i \rightarrow Pos_2(x, i, m_1, n_1, a))$$

as inductive hypothesis. We wish to prove

$$Pos_2(x, i, m, n, a) \ . \tag{5}$$

We consider two cases. If $m \geq n$ then the assumption (4) leads to contradiction since by definition $Bsearch_1(x, m, n, a) = 0$. So suppose $m < n$. Let $k := (m + n) \div 2$. Note that we have $m \leq k < n$. We proceed by trichotomy case analysis on $a[k]$ and x. If $a[k] < x$ then we have

$$Bsearch_1(x, k+1, n, a) \stackrel{\text{def}}{=} Bsearch_1(x, m, n, a) \stackrel{(4)}{=} 0, i \ .$$

We apply IH to $k + 1$ and n whereby we obtain that $Pos_2(x, i, k+1, n, a)$ holds. We get (5) by (4). If $a[k] = x$ then $k = i$ by definition and we get (5) by (2). If $a[k] < x$ then we have

$$Bsearch_1(x, m, k, a) \stackrel{\text{def}}{=} Bsearch_1(x, m, n, a) \stackrel{(4)}{=} 0, i \ .$$

We apply IH to m and k whereby we obtain that $Pos_2(x, i, m, k, a)$ holds. We get (5) by (5).

The proof of (3) is based on the following property of ordered arrays:

$$\begin{aligned} & Orda(n, a) \wedge Pos_2(x, i, m, n, a) \wedge k < n \rightarrow \\ & \qquad (a[k] < x \rightarrow Pos_2(x, i, k+1, n, a)) \wedge \\ & \qquad (a[k] = x \rightarrow k = i) \wedge \\ & \qquad (a[k] > x \rightarrow Pos_2(x, i, m, k, a)) \ . \end{aligned} \tag{6}$$

We prove (3) by course of values induction on m and n w.r.t. measure $n \dot{-} m$. Take any m and n such that

$$Orda(n, a) \wedge Pos_2(x, m, n, a) \tag{7}$$

holds and assume

$$\forall m_1 \forall n_1 (n_1 \dot{-} m_1 < n \dot{-} m \rightarrow$$
$$Orda(n_1, a) \wedge Pos_2(x, i, m_1, n_1, a) \rightarrow Bsearch_1(x, m_1, n_1, a) = 0, i)$$

as inductive hypothesis. We consider two cases. If $m \geq n$ then the assumption (7) leads to contradiction by 15.1.6(3). So suppose $m < n$. Let $k := (m+n) \div 2$. Note that we have $m \leq k < n$. We proceed by trichotomy case analysis on $a[k]$ and x. If $a[k] < x$ then we have

$$Bsearch_1(x, m, n, a) \stackrel{\text{def}}{=} Bsearch_1(x, k+1, n, a) \stackrel{\text{IH}(k+1, n), (6)}{=} 0, i \ .$$

If $a[k] = x$ then we have

$$Bsearch_1(x, m, n, a) \stackrel{\text{def}}{=} 0, k \stackrel{(6)}{=} 0, i \ .$$

If $a[k] > x$ then $Orda(k, a)$ by 15.1.7(2) and we have

$$Bsearch_1(x, m, n, a) \stackrel{\text{def}}{=} Bsearch_1(x, m, k, a) \stackrel{\text{IH}(m,k),(6)}{=} 0, i \ .$$

16. Programs Operating on Word Domains

17. Computation of Clausal Programs

Until now we were interested only in the definability of functions and predicates over natural numbers. We will now investigate questions of their effective computability.

17.1 Computation over Monadic Numerals

17.1.1 Monadic numerals. We recall the notation

$$\underline{n}_m \equiv 0\overbrace{{}'\ldots{}'}^{n}$$

introduced in Par. 8.4.3 for monadic numerals. Monadic numerals are the least class of terms containing the constant 0 and with every term ρ containing also the term ρ'.

17.1.2 Generalized terms for monadic numerals. The basic generalized term for the definition of clausal programs operating over monadic numerals is

$$Mon_x(\tau, \alpha_1[x], \alpha_2) = z \leftrightarrow \exists x(\tau = x' \land \alpha_1[x] = z) \lor \tau = 0 \land \alpha_2 = z \ .$$

17.1.3 Monadic clausal definitions. *Monadic* functions and predicates are defined by monadic clausal definitions. We have two classes of functions, primitive recursive and μ-recursive.

All primitive recursive functions are provably recursive in PA but not all μ-recursive functions are such.

17.1.4 Reductions over monadic numerals.

$$Mon_x(0, \alpha_1[x], \alpha_2) \blacktriangleright \alpha_2$$
$$Mon_x(\rho', \alpha_1[x], \alpha_2) \blacktriangleright \alpha_1[\rho] \ .$$

17.1.5 Computability of functions defined by monadic clausal definitions. Both primitive recursive and μ-recursive functions can be effectively computed by reductions.

17.2 Computation over Binary Numerals

If we were interested only in the effective computability of functions and predicates then we would not need more than monadic functions and predicates. Since we are discussing computer programming, we are also interested in the efficiency of computed programs. Monadic computation is exponentially slower than it should be. Computationally optimal is the so-called recursion on notation of which binary notation is the most well-known.

17.2.1 Binary numerals. *Binary numerals* are the least set of terms containing the constant 0, with every term ρ also the term $\rho\mathbf{1}$, and with every term $\rho \not\equiv 0$ also the term $\rho\mathbf{0}$. Thus the term $0\mathbf{0}$ is not a binary numeral.

17.2.2 Generalized terms for binary numerals. The basic generalized terms for clausal programs operating over binary numerals are

$$Bin([\tau = x\mathbf{0}; \alpha_1]_x, [\tau = x\mathbf{1}; \alpha_2]_x)$$
$$\mathcal{D}([\tau > 0; \alpha_1], [\tau = 0; \alpha_2]) \ .$$

17.2.3 Binary clausal definitions. *Binary* functions and predicates are defined by binary clausal definitions.

17.2.4 Fast binary arithmetic. Basic operations and comparisons.

17.2.5 Binary pairing function. $P_b(x, y)$

17.2.6 Binary projections. $H_b(x)$, $T_b(x)$

17.2.7 Characterization of binary functions and predicates. Binary functions and predicates are exactly the monadic ones.

17.2.8 Reductions over binary numerals.

$$\begin{aligned}
Bin([0 = x\mathbf{0}; \alpha_1]_x, [0 = x\mathbf{1}; \alpha_2]_x) &\blacktriangleright \alpha_1{}_x[0]\\
Bin([\rho\mathbf{0} = x\mathbf{0}; \alpha_1]_x, [\rho\mathbf{0} = x\mathbf{1}; \alpha_2]_x) &\blacktriangleright \alpha_1{}_x[\rho]\\
Bin([\rho\mathbf{1} = x\mathbf{0}; \alpha_1]_x, [\rho\mathbf{1} = x\mathbf{1}; \alpha_2]_x) &\blacktriangleright \alpha_2{}_x[\rho]\\
\mathcal{D}([0 > 0; \alpha_1], [0 = 0; \alpha_2]) &\blacktriangleright \alpha_2\\
\mathcal{D}([\rho\mathbf{0} > 0; \alpha_1], [\rho\mathbf{0} = 0; \alpha_2]) &\blacktriangleright \alpha_1\\
\mathcal{D}([\rho\mathbf{1} > 0; \alpha_1], [\rho\mathbf{1} = 0; \alpha_2]) &\blacktriangleright \alpha_1 \ .
\end{aligned}$$

17.2.9 Computability of binary functions and predicates. Binary functions and predicates are effectively computable by reductions.

17.2.10 Memory models for binary numerals. Computation is a syntactic process which proceeds by the manipulation of concrete objects. In the above discussion the concrete objects were monadic and binary numerals. In any practical implementation of computations over binary numerals on an electronic computer the d numerals will have to be mapped into the memory structures of the computer.

UNFINISHED Bignums

17.3 Computation over Pair Numerals

Although exponentially more efficient than monadic computation, the binary computation greatly suffers when computing with symbolic (coded) data.

17.3.1 Pair numerals. We recall the definition in Par. 1.3.8 of pair numerals as the least class of terms containing 0 and with every two terms ρ_1 and ρ_2 also the term (ρ_1, ρ_2).

17.3.2 Generalized term for pair numerals. The basic generalized term for clausal programs operating over pair numerals is

$$Pair([\tau = v, w; \alpha_1]_{v,w}, [\tau = 0; \alpha_2]) \ .$$

17.3.3 Pair clausal definitions. *Pair* functions and predicates are defined by pair clausal definitions.

17.3.4 Pair arithmetic. Basic operations and comparisons.

17.3.5 Characterization of pair functions and predicates. Pair functions and predicates are exactly the monadic ones.

17.3.6 Reductions over pair numerals.

$$Pair([0 = v, w; \alpha_1]_{v,w}, [0 = 0; \alpha_2]) \blacktriangleright \alpha_2$$
$$Pair([(\rho_1, \rho_2) = v, w; \alpha_1]_{v,w}, [(\rho_1, \rho_2) = 0; \alpha_2]) \blacktriangleright {\alpha_1}_v[\rho_1]_w[\rho_2] \ .$$

17.3.7 Computability of pair functions. Pair functions and predicates are effectively computable by reductions.

17.3.8 Memory models for pair numerals. The memory model of LISP is natural for the representation of pair numerals. The pair numeral 0 is represented in computer's memory with, say 32-bit words, by the word 0. The pair numeral (ρ_1, ρ_2) is represented by a non-zero word interpreted as a pointer to a *LISP-cell*, i.e. to two adjacent 32-bit words. The first word represents the first projection ρ_1 and the second word the second projection ρ_2. **UNFINISHED**

17.4 Computation over Mixed Numerals

We can combine the fast computation of numeric functions and predicates defined as binary functions with the gast computation of symbolic functions and predicates defined in pair notations by computing over mixed numerals.

17.4.1 Mixed numerals. *Mixed numerals* are the least set of terms containing the constant 0, with every terms ρ_1, ρ_2 also the terms $\rho_1\mathbf{1}$ and (ρ_1, ρ_2), and with every term $\rho \not\equiv 0$ also the term $\rho\mathbf{0}$. Binary and pair numerals are thus proper subsets of mixed numerals.

In contrast to monadic, binary, and pair numerals, the mixed numerals do not enjoy the unique representation of natural numbers. For instance, the number three is denoted by four mixed numerals which are all different as terms:

$$0\mathbf{11} \quad (0,0)\mathbf{1} \quad (0\mathbf{1},0) \quad ((0,0),0) \ .$$

17.4.2 Mixed clausal definitions. *Mixed* functions and predicates are defined by mixed clausal definitions which are constructed from the *Bin*, *Pair*, and $\mathcal{D}$ generalized terms.

Mixed clausal definitions clearly define all primitive recursive and μ-recursive functions.

17.4.3 Reductions over mixed numerals. Since binary and pair numerals are a subset of mixed ones, the reductions given in Paragrahps 17.2.8 and 17.3.6 apply also to mixed numerals. A pair (ρ_1, ρ_2) as an argument of a $\mathcal{D}$ generalized term has a natural reduction:

$$\mathcal{D}([(\rho_1,\rho_2) > 0; \alpha_1], [(\rho_1,\rho_2) = 0; \alpha_2]) \blacktriangleright \alpha_1 \ .$$

Reductions without conversion between representations are impossible in the following three cases:

$$\begin{aligned} &\mathit{Bin}([(\rho_1,\rho_2) = x\mathbf{0}; \alpha_1]_x, [(\rho_1,\rho_2) = x\mathbf{1}; \alpha_2]_x) \blacktriangleright \\ &\qquad\qquad \mathit{Bin}([\boldsymbol{M_2B}(\rho_1,\rho_2) = x\mathbf{0}; \alpha_1]_x, [\boldsymbol{M_2B}(\rho_1,\rho_2) = x\mathbf{1}; \alpha_2]_x) \\ &\quad \mathit{Pair}([\rho\mathbf{0} = v,w; \alpha_1]_{v,w}, [\rho\mathbf{0} = 0; \alpha_2]) \blacktriangleright {\alpha_1}_v[\boldsymbol{H}(\rho\mathbf{0})]_w[\boldsymbol{T}(\rho\mathbf{0})] \\ &\quad \mathit{Pair}([\rho\mathbf{1} = v,w; \alpha_1]_{v,w}, [\rho\mathbf{1} = 0; \alpha_2]) \blacktriangleright {\alpha_1}_v[\boldsymbol{H}(\rho\mathbf{1})]_w[\boldsymbol{T}(\rho\mathbf{1})] \end{aligned}$$

where we have denoted by $\boldsymbol{M_2B}$, $\boldsymbol{H}$, and $\boldsymbol{T}$ three conversion functions which are defined in the following paragraph to operate over mixed numerals.

17.4.4 Conversion of mixed to binary numerals. The conversion function $\boldsymbol{M_2B}$ takes a mixed numeral into a binary numeral with the same denotation. The function is defined by recursion on the structure of mixed numerals to satisfy:

$$\begin{aligned}
&\boldsymbol{M_2B}(0) \equiv 0\\
&\boldsymbol{M_2B}(\rho\mathbf{0}) \equiv \boldsymbol{M_2B}(\rho)\mathbf{0}\\
&\boldsymbol{M_2B}(\rho\mathbf{1}) \equiv \boldsymbol{M_2B}(\rho)\mathbf{1}\\
&\boldsymbol{M_2B}(\rho_1,\rho_2) \equiv \rho \Leftarrow P_b(\boldsymbol{M_2B}(\rho_1), \boldsymbol{M_2B}(\rho_2)) \blacktriangleright \rho\ .
\end{aligned}$$

The function is clearly effectively computable.

The conversion function $\boldsymbol{H}(\rho)$ takes a mixed numeral and yields a mixed numeral with the same denotation as $H(\rho)$. The function $\boldsymbol{T}(\rho)$ is similar. The functions satisfy the following:

$$\begin{aligned}
&\boldsymbol{H}(0) \equiv 0\\
&\boldsymbol{H}(\rho_1,\rho_2) \equiv \rho_1\\
&\boldsymbol{H}(\rho\mathbf{0}) \equiv \rho_1 \Leftarrow H_b(\boldsymbol{M_2B}(\rho)\mathbf{0}) \blacktriangleright \rho_1\\
&\boldsymbol{H}(\rho\mathbf{1}) \equiv \rho_1 \Leftarrow H_b(\boldsymbol{M_2B}(\rho)\mathbf{1}) \blacktriangleright \rho_1\\
&\boldsymbol{T}(0) \equiv 0\\
&\boldsymbol{T}(\rho_1,\rho_2) \equiv \rho_2\\
&\boldsymbol{T}(\rho\mathbf{0}) \equiv \rho_1 \Leftarrow T_b(\boldsymbol{M_2B}(\rho)\mathbf{0}) \blacktriangleright \rho_1\\
&\boldsymbol{T}(\rho\mathbf{1}) \equiv \rho_1 \Leftarrow T_b(\boldsymbol{M_2B}(\rho)\mathbf{1}) \blacktriangleright \rho_1
\end{aligned}$$

and are clearly effectively computable.

17.4.5 Computability of clausal definitions. A clausally defined function f of T is *reducible* if for all mixed numerals $\vec{\rho}$ we have $f(\vec{\rho}) \blacktriangleright \tau$ for a mixed numeral τ and $T \vdash f(\vec{\rho}) = \tau$.

Let T be an extension of S with a (guarded) clausal definition of f. Assume that all clausally defined functions of S are reducible.

The mixed functions are computable over mixed numerals.

17.4.6 A memory model for mixed pumerals. A mixed numeral can be represented in a memory of an electronic computer with a 32-bit words, by a word whose lowest two bits serve as four tags distinguishing the four kinds of mixed numerals.

We assign the tag 0 to represent the numerals which are pairs of the form (ρ_1,ρ_2). A 32-bit number n with the tag 0 (note that $n \bmod 4 = 0$) is interpreted as a pointer to a LISP-cell as in Par. 17.3.8. A word n with the tag 1 represents the mixed numeral $\rho\mathbf{0}$ by interpreting the number $n-1$ as a pointer to a word representing the mixed numeral ρ. Similarly, a word n with the tag 2 represents the mixed numeral $\rho\mathbf{1}$ by interpreting the number $n-2$ as a pointer to a word representing the mixed numeral ρ. Finally, a word n with the tag 3 represents the fourth kind of mixed numerals. Normally this would be the single numeral 0. It is, however, advantageous to utilize the remaining 30-bits of such words to store small natural numbers directly. This means that the word represents the binary numeral denoting $n \div 4$.

This representation of mixed numerals can be described purely in the language of logic by defining the class of *extended mixed numerals* as the smallest class of terms which contains decimal numerals denoting the numbers n such that

$$n \leq 1,073,741,823 = 2^{30} - 1 = 0\mathbf{1}^{30}$$

holds and such that with each two extended mixed numerals ρ_1 and ρ_2 also the terms $\rho_1\mathbf{0}$ (provided $\rho_1 \not\equiv 0$), $\rho_2\mathbf{1}$, and (ρ_1, ρ_2) are extended mixed numerals. Figure 17.1 shows the memory representation of the extended mixed numeral $(5, 1073741823\mathbf{1})\mathbf{01}$.

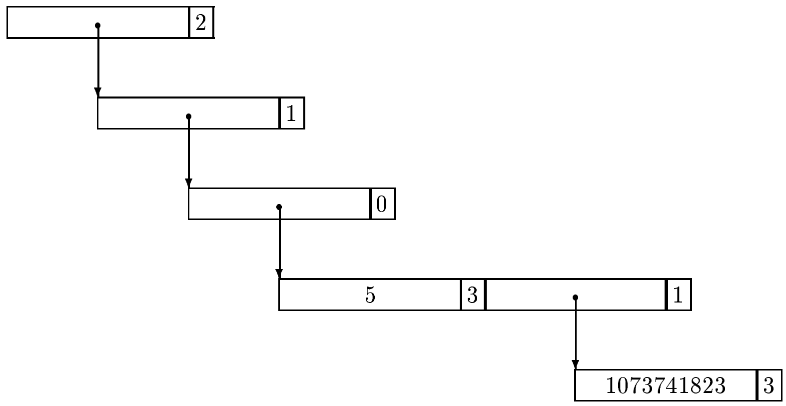


Fig. 17.1. Memory representation of the extended mixed numeral $(5, 1073741823\mathbf{1})\mathbf{21}$

18. Data Types

Typed programming languages, especially the functional ones, are popular for three reasons:

1. types naturally express properties of programs,
2. types permit good memory representation of data and the programs can be efficiently compiled,
3. types are indispensable for a natural semantics of higher-order functions (functionals).

The first reason for types is irrelevant for a programming language integrated with its own proof system (such as CL) because the formulas of the language permit a simpler formulation and proofs of much more complex properties than those expressible by typing. The remaining reasons for typing are exteremely important and we discuss the second reason in this chapter and the third one in Chapter 19.

However, there is a negative side to typing in a complication of syntax and semantics. The usual approach to types is via many-sorted languages and theories. The simple languages and semantics of LISP, PROLOG, and CL are lost. We now propose a type system which enables us both to have and eat the proverbial cake.

18.1 Pascal-Style Typing

Pascal was the first computer programming language whose data types supported good representation in memory.

18.1.1 Type predicates. Pascal-style types will be defined in **UNFINISHED** as codes of certain unary *type* predicates. By convention we write $x : T$ instead of $T(x)$ and read it as the code of T is the type of x Not every unary predicate is a type predicate. We will introduce in the following paragraphs several kinds of syntactic restrictions on the clauses of type predicates $x : T$ which will guarantee that the value x can be efficiently represented in computer memory.

Extension of a type predicate T is the set numbers x such that $x : T$ holds in the standard model of PA. *Intension* of T is the set of mixed numerals which are *canonical* terms of type T. This will be precisely defined in **UNFINISHED**

UNFINISHED Canonical terms of type T can be efficiently represented in computer memory. In the following we will see that although extensions of two type predicates T_1 and T_2 may overlap in that there is a mixed numeral ρ such that $\rho : T_1$ and $\rho : T_2$, the intesions are different in that ρ has two different memory representations.

UNFINISHED typing of generalized terms and of clausal definitions. Additionally, a well-typed function or predicate can be reduced over mixed numerals without the three reductions given in Par. 17.4.3 and which involve conversion of representation.

18.1.2 Basic type predicates. Predicates N and Ch with explicit definitions

$x : N$
$x : Ch \leftarrow x < 256$

are the basic type predicates. The code of $\mathbb{N}$ is the *type of natural numbers* and the code of Ch is the *type of characters*.

In programming practice there will be additional basic types inluding integers and floats.

18.1.3 Cartesian type predicates. Suppose that $T_1, \ldots T_n$ are type predicates. The unary type predicate explicitly defined by

$(x_1, \ldots, x_n) : T \leftarrow x : T_1 \wedge \ldots \wedge x : T_n$

is the type predicate of *cartesian product* of codes of $T_1, \ldots, T_n$.

UNFINISHED The extension of T are exactly numbers $x_1, \ldots, x_n$ for some $x_1, \ldots, x_n$. those mixed numerals which can be written as n-tuples $\rho_1, \ldots, \rho_n$.

Memory representation: **UNFINISHED**

18.1.4 List type predicates. Suppose that S is a type predicate. The predicate

$0 : T$
$x,y : T \leftarrow x : S \wedge y : T$.

is the type predicate of *lists of codes of* S.

18.1.5 Fixed vector type predicates. Suppose that S is a type predicate and c a constant. The predicate

$0 : T$
$x,y : T \leftarrow x : S \wedge y : T$.

is the type predicate of *lists of codes of S*.

UNFINISHED typing of definitions

18.2 ML-Style Typing

ML-style *polymorphic* typing is a higher-order calculus where variables and arguments of predicates can range over types.

18.2.1 Type predicates with types as arguments. List types are best viewed as higher-order predicates with types as arguments Instead of viewing type predicates as unary we may permit additional argument. Consider as an example the binary type predicate of lists *List*:

$0 : List(t)$
$x, y : List(t) \leftarrow x \mathbin{\boldsymbol{:}} t \land y : List(t)$.

We can view the binary predicate $x \mathbin{\boldsymbol{:}} t$ as a *universal typing* predicate where the second argument t ranges over type predicates T in such a way that

$$x : T \leftrightarrow x \mathbin{\boldsymbol{:}} T$$

holds.

For concrete type predicates t we can then consider $x : List(t)$ to be a unary predicate in x. For instance, $x : List(N)$ and $x : List(Ch)$ can be viewed as type predicates which would have to be introduced in Pascal-style typing by two definitions:

$0 : ListN$
$x, y : ListN \leftarrow x : ListN \land y : ListN$
$0 : ListCh$
$x, y : ListCh \leftarrow x : ListCh \land y : ListCh$.

18.2.2 Example of polymorphic typing. UNFINISHED

18.2.3 Vectors. Higher-order type predicates such as $x : List(t)$ do need to have their arguments restricted to types. Consider for instance, the ternary predicate $x : V_1(n, t)$ of *fixed vectors* which for any number n and type t behaves as the Pascal-like type *array* $[0..n-1]$ *of* t.

$0 : V_1(0, t)$
$x, y : V_1(n+1, t) \leftarrow x \mathbin{\boldsymbol{:}} t \land y : V_1(n, t)$.

UNFINISHED discussion that they are lists but can be mapped into memory in a better way.

We can now introduce a binary typing predicate $x : V_2(t)$ of *flexible vectors* with the definition

$$n, x : V_2(t) \leftarrow x : V_1(n, t)\ .$$

UNFINISHED discussion and memory representation

UNFINISHED Without ontological commitment to types which would get us outside of first-order theories we can treat types as codes of type predicates. Universal functions in recursion theory. Assignment of indices, choices are endless but we will for illustration purposes stick to one type system with good mapping onto memory.

Higher-order typing even without functionals. We can deal with the problem by intensionality. The value of extensionality is diminished when types are used for intensional reasons such as computation.

19. Functional Programming

20. Modular Programming

1. J. Barwise. em An Introduction to First-Order Logic. In Handbook of Mathematical Logic, J. Barwise ed., North-Holland Publishing Co, 1977.
2. **UNFINISHED** Beth, tableaux
3. G. Boolos and R. Jeffrey, *Computability and Logic*, Cambridge University Press, Cambridge, 1974.
4. M. Davis, *Computability and Unsolvability*, McGraw Hill, New York, 1958.
5. **UNFINISHED** Dreben Andrews Aandreaa False lemmas
6. S. Feferman. *Theory of Finite Type Related to Mathematical Practice*, In Handbook of Mathematical Logic, J. Barwise ed., North-Holland Publishing Co, 1977.
7. **UNFINISHED** Fitting tableaux
8. **UNFINISHED** Gentzen
9. K. Gödel, Üeber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Monatshefte Math. Phys. vol. 38 (1931) pages 173-198.
10. M. J. Gordon, R. Milner, C. P. Wadsworth, *Edinburgh LCF*. Lecture Notes in Computer Science, vol 78. Springer, Berlin 1979.
11. P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic*. Springer Verlag, 1993.
12. J. Herbrand Recherches
13. **UNFINISHED** Hilbert Ackermann logic
14. R. Milner, *A Theory of Type Polymorphism in Programming*. J. Comput. System Sci. 17 (1978) 348-375.
15. J. C. Mitchell. *Type Systems for Programming Languages*. In Handbook of Theoretical Compute Science (vol B), J. van Leeuwen ed., Elsevier 1990.
16. Ch. Okasaki, *Breadth-First Numbering: Lessons from a Small Exercise in Algorithm Design* **UNFINISHED**
17. R. Péter. *Konstruktion nichtrekursiver Funktionen*. Math. Ann. vol 111 (1935), pages 42-60.
18. H. E. Rose. *Subrecursion: Functions and Hierarchies*. Number 9 in Oxford Logic Guides. Clarendon Press, Oxford, 1982.
19. H. Schwichtenberg, *Eine Klassifikation der ϵ_0-rekursiven Funktionen*, Zeitschrift für mathematische Logik und Grundlagen der Mathematik, vol. 17, (1971), pp. 91-74.
20. J. R. Shoenfield. *Mathematical Logic*, Addison-Wesley, 1967.
21. **UNFINISHED** Smullyan First-order logic
22. **UNFINISHED** Takeuti, Proof theory
23. A. S. Troelstra. *Aspects of Constructive Mathematics*. In Handbook of Mathematical Logic, J. Barwise ed., North-Holland Publishing Co, 1977.
24. P. J. Voda. *Subrecursion as a basis for a feasible programming language*, in L. Pacholski and J. Tiuryn, editors, Proceedings of CSL'94, number 933 in LNCS Springer Verlag, 1995, pages 324-338.

25. S. S. Wainer. *A classification of the ordinal recursive functions*, Archiv für mathematische Logik und Grundlagen Forschung, vol. 13, 1970, pp. 136-153.