Peano Arithmetic and Clausal Language

Paul J. Voda

November 2004

Table of Contents

1 Basic Bootstrapping of PA

In this section we introduce and prove basic theorems of the formal system of arithmetic called Peano arithmetic.

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.

1.2 Axioms of Peano arithmetic. The axioms of Peano arithmetic consist of universal closures of the following six formulas:

$$\vdash_{\mathrm{PA}} 0 \neq x' \tag{1}$$
$$\vdash_{\mathrm{PA}} x' = y' \rightarrow x = y \tag{2}$$
$$\vdash_{\mathrm{PA}} 0 + y = y \tag{3}$$
$$\vdash_{\mathrm{PA}} x' + y = (x + y)' \tag{4}$$
$$\vdash_{\mathrm{PA}} 0{\cdot}y = y \tag{5}$$
$$\vdash_{\mathrm{PA}} x'{\cdot}y = x{\cdot}y + y \tag{6}$$

and for every formula $\phi[x]$ of $\mathcal{L}_{\mathrm{PA}}$ and an indicated variable x a universal closure of the axiom of (mathematical) *induction* $I_x\phi[x]$:

$$\vdash_{\mathrm{PA}} \phi[0] \land \forall x(\phi[x] \rightarrow \phi[x']) \rightarrow \phi[x] \ . \tag{7}$$

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 $\models_{\mathrm{PA}} \phi$ of *provability in* PA as an abbreviation for PA $\vdash \phi$.

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 1.2(1) through 1.2(6).

We now prove that also the induction axioms 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 $\mathcal{N} \models \forall x \forall \vec{y} I_x \phi[x, \vec{y}]$. For that we take any $\vec{d} \equiv d_1, \ldots, d_n \in \mathbb{N}$ and it clearly suffices to show $\mathcal{N} \models \forall x \phi[x, \vec{d}]$. So assume on the contrary that $\mathcal{N} \not\models \phi[m, \vec{d}]$ for some $m \in \mathbb{N}$. Furthermore, assume that m is the least such number. We thus have the base case assumption $\mathcal{N} \models \phi[0, \vec{d}]$, the inductive assumption: $\mathcal{N} \models \forall x(\phi[x, \vec{d}] \to \phi[x, \vec{d}])$, and $\mathcal{N} \not\models \phi[m, \vec{d}]$. Consider now two cases. If $m = 0$ then we get a contradiction with the base case assumption. If $m > 0$ then we have $\mathcal{N} \models \phi[m - 1, \vec{d}]$ by the minimality of m and we get a contradiction $\mathcal{N} \models \phi[(m - 1) + 1, \vec{d}]$ from the inductive assumption.

1.4 Informal reasoning by induction. The typical situation of use of axioms of mathematical induction $I_x \phi[x]$ is that we use it 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 goal 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 $\phi[x']$ 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.

1.5 Induction rules in CL. CL has many built in rules of induction all of which are justified by a reduction to the axioms of mathematical induction 1.2(7). The use of induction rules in CL is restricted to the beginning of proofs where after some initial flattennings we have a goal $\phi[x, y_1, \ldots, y_n]*$ under assumptions (also called *side formulas*) $\psi_1, \ldots, \psi_k$ neither of which has the induction variable x nor the optional *distinguished* variables $y_1, \ldots, y_n$ free. Both the induction formula and side formulas may contain additional parameters $\vec{z}$ free.

In order to prove the formula $\forall y_1 \ldots \forall y_n \phi[x, y_1, \ldots, y_n]$ by an induction rule called R we use a CL-command $\mathsf{ind}\ R; x; y_1; \ldots; y_n$. The reader will note that the distinguished variables are universally quantified in the induction formula (the parameters $\vec{z}$ (if any) are not). The number n is usually 0, i.e. $\mathsf{ind}\ R; x$, when the induction formula is $\phi[x, y_1, \ldots, y_n]$.

The axioms 1.2(7) of mathematical induction directly justify the induction rule of CL called N_1. The above command with $R = N_1$, i.e. the command ind $N_1; x; y_1; \ldots; y_n$, invokes the rule

$$\frac{}{\phi[0,\vec{y}]* \;\Big|\; \begin{array}{c}\forall\vec{y}\phi[x,\vec{y}]\\ \phi[x',\vec{y}]*\end{array}} \tag{1}$$

which is equivalent to the use of the axiom of mathematical induction

$$\vdash_{\text{PA}} \forall\vec{y}\phi[0,\vec{y}] \land \forall x(\forall\vec{y}\phi[x,\vec{y}] \to \forall\vec{y}\phi[x',\vec{y}]) \to \forall\vec{y}\phi[x,\vec{y}] \tag{2}$$

followed by two splits, eigen-variable rules on x and $\vec{y}$, and a flatten.

1.6 Case analysis on 0 and positive numbers. The base case analysis is on 0 and on positive numbers:

$$\vdash_{\text{PA}} x = 0 \lor \exists y\, x = y' \tag{1}$$

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 $x' = x'$.

1.7 Case analysis rules in CL. CL has many built in rules of *case analysis on* x which are justified by theorems in a form of disjunctions as 1.6(1) which specify possible forms of x. If we wish to use a rule of case analysis called R with the variable z we give a CL-command case $R; z$.

The theorem 1.6(1) justifies a case rule called N_1 where after saying case $N_1; z$ the following rule is applied:

$$\frac{}{z = 0 \mid z = y'}$$

with an eigen-variable y. The rule is equivalent to a use of the theorem 1.6(1) followed by a split and an eigen-variable rule on y.

1.8 Nullpoints of addition. We have the following property of addition:

$$\vdash_{\text{PA}} x + y = 0 \leftrightarrow x = 0 \land y = 0 \tag{1}$$

In the direction $(\to)$ assume $x+y=0$ and consider two cases by 1.6(1). If $x=0$ then we have $0 = 0+y \overset{1.2(3)}{=} 0$. The case $x = x_1'$ for some x_1 cannot hold because it leads to a contradiction: $0 = x_1' + y \overset{1.2(4)}{=} (x+y)'$ by 1.2(1). In the direction $(\leftarrow)$ the property is a direct consequence of 1.2(3).

1.9 Addition is commutative. In order to prove that $+$ commutes

$$\vdash_{\text{PA}} x + y = y + x \tag{1}$$

we need two lemmas

$$\vdash_{\text{PA}} \ x + 0 = x \tag{2}$$
$$\vdash_{\text{PA}} \ x + y' = x' + y. \tag{3}$$

(2) is proved by induction on x. In the base case we have $0 + 0 \overset{1.2(3)}{=} 0$ and in the inductive case:

$$x' + 0 \overset{1.2(4)}{=} (x + 0)' \overset{IH}{=} x' \ .$$

(3) is proved by induction on x. In the base case we have

$$0 + y' \overset{1.2(3)}{=} y' \overset{1.2(3)}{=} (0 + y)' \overset{1.2(4)}{=} 0' + y \ .$$

In the inductive case we have

$$x' + y' \overset{1.2(4)}{=} (x + y')' \overset{IH}{=} (x' + y)' \overset{1.2(4)}{=} x'' + y \ .$$

We now prove (1) by induction on x. In the base case we have

$$0 + y \overset{1.2(3)}{=} y \overset{(2)}{=} y + 0 \ .$$

In the inductive case we have

$$x' + y \overset{1.2(4)}{=} (x + y)' \overset{IH}{=} (y + x)' \overset{1.2(4)}{=} y' + x \overset{(3)}{=} y + x' \ .$$

From now on we will not explicitly indicate the uses of the two axioms of addition 1.2(3)(4).

1.10 Addition is associative. That the addition is associative

$$\vdash_{\text{PA}} (x + y) + z = x + (y + z) \tag{1}$$

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:

$$(x' + y) + z = (x + y)' + z = ((x + y) + z)' \overset{IH}{=} (x + (y + z))' = x' + (y + z) \ .$$

1.11 Cancellation rules for addition. *Cancellation* rules for the addition are:

$$\vdash_{\text{PA}} \ z + x = z + y \rightarrow x = y \tag{1}$$
$$\vdash_{\text{PA}} \ x + z = y + z \rightarrow x = y \ . \tag{2}$$

(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

$$z' + x = z' + y \Rightarrow (z+x)' = (z+y)' \overset{1.2(2)}{\Rightarrow} z + x = z + y \overset{IH}{\Rightarrow} x = y \ .$$

(2) is proved as follows:

$$x + z = y + z \overset{1.9(1)}{\Rightarrow} z + x = z + y \overset{(1)}{\Rightarrow} x = y \ .$$

From now on we will not explicitly indicate the properties of addition proved until now.

1.12 Successor versus addition. We have

$$\vdash_{\text{PA}} \ x + 1 = x' \tag{1}$$

because

$$x + 1 = x + 0' \overset{1.9(3)}{=} x' + 0 \overset{1.9(2)}{=} x' \ .$$

This means that PA proves $\vdash_{\text{PA}} \ 0 \vee \exists y \, x = y + 1$ from 1.6(1). This justifies the case rule of CL called N such that the command `case` $N; z$ applies the rule:

$$\frac{}{z = 0 \mid z = y + 1}$$

with an eigen-variable y.

Similarly, CL has an induction rule called N which for a command `ind` $N; x; y_1; \dots y_n$ issued in the situation described in Par. 1.5 applies the rule:

$$\frac{}{\phi[0, \vec{y}]* \;\Bigg|\; \begin{array}{c} \forall \vec{y} \phi[x, \vec{y}] \\ \phi[x+1, \vec{y}]* \end{array}} \tag{2}$$

The rule is justified by

$$\vdash_{\text{PA}} \ \forall \vec{y} \phi[0, \vec{y}] \wedge \forall x (\forall \vec{y} \phi[x, \vec{y}] \to \forall \vec{y} \phi[x+1, \vec{y}]) \to \forall \vec{y} \phi[x, \vec{y}] \tag{3}$$

which is straightforwardly proved from (1) and 1.5(2).

1.13 Multiplication by 0 and 1. We have

$$\vdash_{\text{PA}} \ x \cdot 0 = 0 \tag{1}$$

$$\vdash_{\text{PA}} \ x \cdot 1 = 1 \ . \tag{2}$$

(1) is proved by induction on x. In the base case we have $0 \cdot 0 \overset{1.2(5)}{=} 0$. In the inductive case we have:

$$x' \cdot 0 \overset{1.2(6)}{=} x \cdot 0 + 0 = x \cdot 0 \overset{IH}{=} 0 \ .$$

(2) is proved by induction on x. In the base case we have $0 \cdot 1 \overset{1.2(5)}{=} 0$. In the inductive case we have

$$x' \cdot 1 \overset{1.2(6)}{=} x \cdot 1 + 1 = 1 + x \cdot 1 \overset{IH}{=} 1 + x = x + 1 = x' \ .$$

1.14 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 ($\rightarrow$) we assume $x \cdot y = 1$ and consider three cases for x. The case $x = 0$ leads to the contradiction $0' = 1 = 0 \cdot y \overset{1.2(5)}{=} 0$. If $x = 1$ then we have

$$1 = 1 \cdot y = 0' \cdot y \overset{1.2(6)}{=} 0 \cdot y + y \overset{1.2(5)}{=} 0 + y = y \; .$$

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

$$0' = 1 = x_1'' \cdot 0 \overset{1.13(1)}{=} 0 \; .$$

Also the second case $y = y_1'$ for some y_1 leads to a contradiction:

$$0' = 1 = x_1'' \cdot y_1' \overset{1.2(6)}{=} x_1' \cdot y_1' + y_1' \overset{1.2(6)}{=} x_1 \cdot y_1' + y_1' + y_1' = (x_1 \cdot y_1' + y_1 + y_1)'' \; .$$

The direction ($\leftarrow$) follows from the following

$$1 \cdot 1 = 0' \cdot 1 \overset{1.2(6)}{=} 0 \cdot 1 + 1 \overset{1.2(5)}{=} 0 + 1 = 1 \; .$$

1.15 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

$$0 \cdot (x + y) \overset{1.2(5)}{=} 0 = 0 + 0 \overset{1.2(5)}{=} 0 \cdot x + 0 \cdot y \; .$$

In the inductive case we have

$$z' \cdot (x + y) \overset{1.2(6)}{=} z \cdot (x + y) + (x + y) \overset{IH}{=} (z \cdot x + z \cdot y) + (x + y) =$$
$$z \cdot x + (z \cdot y + (x + y)) = z \cdot x + (z \cdot y + (y + x)) = z \cdot x + ((z \cdot y + y) + x) \overset{1.2(6)}{=}$$
$$z \cdot x + (z' \cdot y + x) = z \cdot x + (x + z' \cdot y) = (z \cdot x + x) + z' \cdot y \overset{1.2(6)}{=} z' \cdot x + z' \cdot y \; .$$

From now on we will not explicitly indicate the uses of the two axioms of multiplication 1.2(5)(6).

1.16 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

$$0 \cdot y = 0 \overset{1.13(1)}{=} y \cdot 0 \; .$$

In the inductive case we have

$$x' \cdot y = x \cdot y + y \overset{1.13(2)}{=} x \cdot y + y \cdot 1 \overset{IH}{=} y \cdot x + y \cdot 1 \overset{1.15(1)}{=} y \cdot (x + 1) = y \cdot x' \; .$$

1.17 Multiplication is associative. The proof that the multiplication is associative:

$$\vdash_{\text{PA}} (x{\cdot}y){\cdot}z = x{\cdot}(y{\cdot}z) \tag{1}$$

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

$$(x'{\cdot}y){\cdot}z = (x{\cdot}y + y){\cdot}z \overset{1.16(1)}{=} z{\cdot}(x{\cdot}y + y) \overset{1.15(1)}{=} z{\cdot}(x{\cdot}y) + z{\cdot}y \overset{1.16(1)}{=}$$
$$(x{\cdot}y){\cdot}z + y{\cdot}z \overset{IH}{=} x{\cdot}(y{\cdot}z) + y{\cdot}z = x'{\cdot}(y{\cdot}z)\ .$$

1.18 Cancellation rules for multiplication. *Cancellation* rules for the multiplication are:

$$\vdash_{\text{PA}} z \neq 0 \land z{\cdot}x = z{\cdot}y \to x = y \tag{1}$$
$$\vdash_{\text{PA}} z \neq 0 \land x{\cdot}z = y{\cdot}z \to x = y\ . \tag{2}$$

(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 $\forall y(x{\cdot}z_1' = y{\cdot}z_1' \to x = y)$. 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.

2 Extensions of PA by Predicate Symbols

We study in this section the effect of extensions by definitions of PA on the axioms of induction.

2.1 Extensions of PA by definitions and induction axioms. Extensions T of PA by definitions prove all induction axioms of T, i.e. $T \vdash I_x\phi[x]$ for all formulas ϕ of $\mathcal{L}_T$. This is because the new symbols in $\mathcal{L}_T$ can be translated away from ϕ to the formula $\phi^* \in \mathcal{L}_{\mathrm{PA}}$. We, namely, have $T \vdash I_x\phi[x] \leftrightarrow (I_x\phi[x])^\star$ and $\mathrm{PA} \vdash (I_x\phi[x])^\star$. Hence $T \vdash (I_x\phi[x])^\star$ because T extends PA and thus $T \vdash I_x\phi[x]$.

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.

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.

We will be using the symbol of provability $\vdash_{\overline{\mathrm{PA}}} \phi$ in the relativized sense as $T \vdash \phi$ where T is the current extension of PA. We will also use the symbol $\vdash_{\overline{\mathrm{PAx}}} \phi$ with the meaning of $\vdash_{\overline{\mathrm{PA}}} \phi$ when we will wish to emphasize that the formula ϕ is the defining axiom of the new extension of PA.

2.2 Comparison predicates. We introduce into PA the binary *comparison* predicates $<$, $\leq$, $>$, and $\geq$ by explicit definitions:

$$\vdash_{\overline{\mathrm{PAx}}} x < y \leftrightarrow \exists z\, x + z' = y \tag{1}$$
$$\vdash_{\overline{\mathrm{PAx}}} x \leq y \leftrightarrow x < y \lor x = y \tag{2}$$
$$\vdash_{\overline{\mathrm{PAx}}} x > y \leftrightarrow y < x \tag{3}$$
$$\vdash_{\overline{\mathrm{PAx}}} x \geq y \leftrightarrow y \leq x\ . \tag{4}$$

The relation $\leq$ has the following property:

$$\vdash_{\overline{\mathrm{PA}}} x \leq y \leftrightarrow \exists z\, x + z = y\ . \tag{5}$$

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.

2.3 The relation $<$ is a linear order. The relation $<$ (and also $>$) is a linear order because we have

$$\vdash_{\overline{\mathrm{PA}}} \neg x < x \tag{1}$$
$$\vdash_{\overline{\mathrm{PA}}} x < y \land y < z \rightarrow x < z \tag{2}$$
$$\vdash_{\overline{\mathrm{PA}}} x < y \lor x = y \lor y < x\ . \tag{3}$$

The properties are called in that order *irreflexivity*, *transitivity*, and *linearity*.

(1): 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.

(2): Assume $x < y$ 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 (3) we need an auxiliary property

$$\vdash_{\text{PA}} 0 < x' \tag{4}$$

which follows from $0+x' = x'$ by existential instantiation and the definition.

(3): By induction on x. In the base case we wish to prove $0 < y \vee 0 = y \vee y < 0$ 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 $x' < y \vee x' = y \vee y < x'$. 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 $x' \leq y$ by 2.2(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.

2.4 Ordering properties of relation $\leq$. The predicate $\leq$ constitutes a (total) *ordering relation* which is reflexive, transitive, *antisymmetric*, and linear. This is expressed in that order as follows:

$$\vdash_{\text{PA}} x \leq x \tag{1}$$
$$\vdash_{\text{PA}} x \leq y \wedge y \leq z \to x \leq z \tag{2}$$
$$\vdash_{\text{PA}} x \leq y \wedge y \leq x \to x = y \tag{3}$$
$$\vdash_{\text{PA}} x \leq y \vee y \leq x\;. \tag{4}$$

Property (1) follows directly from the definition. Property (2) follows from the transitivity of $<$.

(3): If $x \leq y$, $y \leq x$, and $x \neq y$ 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 2.3(3) of $<$.

2.5 Laws and rules of trichotomy and dichotomy. The laws of trichotomy and dichotomy are in that order the following formulas:

$$\vdash_{\text{PA}} x < y \vee x = y \vee x > y \tag{1}$$
$$\vdash_{\text{PA}} x \leq y \vee x > y\;. \tag{2}$$

The laws are typically used for case analysis and they are directly proved from the definitions of $<$, $>$, $\leq$, and from the linearity 2.3(3).

CL has built in case rules called *Trich* and *Dich* which are justified in that order by (1) and (1). The command `case` *Trich*$; x, y$ applies the rule:

$$\frac{}{x < y \mid x = y \mid x > y}$$

and the command `case` *Dich*$; x, y$ applies the rule:

$$\frac{}{x \leq y \mid x > y}$$

2.6 Additional properties of comparisons. We have the following additional properties of the comparison relations:

$$\vdash_{\text{PA}} x \not< 0 \tag{1}$$
$$\vdash_{\text{PA}} 0 \leq x \tag{2}$$
$$\vdash_{\text{PA}} x < x' \tag{3}$$
$$\vdash_{\text{PA}} x < y \leftrightarrow x' \leq y\ . \tag{4}$$

(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 1.8(1).

(2) is a direct consequence of (1) and 2.5(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 2.2(5).

2.7 Monotonicity of addition and multiplication. Addition and multiplication are monotone:

$$\vdash_{\text{PA}} x < y \leftrightarrow z + x < z + y \tag{1}$$
$$\vdash_{\text{PA}} x < y \leftrightarrow x + z < y + z \tag{2}$$
$$\vdash_{\text{PA}} z > 0 \rightarrow x < y \leftrightarrow z{\cdot}x < z{\cdot}y \tag{3}$$
$$\vdash_{\text{PA}} z > 0 \rightarrow x < y \leftrightarrow x{\cdot}z < y{\cdot}z\ . \tag{4}$$

(1): We have $x < y$ iff $x + u' = y$ for some u iff, by 1.11(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 2.3(1). Hence $y = y_1'$ for some y_1 and we have $0 < y$ by 2.3(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 2.6(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.

2.8 Induction with measure. Suppose that PA has been extended to contain the predicate $<$ and that $\mu[\vec{x}]$ and $\phi[\vec{x}]$ are respectively a term and a formula in the language of (the current extension of) PA. Then the following formula is called the *induction on the measure* $\mu[\vec{x}]$ *for* $\phi[\vec{x}]$:

$$\vdash_{\mathrm{PA}} \forall \vec{x}(\forall \vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \rightarrow \phi[\vec{y}]) \rightarrow \phi[\vec{x}]) \rightarrow \phi[\vec{x}] \tag{1}$$

The measure induction is proved by taking any $\vec{x}$, assuming its antecedent formula (which is said to assert the *progressiveness* of μ) and proving by induction on z the auxiliary formula:

$$\forall \vec{y}(\mu[\vec{y}] < z \rightarrow \phi[\vec{y}]) \tag{2}$$

In the base case when $z = 0$ there is nothing to prove. In the inductive case assume (2) as IH, take any $\vec{y}$ such that $\mu[\vec{y}] < z + 1$ and we wish to prove $\phi[\vec{y}]$. Towards that end we consider two cases. If $\mu[\vec{y}] < z$ then the goal follows from IH. If $\mu[\vec{y}] = z$ then we instantiate the assumption of the progressivess with $\vec{x} := \vec{y}$ and obtain $\phi[\vec{y}]$ from it since its antecedent is equivalent to (2). With (2) proved, we instantiate it with $\vec{y} := \vec{x}$ and $z := \mu[\vec{x}] + 1$ to obtain $\phi[\vec{x}]$.

Induction with measure (1) justifies in CL the command indm $\mu[\vec{x}]$ where the following rule is applied:

$$\frac{}{\begin{array}{c}\forall \vec{y}(\mu[\vec{y}] < \mu[\vec{x}] \rightarrow \phi[\vec{y}])\\ \phi[\vec{x}]*\end{array}}$$

for eigen-variables $\vec{x}$.

In the special case when $\mu[\vec{x}]$ is just the variable x, the induction formula (1) simplifies to

$$\vdash_{\mathrm{PA}} \forall x(\forall y(y < x \rightarrow \phi[y]) \rightarrow \phi[x]) \rightarrow \phi[x] \tag{3}$$

and it is called the *complete induction on x for $\phi[x]$*. The CL command indm x applies the following rule:

$$\frac{}{\begin{array}{c}\forall y(y < x \to \phi[y])\\ \phi[x]*\end{array}}$$

for an eigen-variable x.

2.9 The least number principle. Let T be an extension by definitions 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:

$$\exists x\phi[x] \to \exists x(\phi[x] \land \forall y(y < x \to \neg\phi[y])) \ . \tag{1}$$

The least number principle says that if the property $\phi[x]$ holds for some x then it holds for the least such x.

2.10 Theorem *Every extension by definitions T of PA containing the predicate $<$ proves the schema of the least number principle 2.9(1).*

Proof. We prove 2.9(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 2.8(3). Its converse is

$$\phi[x] \to \exists x(\forall y(y < x \to \neg\phi[y]) \land \phi[x])$$

and 2.9(1) logically follows by quantifier operations. □

3 Extensions of PA by Function Symbols

We will extend PA by some basic functions such as division, introduce extensions by minimization, and prove that they are extensions by definition.

3.1 Explicit definitions. Let T be an extension of PA and $\tau[\vec{x}]$ a term of $\mathcal{L}_T$ with at most the n-variables $\vec{t}$ free. The extension of T with the new $n-ary$ function symbol f and the defining axiom the universal closure of $T \vdash f(\vec{x}) = \tau[\vec{x}]$ is called an *extension by an explicit definition.*

3.2 Theorem *If T is an extension by definitions of PA then an extension of T by explicit definition of a function symbol is also an extension by definition.*

Proof. Extend T to S by $f(\vec{x}) = y \leftrightarrow \tau[\vec{x}] = y$ whose existence and uniqueness conditions are trivially provable in T. This last formula is equivalent in S to $f(\vec{x}) = \tau[\vec{x}]$. □

3.3 Small constants. We have used 1 as abbreviation for the term $0'$ in Sect. 1. We now introduce the symbols 1, 2, 3, 4, ... into PA as constants by explicit definitions:

$$\vdash_{\text{PAx}} 1 = 0' \tag{1}$$
$$\vdash_{\text{PAx}} 2 = 1' \tag{2}$$
$$\vdash_{\text{PAx}} 3 = 2' \tag{3}$$
$$\vdash_{\text{PAx}} 4 = 3' \tag{4}$$
$$\vdots$$

3.4 Extensions by minimization. Let T be an 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 with the defining axioms the universal closures of $\phi[\vec{x}, f(\vec{x})]$ and

$$y < f(\vec{x}) \rightarrow \neg\phi[\vec{x}, y] \ . \tag{2}$$

is called *extension by minimization*.

We will use a more suggestive notation as an abbreviation for both defining axioms:

$$f(\vec{x}) = \mu_y[\phi[\vec{x}, y]] \ . \tag{3}$$

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.

Note that the second defining axiom is equivalent in S to

$$\phi[\vec{x}, y] \rightarrow f(\vec{x}) \leq y$$

whenever T contains also the predicate $\leq$.

3.5 Theorem *If T is an extension by definitions of PA containing the predicate $<$ then an extension of T by minimization is also an extension by definition.*

Proof. Extend T to S with $f(\vec{x}) = y \leftrightarrow \psi[\vec{x}, y]$ where $\psi[\vec{x}, y]$ abbreviates $\phi[\vec{x}, y] \land \forall z(z < y \rightarrow \neg\phi[\vec{x}, z])$.

Since $\psi[\vec{x}, f(\vec{x})]$ is equivalent in S to the both defining axioms for the minimization, it suffices to prove in T 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

$$T \vdash \exists y \phi[\vec{x}, y] \rightarrow \exists y(\phi[\vec{x}, y] \land \forall z(z < y \rightarrow \neg\phi[\vec{x}, z])) \ ,$$

which is provable in T by Thm. 2.10. We thus get $\exists y\psi[\vec{x},y]$ in T from 3.4(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 $y_1 = y_2$. □

3.6 Modified subtraction. The following property is needed for the introduction of the modified subtraction:

$$\vdash_{\mathrm{PA}} y \le x \to \exists d\, x = y + d \; . \tag{1}$$

The property follows directly from 2.2(5). However, in CL it must be proved by induction on y. In the base case when $y = 0$ it suffices to instantiate the existential quantifier with $d := x$. In the inductive when $y + 1 \le x$ we wish to prove $\exists d\, x = (y + 1) + d$. Since $y < x$, we get $x = y + d_0$ for some d_0 by IH. It must be the case that $d_0 > 0$, i.e. $d_0 = d_1 + 1$ for some d_1, and it suffices to instantiate $d := d_1$.

We can now introduce the *modified subtraction* function by minimization:

$$\vdash_{\mathrm{PAx}} x \dot{-} y = \mu_d[y \le x \to y + d = x] \tag{2}$$

because its existence condition $\exists d(y \le x \to x = y+d)$ follows from (1) by prenex operations. We have

$$\vdash_{\mathrm{PA}} y \le x \to y + (x \dot{-} y) = x \tag{3}$$

$$\vdash_{\mathrm{PA}} x < y \to x \dot{-} y = 0 \tag{4}$$

(3): This is the positive part of the defining axiom (2).

(4): Assume $x < y$ and take any $z < x \dot{-} y$. From the negative part of (2) we get not $y \le x \to y + z = x$ contradicting $x < y$. Thus $x \dot{-} y \le z$ and hence $x \dot{-} y = 0$.

3.7 Integer division and remainder. The property (1) is needed for the introduction of the integer division and remainder functions and the property (2) asserts their uniqueness:

$$\vdash_{\mathrm{PA}} y > 0 \to \exists q \exists r(x = q{\cdot}y + r \land r < y) \tag{1}$$

$$\vdash_{\mathrm{PA}} r_1 < y \land r_2 < y \land q_1{\cdot}y + r_1 = q_2{\cdot}y + r_2 \to q_1 = q_2 \land r_1 = r_2 \; . \tag{2}$$

(1): We assume $y > 0$ and prove the consequent by complete induction on x where we consider three cases by trichotomy. When $x < y$ then we instantiate $q := 0$ and $r := x$. When $x = y$ we instantiate $q := 1$ and $r := 0$. Finally, when $x > y$ we obtain a d such that $y + d = x$ from 3.6(1). Since $d < x$, we obtain q_1 and r_1 such that $x = q_1{\cdot}d + r_1$ and $r_1 < y$ from IH. We now instantiate: $q := q_1 + 1$ and $r = r_1$.

(2): We assume $r_1 < y$ and $r_2 < y$ and prove $\forall q_2(q_1{\cdot}y + r_1 = q_2{\cdot}y + r_2 \to q_1 = q_2 \land r_1 = r_2)$ by induction on q_1. In the base case when $q_1 = 0$ we assume

$r_1 = q_2{\cdot}y + r_2$ and consider two cases on q_2. If $q_2 = 0$ then $r_1 = r_2$ directly. If $q_2 = p+1$ for some p then we have a contradiction $r_1 = p{\cdot}y + y + r_2 \geq y$.

In the inductive case we assume $(q_1+1){\cdot}y + r_1 = q_2{\cdot}y + r_2$ and consider again two cases on q_2. The case $q_2 = 0$ leads to a similar contradiction as above so we must have $q_2 = p+1$ for some p. Hence $q_1{\cdot}y + r_1 = p{\cdot}y + r_2$ by cancelling y and we get $q_1 = p$, $r_1 = r_2$ from IH and then $q_1 + 1 = q_2$.

We can now introduce the integer division and remainder functions by two minimizations:

$$\vdash_{\text{PAx}} x \div y = \mu_q[y > 0 \to \exists r(x = q{\cdot}y + r \wedge r < y)]$$
$$\vdash_{\text{PAx}} x \bmod y = \mu_r[y > 0 \to \exists q(x = q{\cdot}y + r \wedge r < y)]$$

because their existence conditions follow from (1) by prenex operations.

4 Dyadic Concatenation Function in PA

In order to be able to introduce into PA recursive definitions we need some kind of coding afforded by a pairing function and its associated concatenation function. The extensions of PA presented in this section lead to the introduction of both in Paragraphs 5.3 and 5.4.

4.1 The predicate of divisibility. The binary *divisibility* predicate $x \mid y$, read as x *divides* y is defined in PA by an explicit definition:

$$\vdash_{\text{PAx}} x \mid y \leftrightarrow \exists z\, y = z{\cdot}x \;. \tag{1}$$

The predicate of divisibility is a relation of *partial order* (similar to $\leq$ but without the linearity 2.4(4)) which satisfies the reflexivity, transitivity, and antisymmetry. The partial order is with the least element 1 and the greatest element 0:

$$\vdash_{\text{PA}} x \mid x \tag{2}$$
$$\vdash_{\text{PA}} x \mid y \wedge y \mid z \to x \mid z \tag{3}$$
$$\vdash_{\text{PA}} x \mid 0 \tag{4}$$
$$\vdash_{\text{PA}} x \mid 1 \leftrightarrow x = 1 \tag{5}$$
$$\vdash_{\text{PA}} x \mid y \to x \mid y{\cdot}z \tag{6}$$
$$\vdash_{\text{PA}} x \mid 2{\cdot}y \to 2 \mid x \vee x \mid y \;. \tag{7}$$

(2): We have $x = 1{\cdot}x$ and so 1 witnesses $x \mid x$, i.e. $\exists z\, x = z{\cdot}x$.

(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 $b{\cdot}a$ witnesses $x \mid z$.

(4): We have $0 = 0{\cdot}x$ and so 0 witnesses $x \mid 0$.

(5): The direction $(\leftarrow)$ follows from (2). In the direction $(\rightarrow)$ we assume $x \mid 1$, i.e. $x{\cdot}z = 1$ for some z, and obtain $x = 1$ from 1.14(1).

(6): From $x \mid y$ we get $x{\cdot}w = y$ for some w and thus $w{\cdot}z$ witnesses $x \mid y{\cdot}z$.

(7): Assume $x \mid 2{\cdot}y$, i.e. $x{\cdot}z = 2{\cdot}y$ for some z. We have $x = 2{\cdot}q + r$ for some q and $r < 2$ from 3.7(1). If $r = 0$ then $q{\cdot}z$ witnesses $2 \mid x$. If $r = 1$ we use 3.7(1) again to get $z = 2{\cdot}p + s$ for some p and $s < 2$. Thus $2{\cdot}(2{\cdot}q{\cdot}p + p + q{\cdot}s) + s = 2{\cdot}y$ and we get $2{\cdot}q{\cdot}p + p = y$ from 3.7(2) and p witnesses $x = (2{\cdot}q + 1) \mid y$.

4.2 Powers of two. The predicate $Pow_2(p)$ of p *being a power of* 2, i.e. such that $\exists x\, p = 2^x$, cannot be introduced without coding via 2^x but it has a neat explicit definition:

$$\vdash_{\mathrm{PAx}} Pow_2(p) \leftrightarrow \forall d(d \mid p \to d = 1 \lor 2 \mid d) \; .$$

We first prove the following properties of the predicate:

$$\vdash_{\mathrm{PA}} \neg Pow_2(0) \tag{1}$$
$$\vdash_{\mathrm{PA}} Pow_2(x\mathbf{1}) \leftrightarrow x = 0 \tag{2}$$
$$\vdash_{\mathrm{PA}} Pow_2(x\mathbf{0}) \leftrightarrow x > 0 \land Pow_2(x) \; . \tag{3}$$

(1): Assume contrary $Pow_2(0)$. We have $3 \mid 0$ by 4.1(4) and the instantiation of the definition of $Pow_2(0)$ with $d := 3$ yields $2 \mid 3$, i.e. $2{\cdot}z = 3 = 2{\cdot}1 + 1$ for some z. The use of 3.7(2) yields a contradiction $0 = 1$.

(2): In the direction ($\to$) we assume $Pow_2(x\mathbf{1})$. We have $x\mathbf{1} \mid x\mathbf{1}$ by 4.1(2) and we consider two cases. The case $2 \mid x\mathbf{1}$ leads to a contradiction by 3.7(2). Thus $2 \nmid x\mathbf{1}$ and using the definition of $Pow_2(x\mathbf{1})$ with $d := x\mathbf{1}$ yields $x\mathbf{1} = 1$ and hence $x = 0$. In the direction ($\leftarrow$) we wish to prove $Pow_2(1)$, i.e. $\forall d(d \mid 1 \to d = 1 \lor 2 \mid d)$, so we take any d such that $d \mid 1$ and obtain $d = 1$ by 4.1(5).

(3): In the direction ($\to$) we assume $Pow_2(x\mathbf{0})$ and consider two cases. The case $x = 0$ contradicts (1). Thus $x > 0$. In order to prove $Pow_2(x)$ we take any d such that $d \mid x$. By 4.1(6) we have $d \mid x\mathbf{0}$ and from the assumption $Pow_2(x\mathbf{0})$ we get the desired $d = 1$ or $2 \mid d$. In the direction ($\leftarrow$) we assume $x > 0$ and $Pow_2(x)$. In order to prove $Pow_2(x\mathbf{0})$ we take any d such that $d \mid x\mathbf{0}$. We consider two cases. If $2 \mid d$ there is nothing to prove. If $2 \nmid d$ then we get $d \mid x$ by 4.1(7). We now use the assumption $Pow_2(x)$ to get the desired $d = 1$.

The three above theorems of PA are equivalent to the clauses for Pow_2 which are by *recursion on binary notation*:

$$Pow_2(x\mathbf{1}) \leftarrow x = 0 \tag{4}$$
$$Pow_2(x\mathbf{0}) \leftarrow x > 0 \land Pow_2(x) \tag{5}$$
$$\neg Pow_2(x\mathbf{0}) \leftarrow x = 0 \; . \tag{6}$$

The following paragraph introduces tools for proving properties of functions and predicates satisfying clausal recurrences with recursion on binary notation.

4.3 Binary case analysis and induction. Assume that PA has been extended to contain the predicate $<$ and the explictly introduced *binary successor* functions $x\mathbf{0} = 2{\cdot}x + 0$ and $x\mathbf{1} = 2{\cdot}x + 1$. We have

$$\vdash_{\mathrm{PA}} x > 0 \land x = y\mathbf{0} \to y < x \tag{1}$$
$$\vdash_{\mathrm{PA}} x < x\mathbf{1} \tag{2}$$
$$\vdash_{\mathrm{PA}} \exists y\, x = y\mathbf{0} \lor \exists y\, x = y\mathbf{1} \tag{3}$$
$$\vdash_{\mathrm{PA}} \exists y(x = y\mathbf{0} \land y = 0) \lor \exists y(x = y\mathbf{0} \land y > 0) \lor \exists y\, x = y\mathbf{1}\ . \tag{4}$$

(1): It cannot be the case that $y = 0$ and so $y = z+1$ for some z which witnesses $y < x$ in 2.2(1).

(2): y witnesses $y < x$ in 2.2(1).

(3): Use 3.7(1) with $y := 2$ to obtain $x = 2{\cdot}y + r$ and $r < 2$ for some y and r and consider two cases. When $r = 0$ then $x = y\mathbf{0}$. When $r = 1$ then $x = y\mathbf{1}$.

(4): A straigthforward consequence of (3) by considering two subcases $y = 0$ and $y > 0$ when $x = y\mathbf{0}$.

The theorem (4) justifies the *binary case rule* of CL invoked by `case` $Nb; x$ where CL automatically performs the obvious split, flatten, and eigen-variable rules:

$$\frac{}{\begin{array}{c|c|c} x = y\mathbf{0} & x = y\mathbf{0} & \\ y = 0 & y > 0 & x = y\mathbf{1} \end{array}}$$

with y a new eigen-variable.

Let $\phi[x]$ be a formula of PA with the indicated variable x free and with possibly additional parameters. The *binary induction on x for $\phi[x]$* is the following formula:

$$\vdash_{\mathrm{PA}} \phi[0] \land \forall x(x > 0 \land \phi[x] \to \phi[x\mathbf{0}]) \land \forall x(\phi[x] \to \phi[x\mathbf{1}]) \to \phi[x]\ . \tag{5}$$

Binary induction is reducible to complete induction as follows. Assume the three formulas in the antecedent and continue with complete induction on x for the formula $\phi[x]$ where we do the binary case analysis on x. When $x = y\mathbf{0}$ and $y = 0$ for some y then $x = y\mathbf{0} = 0$ and so $\phi[x]$ holds from the first assumption. When $x = y\mathbf{0}$ and $y > 0$ for some y then $y < x$ by (1) and so $\phi[y]$ holds by the inductive hypothesis of the complete induction. We now use the second assumption to derive $\phi[y\mathbf{0}]$. Finally, when $x = y\mathbf{1}$ for some y then $y < x$ by (2), we get $\phi[y]$ by IH, and $\phi[y\mathbf{1}]$ follows from the third assumption.

The theorem (5) justifies the *rule of binary induction* of CL invoked by ind $Nb; x$ where CL automatically performs the obvious split, flatten, and eigen-variable rules:

$$\frac{}{\begin{array}{c|c|c} & x > 0 & \\ x = 0 & \phi[x] & \phi[x] \\ \phi[x\mathbf{0}]* & \phi[x\mathbf{0}]* & \phi[x\mathbf{1}]* \end{array}}$$

4.4 An auxiliary property of Pow_2. We can now use the clausal recurrences of Pow_2 from Par. 4.2 to prove

$$\vdash_{\mathrm{PA}} Pow_2(p) \land Pow_2(q) \land p < 2{\cdot}q \to p \le q \tag{1}$$

by binary induction on p with the induction formula $\forall q(1)$. The only interesting case is $p\mathbf{0}$ with $p > 0$ and $p\mathbf{0} < 2{\cdot}q$, i.e. $p < q$. We then do a binary case on q, and again, the only interesting case is when $q = q_1\mathbf{0}$ for some $q_1 > 0$. But then IH applies with $q := q_1$, since $Pow_2(q_1)$.

4.5 Powers of dyadic length. The function $2^{|x|}$ yields *two to the power of* $|x|$ which is the *dyadic length* (i.e. a number of dyadic digits) of x. We cannot introduce into PA without additional coding either the dyadic length function or the exponentiation function 2^z. Fortunately, for positive numbers $x + 1$ the power $2^{|x+1|}$ is of the same dyadic size as $x + 1$. This suggests the contextual definition (3). However, in CL we must define $2^{|x|}$ by minimization:

$$\vdash_{\text{PAx}} 2^{|x|} = \mu_p[Pow_2(p) \wedge x + 1 < 2{\cdot}p] \tag{1}$$

whose existence condition

$$\vdash_{\text{PA}} \exists p(Pow_2(p) \wedge x + 1 < 2{\cdot}p) \tag{2}$$

is proved by induction on x. When $x = 0$ we take $p := 1$. For $x + 1$ we obtain from IH a power q such that $x + 1 < 2{\cdot}q$ and take $p := q\mathbf{0}$. Note that (2) asserts that there are anboundedly many powers of two.

$$\vdash_{\text{PA}} 2^{|x|} = p \leftrightarrow Pow_2(p) \wedge p \leq x + 1 \wedge x + 1 < 2{\cdot}p\ . \tag{3}$$

In the direction ($\rightarrow$) we get $Pow_2(2^{|x|})$ and $x + 1 < 2{\cdot}2^{|x|}$ from the positive part of (1). In order to obtain $2^{|x|} \leq x + 1$ we consider three binary cases for $2^{|x|}$. The case $2^{|x|} = 0$ contradicts $x + 1 < 2{\cdot}2^{|x|}$. The case $2^{|x|} = q\mathbf{1}$ for some q implies $q = 0$ and hence $2^{|x|} = 1$ by the clauses for Pow_2. But then $x = 0$ from $x + 1 < 2{\cdot}2^{|x|}$ and so $2^{|x|} \leq x + 1$. The most interesting case is the remaining one when $2^{|x|} = q\mathbf{0}$ for some $q > 0$. Then $Pow_2(q)$ by the clauses for Pow_2 and, since $q < 2^{|x|}$, we get $2^{|x|} = 2{\cdot}q \overset{\text{minimal part of (1)}}{\leq} x + 1$.

In the direction ($\leftarrow$) we assume $Pow_2(p)$ and $p \leq x + 1 < 2{\cdot}p$. We then have:

$$2^{|x|} \overset{\text{minimal part of (1)}}{\leq} p \leq x + 1 \overset{\text{positive part of (1)}}{<} 2{\cdot}2^{|x|}\ .$$

By the positive part also $Pow_2(2^{|x|})$ which, used with $Pow_2(p)$ in 4.4(1), yields also $p \leq 2^{|x|}$.

We now prove as theorems of PA the following properties which are also clauses of CL for $2^{|x|}$ by *dyadic recursion on notation*:

$$\vdash_{\text{PA}} 2^{|0|} = 1 \tag{4}$$

$$\vdash_{\text{PA}} 2^{|x\mathbf{1}|} = 2{\cdot}2^{|x|} \tag{5}$$

$$\vdash_{\text{PA}} 2^{|x\mathbf{2}|} = 2{\cdot}2^{|x|} \tag{6}$$

where the *dyadic successor function* $x\mathbf{2} = 2{\cdot}x + 2$ is introduced into PA by an explicit definition. The proofs are straightforward, for instance in order to prove

(6), we use the implication $\rightarrow$ of (3) to get $Pow_2(2^{|x|})$ and $2^{|x|} \leq x+1 < 2{\cdot}2^{|x|}$. Thus $2^{|x|} > 0$ and hence $Pow_2(2{\cdot}2^{|x|})$ by the clauses for Pow_2. Since the above inequalities trivially imply $2{\cdot}2^{|x|} \leq x\mathbf{2} < 2{\cdot}(2{\cdot}2^{|x|})$, we use $\leftarrow$ of (3) with $x := x\mathbf{2}$ and $p := 2{\cdot}2^{|x|}$ to obtain the desired $2^{|x\mathbf{2}|} = 2{\cdot}2^{|x|}$.

The following paragraph introduces tools for proving properties of functions and predicates satisfying clausal recurrences with recursion on dyadic notation.

4.6 Dyadic case analysis and induction. Assume that PA has been extended to contain the predicate $<$ and the binary-dyadic successor functions. We then have

$$\vdash_{\mathrm{PA}} \; x < x\mathbf{2} \tag{1}$$

$$\vdash_{\mathrm{PA}} \; x = 0 \lor \exists y\, x = y\mathbf{1} \lor \exists y\, x = y\mathbf{2}\ . \tag{2}$$

(1): Use $x:1$ as the witness for $x < x\mathbf{2}$ in 2.2(1).

(2): Do the binary case analysis on x. When $x = y\mathbf{0}$ and $y = 0$ for some y then the first goal $x = 0$ holds. When $x = y\mathbf{0}$ and $y > 0$ for some y then $y = z+1$ for some z. Since $x = (z+1)\mathbf{0} = z\mathbf{2}$, the third goal $\exists y\, x = y\mathbf{2}$ holds for $y := z$. Finally, when $x = y\mathbf{1}$ for some y then the second goal $\exists y\, x = y\mathbf{1}$ holds.

The theorem (2) justifies the *dyadic case rule* of CL invoked by `case` $N_2; x$ where CL automatically performs the obvious split and eigen-variable rules:

$$\frac{}{x = 0 \mid x = y\mathbf{1} \mid x = y\mathbf{2}}$$

with y a new eigen-variable.

Let $\phi[x]$ be a formula of PA with the indicated variable x free and with possibly additional parameters. The *dyadic induction on x for $\phi[x]$* is the following formula:

$$\vdash_{\mathrm{PA}} \; \phi[0] \land \forall x(\phi[x] \rightarrow \phi[x\mathbf{1}]) \land \forall x(\phi[x] \rightarrow \phi[x\mathbf{2}]) \rightarrow \phi[x]\ . \tag{3}$$

Dyadic induction is reducible to complete induction as follows. Assume the three formulas in the antecedent and continue with the complete induction on x for the formula $\phi[x]$ where we do the dyadic case analysis on x. When $x = 0$ then $\phi[x]$ holds from the first assumption. When $x = y\mathbf{1}$ for some y then $y < x$ by 4.3(2) and so $\phi[y]$ holds by the inductive hypothesis of the complete induction. We now use the second assumption to derive $\phi[y\mathbf{1}]$. Finally, when $x = y\mathbf{2}$ for some y then $y < x$ by (1), we get $\phi[y]$ by IH, and $\phi[y\mathbf{2}]$ follows from the third assumption.

The theorem (3) justifies the *rule of dyadic induction* of CL invoked by `ind` $N_2; x$ where CL automatically performs the obvious split, flatten, and eigen-variable rules:

$$\frac{}{\phi[0]* \;\Big|\; \begin{array}{c}\phi[x]\\ \phi[x\mathbf{1}]*\end{array} \;\Big|\; \begin{array}{c}\phi[x]\\ \phi[x\mathbf{2}]*\end{array}}$$

4.7 Auxiliary properties of $2^{|x|}$. The clauses for $2^{|x|}$ in Par. 4.5 are by recursion on dyadic notation and they are used together with dyadic induction and case analysis to prove the following properties:

$$\vdash_{\text{PA}} 2^{|x|} > 0 \tag{1}$$

$$\vdash_{\text{PA}} x > 0 \rightarrow 2^{|2^{|x|}|} = 2^{|x|} \; . \tag{2}$$

(1): By a trivial dyadic induction on x.

(2): By dyadic induction on x. In the base case there is nothing to prove.

In the first inductive case, when $x := x\mathbf{1}$, we wish to prove $2^{|2 \cdot 2^{|x|}|} = 2 \cdot 2^{|x|}$. In order to employ the inductive assumption $x > 0 \rightarrow 2^{|2^{|x|}|} = 2^{|x|}$ we consider two cases. When $x = 0$ the goal is trivially satisfied from the clauses for $2^{|x|}$. When $x > 0$ then IH applies. We now consider three dyadic cases for $2^{|x|}$. The case $2^{|x|} = 0$ leads to a contradiction: $1 = 2^{|0|} = 2^{|2^{|x|}|} \overset{IH}{=} 2^{|x|} = 0$.

When $2^{|x|} = y\mathbf{1}$ for somy y then we get a contradiction as follows: $2 \cdot 2^{|y|} = 2^{|y\mathbf{1}|} = 2^{|2^{|x|}|} \overset{IH}{=} 2^{|x|} = y\mathbf{1}$.

Finally, when $2^{|x|} = y\mathbf{2}$ for some y then Then $2 \cdot 2^{|y|} = 2^{|y\mathbf{2}|} = 2^{|2^{|x|}|} \overset{IH}{=} 2^{|x|} = y\mathbf{2}$ and hence:

$$2^{|2 \cdot 2^{|x|}|} = 2^{|2 \cdot y\mathbf{2}|} = 2^{|y\mathbf{12}|} = 4 \cdot 2^{|y|} = 2 \cdot y\mathbf{2} = 2 \cdot 2^{|x|} \; .$$

In the second inductive case when $x := x\mathbf{2}$ the proof is similar.

4.8 Dyadic concatenation. The two-place function $x \star y$ of *dyadic concatenation* is explicitly defined as

$$\vdash_{\text{PAx}} x \star y = x \cdot 2^{|y|} + y \; . \tag{1}$$

We now prove as theorems of PA the following properties which are also clauses of CL for $\star$ by recursion on dyadic notation:

$$\vdash_{\text{PA}} x \star 0 = x \tag{2}$$

$$\vdash_{\text{PA}} x \star y\mathbf{1} = (x \star y)\mathbf{1} \tag{3}$$

$$\vdash_{\text{PA}} x \star y\mathbf{2} = (x \star y)\mathbf{2} \tag{4}$$

The properties have straightforward proofs. For instance, (3):

$$x \star y\mathbf{1} = x \cdot 2^{|y\mathbf{1}|} + y\mathbf{1} = x \cdot 2 \cdot 2^{|y|} + 2 \cdot y + 1 = (x \cdot 2^{|y|} + y)\mathbf{1} = (x \star y)\mathbf{1} \; .$$

The following properties of dyadic concatenation will be needed below:

$$\vdash_{\text{PA}} 0 \star y = y \tag{5}$$

$$\vdash_{\text{PA}} (x \star y) \star z = x \star (y \star z) \tag{6}$$

$$\vdash_{\text{PA}} 2^{|x \star y|} = 2^{|x|} \cdot 2^{|y|} \tag{7}$$

$$\vdash_{\text{PA}} x_1 \star x_2 = y_1 \star y_2 \wedge 2^{|x_2|} = 2^{|y_2|} \rightarrow x_1 = y_1 \wedge x_2 = y_2 \tag{8}$$

$$\vdash_{\text{PA}} x_1 \star x_2 = y_1 \star y_2 \wedge 2^{|x_1|} = 2^{|y_1|} \rightarrow x_1 = y_1 \wedge x_2 = y_2 \tag{9}$$

$$\vdash_{\text{PA}} 2^{|x|} \cdot 2^{|y|} = 2^{|z|} \rightarrow \exists a \exists b (a \star b = z \wedge 2^{|x|} = 2^{|a|} \wedge 2^{|y|} = 2^{|b|}) \; . \tag{10}$$

(5): By straightforward dyadic induction on y.

(6): By straightforward dyadic induction on z.

(7): By straightforward dyadic induction on y.

(8): By dyadic induction on x_2 with the formula $\forall y_2$(8). In the base case and in both inductive cases we do a dyadic case analysis on y_2. The only interesting subcases are in the inductive cases when we have to instantiate the inductive hypotheses. For instance, in the first inductive case the interesting subcase is when $y_2 = w\mathbf{1}$ for some w and we have assumptions $x_1 \star x_2\mathbf{1} = y_1 \star w\mathbf{1}$ and $2^{|x_2\mathbf{1}|} = 2^{|w\mathbf{1}|}$. Then $x_1 \star x_2 = y_1 \star w$ and $2^{|x_2|} = 2^{|w|}$ so IH applies for $y_2 := w$. We then get:

$$x_1 \star x_2\mathbf{1} = (x_1 \star x_2)\mathbf{1} \overset{\text{IH}}{=} (y_1 \star w)\mathbf{1} = y_1 \star w\mathbf{1} = y_1 \star y_2 \ .$$

(9): Assume $x_1 \star x_2 = y_1 \star y_2$ and $2^{|x_1|} = 2^{|y_1|}$. We then get

$$2^{|x_1|} \cdot 2^{|x_2|} \overset{(7)}{=} 2^{|x_1 \star x_2|} = 2^{|y_1 \star y_2|} \overset{(7)}{=} 2^{|y_1|} \cdot 2^{|y_2|} \ .$$

By 4.7(1) we have $2^{|x_1|} = 2^{|y_1|} > 0$ and so $2^{|x_2|} = 2^{|y_2|}$. We now use (8).

(10): By dyadic induction on z with the formula $\forall y$(10). In the base case when $z := 0$ we instantiate the goal with $a := 0$ and $b := 0$. In the first inductive case with $z := z\mathbf{1}$ we have as assumption $2^{|x|} \cdot 2^{|y|} = 2 \cdot 2^{|z|}$ and we wish to prove $\exists a \exists b(a \star b = z\mathbf{1} \land 2^{|x|} = 2^{|a|} \land 2^{|y|} = 2^{|b|})$. We do a dyadic case analysis on y. When $y = 0$ we instantiate the goal with $a := z\mathbf{1}$ and $b := 0$. When $y = y_1\mathbf{1}$ for some y_1 the assumption simplifies to $2^{|x|} \cdot 2^{|y_1|} = 2^{|z|}$ and we obtain a and b from IH such that $a \star b = z$, $2^{|x|} = 2^{|a|}$, and $2^{|y_1|} = 2^{|b|}$. We then instantiate the goal with $a := a$ and $b := b\mathbf{1}$. The subcase when $y = y_1\mathbf{2}$ for some y_1 is identical to the subcase $y = y_1\mathbf{1}$

The second inductive case when $z := z\mathbf{2}$ is similar to the first inductive case.

4.9 Dyadic sequences containing powers of two. Dyadic sequences containing powers of two will play crucial role in our encoding of finite sequences into natural numbers. We first observe that $2^{|0|} = 1$ and $2^{|x+1|} = (\overbrace{1 \star \cdots \star 1}^{|x+1| \,\dot{-}\, 1})\mathbf{2}$. Thus $2^{|x|} \dot{-} 1 = \overbrace{1 \star \cdots \star 1}^{|x|}$. We have:

$$\vdash_{\text{PA}} \ 2 \cdot 2^{|x|} = (2^{|x|} \dot{-} 1)\mathbf{2} \tag{1}$$

$$\vdash_{\text{PA}} \ 2 \cdot 2^{|x+1|} = 1 \star 2^{|x+1|} \ . \tag{2}$$

(1): We have $2^{|x|} > 0$ by 4.7(1). Hence $2 \cdot 2^{|x|} = 2 \cdot (2^{|x|} \dot{-} 1 + 1) = (2^{|x|} \dot{-} 1)\mathbf{2}$.

(2): We have

$$2 \cdot 2^{|x+1|} = 1 \cdot 2^{|x+1|} + 2^{|x+1|} \overset{4.7(2)}{=} 1 \cdot 2^{|2^{|x+1|}|} + 2^{|x+1|} \overset{4.8(1)}{=} 1 \star 2^{|x+1|} \ .$$

We will show that to every natural number m we can be uniquely find numbers $n, b \geq 0$ such that there are n positive numbers $a_1, a_1, \ldots, a_n > 0$ for which we have:

$$m = \overbrace{2^{|a_1|} \star 2^{|a_2|} \star \cdots \star 2^{|a_n|}}^{n} \star (2^{|b|} - 1) \ . \tag{3}$$

The same put differently is:

$$m = \overbrace{\overbrace{1 \star \cdots \star 1}^{|a_1|-1} \star 2 \star \overbrace{1 \cdots 1}^{|a_2|-1} \star 2 \star \cdots \star \overbrace{1 \star \cdots \star 1}^{|a_n|-1} \star 2}^{n} \star \overbrace{1 \star \cdots \star 1}^{|b|} \ .$$

The existence and uniqueness of trailing and leading powers is asserted by following theorems:

$$\vdash_{\mathrm{PA}} \ \exists n \exists x \, m = n\mathbf{0} \star (2^{|x|} \dot{-} 1) \tag{4}$$

$$\vdash_{\mathrm{PA}} \ n_1\mathbf{0} \star (2^{|x_1|} \dot{-} 1) = n_2\mathbf{0} \star (2^{|x_2|} \dot{-} 1) \rightarrow n_1 = n_2 \wedge 2^{|x_1|} = 2^{|x_2|} \tag{5}$$

$$\vdash_{\mathrm{PA}} \ \exists n \exists x \, m\mathbf{2} = 2^{|x+1|} \star n \tag{6}$$

$$\vdash_{\mathrm{PA}} \ 2^{|x_1+1|} \star n_1 = 2^{|x_2+1|} \star n_2 \rightarrow 2^{|x_1+1|} = 2^{|x_2+1|} \wedge n_1 = n_2 \ . \tag{7}$$

(4): By dyadic induction on m. When $m = 0$ then we witness the goal with $n := x := 0$. In the first inductive case when going from m to $m\mathbf{1}$ we obtain $n\mathbf{0} \star (2^{|x|} \dot{-} 1)$ for some n and x from IH and derive

$$m\mathbf{1} = (n\mathbf{0} \star (2^{|x|} \dot{-} 1))\mathbf{1} = n\mathbf{0} \star (2^{|x|} \dot{-} 1)\mathbf{1} \overset{(1)}{=} n\mathbf{0} \star (2 \cdot 2^{|x|} \dot{-} 1) = n\mathbf{0} \star (2^{|x\mathbf{1}|} \dot{-} 1) \ .$$

Thus $n := n$ and $x := x\mathbf{1}$ witness the goal.

In the second inductive case when going from m to $m\mathbf{2}$ we observe that $m\mathbf{2} = (m+1)\mathbf{0} = (m+1)\mathbf{0} \star (2^{|0|} \dot{-} 1)$ and so it sufficess to witness the goal with $n := m + 1$ and $x := 0$.

(5): By dyadic induction on x_1 with the induction formula $\forall x_2$(5). When $x_1 = 0$ then we assume $n_1\mathbf{0} = n_2\mathbf{0} \star (2^{|x_2|} \dot{-} 1)$ and consider three dyadic cases for x_2. The case $x_2 = 0$ is straightforward. The two other cases $x_2 = S_i(y)$ with $i = 1, 2$ for some y lead to contradictions because we have

$$2^{|S_i(y)|} \dot{-} 1 = 2 \cdot 2^{|y|} \dot{-} 1 \overset{(1)}{=} (2^{|y|} \dot{-} 1)\mathbf{2} \dot{-} 1 = (2^{|y|} \dot{-} 1)\mathbf{1} \tag{8}$$

and so the two sides of the following identity are of different parities:

$$n_1\mathbf{0} = n_2\mathbf{0} \star (2^{|S_i(y)|} \dot{-} 1) \overset{(8)}{=} n_2\mathbf{0} \star (2^{|y|} \dot{-} 1)\mathbf{1} = (n_2\mathbf{0} \star (2^{|y|} \dot{-} 1))\mathbf{1} \ . \tag{9}$$

In the first inductive case when going from x_1 to $x_1\mathbf{1}$ we assume $n_1\mathbf{0} \star (2^{|x_1\mathbf{1}|} \dot{-} 1) = n_2\mathbf{0} \star (2^{|x_2|} \dot{-} 1)$. Similarly as above we have $n_1\mathbf{0} \star (2^{|x_1\mathbf{1}|} \dot{-} 1) = (n_1\mathbf{0} \star (2^{|x_1|} \dot{-} 1))\mathbf{1}$. We now consider three dyadic cases for x_2. The case when $x_2 = 0$ leads to a parity contradiction because $n_2\mathbf{0} \star (2^{|0|} \dot{-} 1) = n_1\mathbf{0}$. The two other cases when $x_2 = S_i(y)$ with $i = 1, 2$ are similar because then

$$(n_1\mathbf{0} \star (2^{|x_1|} \dot{-} 1))\mathbf{1} = n_1\mathbf{0} \star (2^{|x_1\mathbf{1}|} \dot{-} 1) = n_2\mathbf{0} \star (2^{|S_i y|} \dot{-} 1) \overset{(9)}{=} (n_2\mathbf{0} \star (2^{|y|} \dot{-} 1))\mathbf{1} \ .$$

After cancelling the dyadic successor S_1 on both sides we can instantiate IH with $x_2 := y$ and obtain $n_1 = n2$, $2^{|x_1|} = 2^{|y|}$ and hence $2^{|x_1\mathbf{1}|} = 2{\cdot}2^{|x_1|} = 2{\cdot}2^{|y|} = 2^{|S_i(y)|} = 2^{|x_2|}$.

The second inductive case when going from x_1 to $x_1\mathbf{2}$ is almost identical to the first one.

(6): By dyadic induction on m. When $m = 0$ then $0\mathbf{2} = 2 = 2^{|0+1|} \star 0$ and so we witness the goal with $x := n := 0$. In the first inductive case when going from m to $m\mathbf{1}$ we obtain $m\mathbf{2} = 2^{|x+1|} \star n$ for some n and x from IH and we observe that $m\mathbf{12} = 4{\cdot}m + 4 = m\mathbf{20} = (2^{|x+1|} \star n)\mathbf{0}$. We now consider three dyadic cases. When $n = 0$ then, since $2^{|x+1|}\mathbf{0} = 2^{|(x+1)\mathbf{1}|} = 2^{|x\mathbf{2}+1|}$, it suffices to witness the goal with $x := x\mathbf{2}$ and $n := 0$. The case $n = k\mathbf{1}$ for some k leads to a contradiction: $4{\cdot}m + 4 = m\mathbf{20} = (2^{|x+1|} \star k\mathbf{1})\mathbf{0} = (2^{|x+1|} \star k)\mathbf{10} = 4 * (2^{|x+1|} \star k) + 2$. Finally, when $n = k\mathbf{2}$ for some k then

$$(2^{|x+1|} \star k\mathbf{2})\mathbf{0} = (2^{|x+1|} \star k)\mathbf{20} = (2^{|x+1|} \star k)\mathbf{12} = 2^{|x+1|} \star k\mathbf{12}$$

and so it suffices to instantiate the goal with $x := x$ and $n := k\mathbf{12}$.

In the second inductive case when going from m to $m\mathbf{2}$ then for some x and n we have $m\mathbf{22} \overset{\text{IH}}{=} (2^{|x+1|} \star n)\mathbf{2} = 2^{|x+1|} \star n\mathbf{2}$ and so we witness the goal with $x := x$ and $n := n\mathbf{2}$.

(7): We have seen in the proof of (5) how the dyadic induction on x_1 followed by a dyadic case analysis on x_2 has led to the duplication of almost identical cases. We could use the same kind of proof with this property also. However, in order to prevent the duplication of cases we prove (7) by complete induction on x_1 with the induction formula $\forall x_2$(7). Incidentally, measure induction with the measure term $(x_1 + 1) + (x_2 + 1)$ and the induction formula (7) works just as fine.

Instead of dyadic case analysis we will perform the following *case analysis on dyadic concatenation*

$$\vdash_{\text{PA}} \; m = 0 \lor \exists u \exists i (m = u \star i \land u < m \land 2^{|i|} = 2) \tag{10}$$

which is proved by a straightforward dyadic case analysis on m. The case $m = 0$ is trivial. The other two cases when $m = S_i(n)$ for some n and $i = 1, 2$ are similar where we witness the goal with $u := n$ and $i := i$.

Returning to the proof of $\forall x_2$(7) by complete induction on x_1, we take any x_2 and assume $2^{|x_1+1|} \star n_1 = 2^{|x_2+1|} \star n_2$. We apply the case analysis formula (10) to $m := x_1 + 1$ and $m := x_2 + 1$. We thus get $x_1 + 1 = u_1 \star i_1$ and $x_2 + 1 = u_2 \star i_2$ for some u_1, u_2 and i_1, i_2 such that $u_1 \leq x_1$, $u_2 \leq x_2$, and $2^{|i_1|} = 2^{|i_2|} = 2$. We then get

$$\begin{aligned} 2{\cdot}2^{|u_1|} \star n_1 = 2^{|u_1|}{\cdot}2^{|i_1|} \star n_1 \overset{4.8(7)}{=} 2^{|x_1+1|} \star n_1 = 2^{|x_2+1|} \star n_2 \overset{4.8(7)}{=} \\ 2^{|u_2|}{\cdot}2^{|i_2|} \star n_2 = 2{\cdot}2^{|u_2|} \star n_2 \; . \end{aligned} \tag{11}$$

We now consider two cases on u_1, u_2 each whereby we get four cases.

If $u_1 = u_2 = 0$ then we trivially have $2^{|u_1|} = 2^{|u_2|} = 1$ from which $2^{|x_1+1|} = 2^{|x_2+1|}$ follows. We get $n_1 = n_2$ by cancelling the two leading twos in $2 \star n_1 \overset{(11)}{=} 2 \star n_1$ with 4.8(9).

If $u_1 = 0$ and $u_2 = v_2 + 1$ for some v_2 then

$$2 \star n_1 \overset{(11)}{=} 2 \cdot 2^{|v_2+1|} \star n_2 \overset{(2)}{=} (1 \star 2^{|v_2+1|}) \star n_2 \overset{4.8(6)}{=} 1 \star (2^{|v_2+1|} \star n_2)$$

leads to a contradiction after applying 4.8(9).

The case if $u_1 = v_1 + 1$ for some v_1 and $u_2 = 0$ leads to a similar contradiction as the preceding case.

Finally, when $u_1 = v_1 + 1$, $u_2 = v_2 + 1$ for some v_1 and v_2 then (11) simplifies similarly as above to $1 \star (2^{|v_1+1|} \star n_1) = 1 \star (2^{|v_2+1|} \star n_2)$. After the cancellation of the two leading ones with 4.8(9), we apply induction hypothesis with $x_2 := v_2$ because we have $v_1 < u_1 \leq x_1$. We thus get $n_1 = n_2$ and $2^{|v_1+1|} = 2^{|v_2+1|}$ from which $2^{|x_1+1|} = 2^{|x_2+1|}$ follows.

4.10 The splitting predicate. We will now define a three-place predicate $t \doteq \begin{bmatrix} v \\ m \end{bmatrix}$ holding if $t = v \star m$ and t and v have almost the same dyadic size. The predicate will be crucial to the introduction of dyadic pairing in the following section.

$$\vdash_{\mathrm{PAx}} \; t \doteq \begin{bmatrix} v \\ m \end{bmatrix} \leftrightarrow t = v \star m \wedge \exists w \exists i (v = w \star i \wedge 2^{|m|} = 2^{|w|} \wedge 2^{|i|} \leq 2) \tag{1}$$

We can vizualize the definition as follows: $t = \begin{array}{c} \boxed{w|i} \\ \boxed{\;v\;} \\ \star \\ \boxed{m|\;\;} \end{array}$.

The following are some consequences of the definition:

$$\vdash_{\mathrm{PA}} \; 2^{|v|} = 2^{|m|} \rightarrow v \star m \doteq \begin{bmatrix} v \\ m \end{bmatrix} \tag{2}$$

$$\vdash_{\mathrm{PA}} \; t \doteq \begin{bmatrix} v \\ m \end{bmatrix} \rightarrow t = v \star m \tag{3}$$

$$\vdash_{\mathrm{PA}} \; t_1 \doteq \begin{bmatrix} v \\ m \end{bmatrix} \wedge t_2 \doteq \begin{bmatrix} v \\ m \end{bmatrix} \rightarrow t_1 = t_2 \tag{4}$$

$$\vdash_{\mathrm{PA}} \; 2^{|v_1|} = 2^{|m_1|} \rightarrow v_2 \star m_2 \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix} \leftrightarrow (v_1 \star v_2) \star (m_1 \star m_2) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix} \tag{5}$$

$$\vdash_{\mathrm{PA}} \; t \doteq \begin{bmatrix} v \\ m_1 \star m_2 \end{bmatrix} \rightarrow \exists v_1 \exists v_2 (v = v_1 \star v_2 \wedge 2^{|v_1|} = 2^{|m_1|} \wedge v_2 \star m_2 \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}) \; . \tag{6}$$

(2): Directly from the definition instantiating $t := v \star m$, $w := v$, and $i := 0$.

(3): Directly from the definition.

(4): By two applications of (3).

(5): We assume $2^{|v_1|} = 2^{|m_1|}$ and in the direction $(\rightarrow)$ also $v_2 \star m_2 \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$. We get $v_2 = w \star i$, $2^{|w|} = 2^{|m_2|}$ and $2^{|i|} \leq 2$ for some w and i from (1). Since

$$2^{|v_1 \star w|} \overset{4.8(7)}{=} 2^{|v_1|}.2^{|w|} = 2^{|m_1|}.2^{|m_2|} \overset{4.8(7)}{=} 2^{|m_1 \star m_2|}$$

and $v_1 \star v_2 \overset{4.8(6)}{=} (v_1 \star w) \star i$, the use of (1) with $w := v_1 \star w$, $i := i$ yields $(v_1 \star v_2) \star (m_1 \star m_2) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}$.

In the direction $(\leftarrow)$ we assume $(v_1 \star v_2) \star (m_1 \star m_2) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}$ and from (1) we get $v_1 \star v_2 = w \star i$, $2^{|m_1 \star m_2|} = 2^{|w|}$, and $2^{|i|} \leq 2$ for some w and i. We then get $2^{|m_1|}.2^{|m_2|} = 2^{|w|}$ by 4.8(7) and $w = w_1 \star w_2$, $2^{|w_1|} = 2^{|m_1|}$, $2^{|w_2|} = 2^{|m_2|}$ for some w_1, w_2 from 4.8(10). The situation can be visualized as follows:

$$(v_1 \star v_2) \star (m_1 \star m_2) = \begin{array}{|c|c|c|} \hline w_1 & w_2 & i \\ \hline \multicolumn{2}{|c|}{w} & i \\ \hline v_1 & \multicolumn{2}{c|}{v_2} \\ \hline \multicolumn{3}{c}{\star} \\ \hline m_1 & m_2 & \\ \hline \end{array} \; .$$

By 4.8(6) we then get $v_1 \star v_2 = w_1 \star (w_2 \star i)$ and 4.8(9) yields $v_2 = w_2 \star i$. We now use (1) with $w := w_2$ and $i := i$ to derive the desired $v_2 \star m_2 \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$.

(6): Using the assumption with (1) yields $t = v \star (m_1 \star m_2)$, $v = w \star i$ and $2^{|m_1 \star m_2|} = 2^{|w|}$ for some w and i. By a threefold use of 4.8(7) we get

$$2^{|v|} = 2^{|w \star i|} \overset{4.8(7)}{=} 2^{|w|}.2^{|i|} = 2^{|m_1 \star m_2|}.2^{|i|} \overset{4.8(7)}{=} 2^{|m_1|}.2^{|m_2|}.2^{|i|} \overset{4.8(7)}{=} 2^{|m_1|}.2^{|m_2 \star i|} \; .$$

Thus by 4.8(10) we get $v_1 \star v_2 = v$ and $2^{|m_1|} = 2^{|v_1|}$ for some v_1 and v_2. We now use (5) in the direction $(\leftarrow)$ to obtain $v_2 \star m_2 \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$. The conclusion of the property is now witnessed by v_1 and v_2.

4.11 The existence of splits. We wish to prove that every natural number can be split as follows:

$$\vdash_{\mathrm{PA}} \exists v \exists m\, t \doteq \begin{bmatrix} v \\ m \end{bmatrix} \; . \tag{1}$$

(1) is proved by obtaining w, i, and m from (2) and then by witnessing $v := w \star i$ and $m := m$.

$$\vdash_{\mathrm{PA}} \exists w \exists i \exists m (t = w \star i \star m \wedge 2^{|w|} = 2^{|m|} \wedge 2^{|i|} \leq 2) \tag{2}$$

(2) is proved by complete induction on t where we consider two cases by 4.9(10). When $t = 0$, we witness the property with $w := i := m := 0$.

When $t = u \star i$, $u < t$, and $2^{|i|} = 2$ for some u and i we obtain by IH w, j, and m such that $u = w \star j \star m$, $2^{|w|} = 2^{|m|}$, and $2^{|j|} \leq 2$.

We now consider two cases. If $2^{|j|} = 2$ then we wish to continue as follows:

$$u = \begin{array}{c} \boxed{w \mid j} \\ \star \\ \boxed{m \mid } \end{array} \quad \overset{j=1,2}{\Rightarrow} \quad t = u \star i = \begin{array}{c} \boxed{w \mid j \mid 0} \\ \star \\ \boxed{m \mid i \mid } \end{array}$$

Namely, we have $2^{|w \star j|} = 2^{|m \star i|}$ by 4.8(7), and

$$t = u \star i = (w \star j \star m) \star i \overset{4.8(6)}{=} w \star j \star (m \star i) = w \star j \star 0 \star (m \star i)\ .$$

Hence it suffices to witness (1) with $w := w \star j$, $i := 0$, and $m := m \star i$.

If $2^{|j|} < 2$ then $2^{|j|} = 1$ by 4.7(1). It cannot be the case that $j = S_k(l)$ with $k = 1, 2$ because then $2^{|S_k(l)|} = 2{\cdot}2^{|l|} \overset{4.9(1)}{=} 2{\cdot}2^{|l|} + 2 \geq 2$. Thus $j = 0$ and we wish to continue as follows:

$$u = \begin{array}{c} \boxed{w \mid 0} \\ \star \\ \boxed{m \mid } \end{array} \wedge\, m \star i = \begin{array}{|c|c|} \hline m & i \\ \hline k \mid & m_1 \\ \hline \end{array} \quad \Rightarrow \quad t = u \star i = \begin{array}{c} \boxed{w \mid k} \\ \star \\ \boxed{m_1 \mid } \end{array}$$

Namely, we have

$$t = u \star i = (w \star 0 \star m) \star i \overset{4.8(6)}{=} w \star (m \star i) \overset{*}{=} w \star (k \star m_1) \overset{4.8(6)}{=} (w \star k) \star m_1$$

where in the step marked by $*$ we obtain $k \star m_1 = m \star i$, $2^{|k|} = 2^{|i|}$, and $2^{|m_1|} = 2^{|m|}$ for some k and m_1 from by 4.8(10) because $2^{|i|}{\cdot}2^{|m|} = 2^{|m|}{\cdot}2^{|i|} \overset{4.8(7)}{=} 2^{|m \star i|}$. Hence $w := w$, $i := k$, and $m := m_1$ witness (1).

4.12 Some properties of squares. In order to be able to prove the theorem 4.13(1) asserting the uniqueness of splits we need two properties of the squaring function. Property (1) asserts that the function is injective. Property (2) is equivalent to the famous theorem already known to the ancient Greeks asserting the irrationality of $\sqrt{2}$. Property (3) is a simple consequence of the two.

$$\vdash_{\mathrm{PA}}\ x^2 = y^2 \rightarrow x = y \tag{1}$$

$$\vdash_{\mathrm{PA}}\ x^2 = 2{\cdot}y^2 \rightarrow x = 0 \wedge y = 0 \tag{2}$$

$$\vdash_{\mathrm{PA}}\ x^2{\cdot}i = y^2{\cdot}j \wedge x > 0 \wedge 1 \leq i \leq 2 \wedge 1 \leq j \leq 2 \rightarrow x = y \wedge i = j \tag{3}$$

(1): Assume to the contrary that $x \neq y$. If $x < y$ then $x + d + 1 = y$ for some d. We get a contradiction $x^2 = (x + d + 1)^2 \geq x^2 + (d + 1)^2 \geq x^2 + 1 > x^2$. The case $y < x$ is similar.

(2): By measure induction with the measure $x + y$. We consider three binary cases on x. The case $x = 0$ is straightforward. When $x = z\mathbf{0}$ for some $z > 0$ then $2{\cdot}z^2 = y^2$ and, since $z + y < x + y$, we get $x = 2{\cdot}z \overset{\mathrm{IH}}{=} 0$ and $y \overset{\mathrm{IH}}{=} 0$. The case

$x = z\mathbf{1}$ for some z leads to a contradiction because the two sides of the identity are of different parities.

(3): We consider four cases. In two cases $i = j = 1$ or $i = j = 2$ we apply (1) and in the remaining cases $i = 1$, $j = 2$ or $i = 2$, $j = 1$ we apply (2).

4.13 The uniqueness of splits.

$$\vdash_{\text{PA}} t \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix} \wedge t \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix} \rightarrow v_1 = v_2 \wedge m_1 = m_2 \tag{1}$$

(1) directly follows from 4.10(1) and from the following auxiliary property:

$$\begin{aligned} &\vdash_{\text{PA}} w_1 \star i_1 \star m_1 = w_2 \star i_2 \star m_2 \wedge 2^{|i_1|} \leq 2 \wedge 2^{|w_1|} = 2^{|m_1|} \wedge \\ &\quad 2^{|i_2|} \leq 2 \wedge 2^{|w_2|} = 2^{|m_2|} \rightarrow w_1 = w_2 \wedge i_1 = i_2 \wedge m_1 = m_2 \ . \end{aligned} \tag{2}$$

(2): We assume the antecedent and derive:

$$\begin{aligned} (2^{|m_1|})^2 \cdot 2^{|i_1|} = 2^{|w_1|} \cdot 2^{|i_1|} \cdot 2^{|m_1|} &\overset{4.8(7)}{=} 2^{|w_1 \star i_1|} \cdot 2^{|m_1|} \overset{4.8(7)}{=} \\ 2^{|w_1 \star i_1 \star m_1|} = 2^{|w_2 \star i_2 \star m_2|} &\overset{4.8(7)}{=} 2^{|w_2 \star i_2|} \cdot 2^{|m_2|} \overset{4.8(7)}{=} \\ 2^{|w_2|} \cdot 2^{|i_2|} \cdot 2^{|m_2|} &= (2^{|m_2|})^2 \cdot 2^{|i_2|} \end{aligned}$$

and $2^{|i_1|} > 0$, $2^{|2_1|} > 0$, $2^{|m_1|} > 0$ by 4.7(1). Property 4.12(3) applies and we obtain $2^{|m_1|} = 2^{|m_2|}$ and $2^{|i_1|} = 2^{|i_2|}$ from it. We now apply 4.8(8) to $w_1 \star i_1 \star m_1 = w_2 \star i_2 \star m_2$ and get $m_1 = m_2$ as well as $w_1 \star i_1 = w_2 \star i_2$. Another application of the same property to the last formula yields $i_1 = i_2$ and $w_1 = w_2$.

5 Dyadic Pairing and List Concatenation Functions in PA

5.1 Dyadic numbers as sequences. The importance of splits can be seen in their relation to finite sequences. Every number t can be uniquely split into a *value* sequence v and a *marker* sequence m such that $t \doteq \begin{bmatrix} v \\ m \end{bmatrix}$, and there are unique numbers n, x_1, …, x_n, y, and $i \leq 2$ such that

$$\begin{aligned} v &= (x_1{+}1) \star (x_2{+}1) \star \cdots \star (x_n{+}1) \star y \qquad\qquad \star\, i \\ m &= 2^{|x_1+1|} \star 2^{|x_2+1|} \star \cdots \star 2^{|x_n+1|} \star (2^{|y|} \dot{-} 1) \ , \end{aligned}$$

The numbers x_1, …, x_n are said to be the *elements* of the sequence t whereas the number $y \star i \star (2^{|y|} \dot{-} 1)$ is the *atom* at its end. The atom is $0 = y \star i \star (2^{|y|} \dot{-} 1)$ iff $y = 0$ and $j = 0$.

5.2 Adjustment of atoms. By the discussion in the preceding paragraph every sequence, i.e. every number, ends with an atom at the end. We will define by (2) a function $Adj(t)$ which replaces the atom with the atom 0. The existence condition for the definition is:

$$\vdash_{\mathrm{PA}} \exists s \exists v_1 \exists v_2 \exists m \exists y (t \doteq \begin{bmatrix} v_1 \star v_2 \\ m\mathbf{0} \star (2^{|y|} \dot{-} 1) \end{bmatrix} \wedge 2^{|v_1|} = 2^{|m\mathbf{0}|} \wedge s \doteq \begin{bmatrix} v_1 \\ m\mathbf{0} \end{bmatrix}) \ . \tag{1}$$

(1): We have $t \doteq \begin{bmatrix} v \\ n \end{bmatrix}$ for some v and n by 4.11(1) and $n = m\mathbf{0} \star (2^{|y|} \dot{-} 1)$ for some m and y by 4.9(4). We use 4.10(6) to obtain v_1 and v_2 such that $v = v_1 \star v_2$ and $2^{|v_1|} = 2^{|m\mathbf{0}|}$. We now witness (1) with v_1, v_2, m, and y.

$$\vdash_{\mathrm{PAx}} Adj(t) = \mu_s [\exists v_1 \exists v_2 \exists m \exists y (t \doteq \begin{bmatrix} v_1 \star v_2 \\ m\mathbf{0} \star (2^{|y|} \dot{-} 1) \end{bmatrix} \wedge 2^{|v_1|} = 2^{|m\mathbf{0}|} \wedge s \doteq \begin{bmatrix} v_1 \\ m\mathbf{0} \end{bmatrix})] \ . \tag{2}$$

A moment of reflection reveals that t is an atom iff $Adj(t) = 0$.

We will find need the following properties of adjustments:

$$\vdash_{\mathrm{PA}} t \doteq \begin{bmatrix} v_1 \star v_2 \\ m\mathbf{0} \star (2^{|y|} \dot{-} 1) \end{bmatrix} \wedge 2^{|v_1|} = 2^{|m\mathbf{0}|} \rightarrow Adj(t) \doteq \begin{bmatrix} v_1 \\ m\mathbf{0} \end{bmatrix} \tag{3}$$

$$\vdash_{\mathrm{PA}} Adj(0) = 0 \tag{4}$$

$$\vdash_{\mathrm{PA}} Adj((x+1) \star 2^{|x+1|}) = (x+1) \star 2^{|x+1|} \tag{5}$$

$$\vdash_{\mathrm{PA}} Adj(t) \doteq \begin{bmatrix} v \\ m \end{bmatrix} \rightarrow 2^{|v|} = 2^{|m|} \tag{6}$$

$$\vdash_{\mathrm{PA}} Adj(t) > 0 \rightarrow \exists x \exists v \exists m \, t \doteq \begin{bmatrix} (x+1) \star v \\ 2^{|x+1|} \star m \end{bmatrix} \ . \tag{7}$$

(3): Assume $t \doteq \begin{bmatrix} v_1 \star v_2 \\ m\mathbf{0} \star (2^{|y|} \dot{-} 1) \end{bmatrix}$ and use (2) to obtain $t \doteq \begin{bmatrix} w_1 \star w_2 \\ n\mathbf{0} \star (2^{|z|} \dot{-} 1) \end{bmatrix}$, $2^{|w_1|} = 2^{|n\mathbf{0}|}$, and $Adj(t) \doteq \begin{bmatrix} w_1 \\ n\mathbf{0} \end{bmatrix}$ for some w_1, w_2, n, and z. By 4.13(1) we get $v_1 \star v_2 = w_1 \star w_2$ and $m\mathbf{0} \star (2^{|y|} \dot{-} 1) = n\mathbf{0} \star (2^{|z|} \dot{-} 1)$. Using the latter identity with 4.9(5) we get $m = n$. Since now $2^{|v_1|} = 2^{|m\mathbf{0}|} = 2^{|n\mathbf{0}|} = 2^{|w_1|}$, we use the former identity with 4.8(9) to get $v_1 = w_1$ and $v_2 = w_2$.

(4): Obtain $0 \doteq \begin{bmatrix} v_1 \star v_2 \\ m\mathbf{0} \star (2^{|y|} \dot{-} 1) \end{bmatrix}$, $2^{|v_1|} = 2^{|m\mathbf{0}|}$, and $Adj(0) \doteq \begin{bmatrix} v_1 \\ m\mathbf{0} \end{bmatrix}$ for some v_1, v_2, m, and y by (2). We have $0 = (v_1 \star v_2) \star (m\mathbf{0} \star (2^{|y|} \dot{-} 1))$ by 4.10(3) and then $v_1 = m\mathbf{0} = 0$ by two dyadic cases on $m\mathbf{0} \star (2^{|y|} \dot{-} 1)$ and $v_1 \star v_2$. Thus $Adj(0) \overset{4.10(3)}{=} v_1 \star m\mathbf{0} = 0$.

(5): We need a small lemma which can be also inserted as a cut into the proof of (5):

$$\vdash_{\mathrm{PA}} \exists m \, 2^{|x+1|} = m\mathbf{0} \ . \tag{8}$$

(8): We use a binary case analysis on x. When $x = 0$ take $m := 1$. When $x = y\mathbf{0}$ for a $y > 0$ then $2^{|x+1|} = 2^{|y\mathbf{1}|} = 2{\cdot}2^{|y|}$ and we can take $m := 2^{|y|}$. When $x = y\mathbf{1}$ then $2^{|x+1|} = 2^{|y\mathbf{2}|} = 2{\cdot}2^{|y|}$ and we can take $m := 2^{|y|}$ again.

Back to the proof of (5), we have $2^{|x+1|} \overset{4.7(2)}{=} 2^{|2^{|x+1|}|}$, and hence $(x+1) \star 2^{|x+1|} \doteq \begin{bmatrix} x+1 \\ 2^{|x+1|} \end{bmatrix}$ by 4.10(2). From (8) we get $2^{|x+1|} = m\mathbf{0}$ for some m. Since $2^{|0|} \dot{-} 1 = 0$, we can use (3) with $v_2 := y := 0$ to obtain $Adj((x+1) \star 2^{|x+1|}) \doteq \begin{bmatrix} x+1 \\ 2^{|x+1|} \end{bmatrix}$. We now use 4.10(4).

(6): Assume $Adj(t) \doteq \begin{bmatrix} v \\ m \end{bmatrix}$ and obtain $Adj(t) \doteq \begin{bmatrix} w \\ n\mathbf{0} \end{bmatrix}$, $2^{|w|} = 2^{|n\mathbf{0}|}$ for some w, n from (2). We now use 4.13(1).

(7): Assume $Adj(t) > 0$ and obtain $t \doteq \begin{bmatrix} v_1 \star v_2 \\ m\mathbf{0} \star (2^{|y|} \dot{-} 1) \end{bmatrix}$, $2^{|v_1|} = 2^{|m\mathbf{0}|}$, and $Adj(t) \doteq \begin{bmatrix} v_1 \\ m\mathbf{0} \end{bmatrix}$ for some v_1, v_2, m, and y by (2). We now consider two monadic cases for m. If $m = 0$ then $2^{|v_1|} = 1$ implies $v_1 = 0$ and we get a contradiction $0 < Adj(t) \overset{4.10(3)}{=} v_1 \star m\mathbf{0} = 0$.

If $m = n+1$ for some n then $m\mathbf{0} = n\mathbf{2} \overset{4.9(6)}{=} 2^{|a+1|} \star k$ for some a and k. From 4.10(6) we now get, w_1, w_2 such that $v_1 = w_1 \star w_2$ and $2^{|w_1|} = 2^{|2^{|a+1|}|} \overset{4.7(2)}{=} 2^{|a+1|}$. It cannot be the case that $w_1 = 0$ because we would then have $1 = 2^{|w_1|} = 2^{|a+1|} = 2^{|2^{|a+1|}|} = 2^{|1|} = 2$. Thus $w_1 = x+1$ for some x and, since $(x+1) \star (w_2 \star v_2) \overset{4.8(6)}{=} (w_1 \star w_2) \star v_2 = v_1 \star v_2$ and also

$$2^{|x+1|} \star (k \star (2^{|y|} \dot{-} 1)) \overset{4.8(6)}{=} (2^{|a+1|} \star k) \star (2^{|y|} \dot{-} 1) = m\mathbf{0} \star (2^{|y|} \dot{-} 1) \ ,$$

we can witness the conclusion of (7) with $x := x$, $v := w_2 \star v_2$, and $m := k \star (2^{|y|} \dot{-} 1)$.

5.3 Introduction of a dyadic list concatenation function into PA. We wish to introduce an infix two-place *dyadic list concatenation* function $\boxplus$ by a minimisation (2). Its existence condition is:

$$\vdash_{\mathrm{PA}} \exists u \forall v_1 \forall v_2 \forall m_1 \forall m_2 (Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix} \land t \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix} \rightarrow u \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}) \qquad (1)$$

(1): We use 4.11(1) twice to obtain $Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix}$ and $t \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$ for some v_1, v_2, m_1, and m_2. We witness the property with $u = (v_1 \star v_2) \star (m_1 \star m_2)$ and in order to prove it we take any w_1, w_2, n_1, and n_2 such that $Adj(s) \doteq \begin{bmatrix} w_1 \\ n_1 \end{bmatrix}$ and $t \doteq \begin{bmatrix} w_2 \\ n_2 \end{bmatrix}$. By a twofold use of 4.13(1) we get $w_1 = v_1$, $w_2 = v_2$, $n_1 = m_1$, and

$n_2 = m_2$. We get $Adj(s) = w_2 \star n_2$ from 4.10(3) and $2^{|w_2|} = 2^{|n_2|}$ from 5.2(6). 4.10(5) now applies in the direction ($\rightarrow$) and we get $u \doteq \begin{bmatrix} w_1 \star w_2 \\ n_1 \star n_2 \end{bmatrix}$.

$$\vdash_{\mathrm{PAx}} s \boxplus t = \mu_u[\forall v_1 \forall v_2 \forall m_1 \forall m_2 (Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix} \land t \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix} \rightarrow u \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix})] \tag{2}$$

The concatenation function has following properties:

$$\vdash_{\mathrm{PA}} s \boxplus Adj(t) = Adj(s \boxplus t) \tag{3}$$
$$\vdash_{\mathrm{PA}} s \boxplus (t \boxplus u) = (s \boxplus t) \boxplus u \tag{4}$$
$$\vdash_{\mathrm{PA}} Adj(s \boxplus t) = 0 \rightarrow Adj(s) = 0 \ . \tag{5}$$

(3): By 5.2(2) we have $s \doteq \begin{bmatrix} v_1 \star w_1 \\ m_1\mathbf{0} \star (2^{|y_1|} \dot{-} 1) \end{bmatrix}$, and $Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1\mathbf{0} \end{bmatrix}$ for some v_1, w_1, m_1, and y_1. We similarly obtain $t \doteq \begin{bmatrix} v_2 \star w_2 \\ m_2\mathbf{0} \star (2^{|y_2|} \dot{-} 1) \end{bmatrix}$, $2^{|v_2|} = 2^{|m_2\mathbf{0}|}$, and $Adj(t) \doteq \begin{bmatrix} v_2 \\ m_2\mathbf{0} \end{bmatrix}$ for some v_2, w_2, m_2, and y_2. By a twofold use of (2) we get $s \boxplus Adj(t) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1\mathbf{0} \star m_2\mathbf{0} \end{bmatrix}$ and $s \boxplus t \doteq \begin{bmatrix} v_1 \star (v_2 \star w_2) \\ m_1\mathbf{0} \star (m_2\mathbf{0} \star (2^{|x_2|} \dot{-} 1)) \end{bmatrix}$. We then get $s \boxplus t \doteq \begin{bmatrix} (v_1 \star v_2) \star w_2 \\ (m_1\mathbf{0} \star m_2\mathbf{0}) \star (2^{|x_2|} \dot{-} 1) \end{bmatrix}$ by two applications of 4.8(6). Since we have

$$2^{|v_1 \star v_2|} \overset{4.8(7)}{=} 2^{|v_1|} \cdot 2^{|v_2|} = 2^{|m_1\mathbf{0}|} \cdot 2^{|m_2\mathbf{0}|} \overset{4.8(7)}{=} 2^{|m_1\mathbf{0} \star m_2\mathbf{0}|}$$

and a simple dyadic case on m_2 proves $m_1\mathbf{0} \star m_2\mathbf{0} = k\mathbf{0}$ for some k, we can apply 5.2(3) to obtain $Adj(s \boxplus t) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1\mathbf{0} \star m_2\mathbf{0} \end{bmatrix}$. We now get the desired $Adj(s \boxplus t) = s \boxplus Adj(t)$ by 4.10(4).

(4): We have $Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix}$, $Adj(t) \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$, and $u \doteq \begin{bmatrix} v_3 \\ m_3 \end{bmatrix}$ for some v_1, v_2, v_3, m_1, m_2, and m_3 by a triple use of 4.11(1). Three uses of (2) then yield $t \boxplus u \doteq \begin{bmatrix} v_2 \star v_3 \\ m_2 \star m_3 \end{bmatrix}$, $s \boxplus (t \boxplus u) \doteq \begin{bmatrix} v_1 \star (v_2 \star v_3) \\ m_1 \star (m_2 \star m_3) \end{bmatrix}$, and $s \boxplus Adj(t) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}$. (3) applied to the last formula yields $Adj(s \boxplus t) \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}$ and another use of (2) gives $(s \boxplus t) \boxplus u \doteq \begin{bmatrix} (v_1 \star v_2) \star v_3 \\ (m_1 \star m_2) \star m_3 \end{bmatrix}$. Two uses of 4.8(6) yield $v_1 \star (v_2 \star v_3) = (v_1 \star v_2) \star v_3$ and $m_1 \star (m_2 \star m_3) = (m_1 \star m_2) \star m_3$. We now get $s \boxplus (t \boxplus u) = (s \boxplus t) \boxplus u$ by 4.10(4).

(5): Assume $Adj(s \boxplus t) = 0$. By a two-fold use of 4.11(1) we have $Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix}$ and $Adj(t) \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$ for some v_1, v_2, m_1, and m_2. Thus $s \boxplus Adj(t) \doteq$

$\begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}$ by (2) and we have:

$$0 = Adj(s \boxplus t) \overset{(3)}{=} s \boxplus Adj(t) \overset{4.10(3)}{=} (v_1 \star v_2) \star (m_1 \star m_2)\ .$$

Some dyadic case analyses now yield $v_1 = v_2 = m_1 = m_2 = 0$ and so $Adj(t) \overset{4.10(3)}{=} v_2 \star m_2 = 0$.

5.4 Introduction of a dyadic pairing function into PA. We define a binary infix function ; by minimisation:

$$\vdash_{\text{PAx}}\ x; t = \mu_s[s = ((x+1) \star 2^{|x+1|}) \boxplus t] \tag{1}$$

whose existence condition is trivially satisfied. The reader will note that we could have defined the function explicitly by $x; t = ((x+1) \star 2^{|x+1|}) \boxplus t$ but then CL would 'open' the definition automatically by replacing terms $x; t$ by the right-hand-side. This would result in decreased readability.

We let ; associate to the right, i.e. $a; b; c$ stands for $a; (b; c)$. We have the following auxiliary property:

$$\vdash_{\text{PA}}\ t \doteq \begin{bmatrix} v \\ m \end{bmatrix} \rightarrow x; t \doteq \begin{bmatrix} (x+1) \star v \\ 2^{|x+1|} \star m \end{bmatrix}\ . \tag{2}$$

Assume $t \doteq \begin{bmatrix} v \\ m \end{bmatrix}$, Since $2^{|x+1|} = 2^{|2^{|x+1|}|}$ by 4.7(2), we have $(x+1) \star 2^{|x+1|} \doteq \begin{bmatrix} x+1 \\ 2^{|x+1|} \end{bmatrix}$ by 4.10(2), and hence $Adj((x+1) \star 2^{|x+1|}) \doteq \begin{bmatrix} x+1 \\ 2^{|x+1|} \end{bmatrix}$ by 5.2(5). Since $x; t = ((x+1) \star 2^{|x+1|}) \boxplus t$, we get $x; t \doteq \begin{bmatrix} (x+1) \star v \\ 2^{|x+1|} \star m \end{bmatrix}$ by 5.3(2).

The function ; is a suitable pairing function because it satisfies the *pairing* property (3), the *case analysis on dyadic lists* (4) asserting that every non-atomic number is a pair, and the property (5) which conversely asserts that the numbers of the form $x; t$ are not atoms.

$$\vdash_{\text{PA}}\ x_1; t_1 = x_2; t_2 \rightarrow x_1 = x_2 \land t_1 = t_2 \tag{3}$$
$$\vdash_{\text{PA}}\ Adj(t) = 0 \lor \exists x \exists s\, t = x; s \tag{4}$$
$$\vdash_{\text{PA}}\ Adj(x; t) > 0 \tag{5}$$

(3): We have $t_1 \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix}$ for some v_1, m_1 by 4.11(1) and $x_1; t_1 \doteq \begin{bmatrix} (x_1+1) \star v_1 \\ 2^{|x_1+1|} \star m_1 \end{bmatrix}$ by (2). We similarly get $x_2; t_2 \doteq \begin{bmatrix} (x_2+1) \star v_2 \\ 2^{|x_2+1|} \star m_2 \end{bmatrix}$ for some v_2 and m_2. A use of 4.13(1) with the assumption $x_1; t_1 = x_2; t_2$ yields $(x_1+1) \star v_1 = (x_2+1) \star v_2$ and $2^{|x_1+1|} \star m_1 = 2^{|x_2+1|} \star m_2$. We get $2^{|x_1+1|} = 2^{|x_2+1|}$ and $m_1 = m_2$ from the latter formula by 4.9(7). A use of 4.8(9) with the former formula yields $x_1 = x_2$ and $v_1 = v_2$. We now obtain $t_1 = t_2$ by 4.10(4).

(4): When $Adj(t) = 0$ there is nothing to prove so assume $Adj(t) > 0$ and use 5.2(7) to obtain x, v, and m such that $t \doteq \begin{bmatrix}(x+1)\star v\\ 2^{|x+1|}\star m\end{bmatrix}$. Since $t \overset{4.10(3)}{=} ((x+1)\star v)\star(2^{|x+1|}\star m)$ and $2^{|x+1|} \overset{4.7(2)}{=} 2^{|2^{|x+1|}|}$, we get $v\star m \doteq \begin{bmatrix}v\\ m\end{bmatrix}$ by the direction ($\leftarrow$) of 4.10(5). Thus $x; v\star m \doteq \begin{bmatrix}(x+1)\star v\\ 2^{|x+1|}\star m\end{bmatrix}$ by (2). We now use 4.10(4) to get $t = x; v\star m$ from which we get $\exists x \exists s\, t = x; s$.

(5): By way of contradiction assume that $Adj(x;t) = 0$ then, since $((x+1)\star 2^{|x+1|}) \boxplus t = x;t$ from the definition, we get a contradiction as follows:

$$0 \overset{5.3(5)}{=} Adj((x{+}1)\star 2^{|x+1|}) \overset{5.2(5)}{=} (x{+}1)\star 2^{|x+1|} \overset{4.8(1)}{=} (x{+}1)\cdot 2^{|2^{|x+1|}|} + 2^{|x+1|} \overset{4.7(1)}{>} 0\,.$$

5.5 Towards the admissibility of pair induction. A very important property of dyadic lists is

$$\vdash_{\mathrm{PA}}\ x < x;t \land t < x;t\ . \tag{1}$$

Its proof requires the following monotone properties of dyadic concatenation:

$$\vdash_{\mathrm{PA}}\ x < y \to x\star z < y\star z \tag{2}$$
$$\vdash_{\mathrm{PA}}\ x \le x\star y\ . \tag{3}$$

(2): Assume $x < y$ and obtain $x\star z \overset{4.8(1)}{=} x\cdot 2^{|z|} + z \overset{4.7(1)}{<} y\cdot 2^{|z|} + z \overset{4.8(1)}{=} y\star z$.
(3): $x \overset{4.7(1)}{\le} x\cdot 2^{|y|} \le x\cdot 2^{|y|} + y \overset{4.8(1)}{=} x\star y$.
(1): By 4.11(1) we have $t \doteq \begin{bmatrix}v\\ m\end{bmatrix}$ for some v and m and by 5.4(2) we get $x;t \doteq \begin{bmatrix}(x+1)\star v\\ 2^{|x+1|}\star m\end{bmatrix}$. Thus $t \overset{4.10(3)}{=} v\star m$ and $x;t \overset{4.10(3)}{=} (x+1)\star v\star(2^{|x+1|}\star m)$.

In order to prove $x < x;t$ we observe that $x;t \overset{4.8(6)}{=} (x+1)\star a$ where we abbreviate by $a = v\star(2^{|x+1|}\star m)$. We now get $x \overset{(3)}{\le} x\star a \overset{(2)}{<} (x+1)\star a = x;t$.

In order to prove $t < x;t$ we obtain

$$v \overset{4.8(5)}{=} 0\star v \overset{(2)}{<} (x+1)\star v \overset{(3)}{\le} (x+1)\star v\star 2^{|x+1|}\ .$$

Hence $t = v\star m \overset{(2)}{<} (x+1)\star v\star 2^{|x+1|}\star m \overset{4.8(6)}{=} x;t$.

We could now prove that the principle of *dyadic pair induction* is admissible:

$$\forall t(Adj(t) = 0 \to \phi[t]) \land \forall x \forall s(\phi[x] \land \phi[s] \to \phi[x;s])) \to \phi[t]\ .$$

We will not do this as we will instead use below complete induction together with the case analysis on dyadic lists 5.4(4).

5.6 Recurrences for dyadic list concatenation. We are now ready to prove the following recurrences for the dyadic list concatenation function:

$$\vdash_{\mathrm{PA}} \ Adj(s) = 0 \rightarrow s \boxplus t = t \tag{1}$$
$$\vdash_{\mathrm{PA}} \ (x;s) \boxplus t = x;(s \boxplus t)\ . \tag{2}$$

(1): Assume $Adj(s) = 0$. We have $Adj(s) \doteq \begin{bmatrix} v_1 \\ m_1 \end{bmatrix}$ and $t \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$ for some v_1, v_2, m_1, and m_2 by 4.11(1). Thus $s \boxplus t \doteq \begin{bmatrix} v_1 \star v_2 \\ m_1 \star m_2 \end{bmatrix}$ by 5.3(2). By 4.10(3) we have $0 = Adj(s) = v_1 \star m_1$ and a simple dyadic case analysis on m_1 gets $v_1 = m_1 = 0$. Hence $s \boxplus t \doteq \begin{bmatrix} v_2 \\ m_2 \end{bmatrix}$ by 4.8(5) and $t = s \boxplus t$ by 4.10(4).

(2): We have

$$(x;s) \boxplus t \overset{\text{def ;}}{=} ((x+1) \star 2^{|x+1|}) \boxplus s \boxplus t \overset{5.3(4)}{=} ((x+1) \star 2^{|x+1|}) \boxplus (s \boxplus t) \overset{\text{def ;}}{=} x;(s \boxplus t)\ .$$

5.7 Tails of dyadic lists. We now introduce into PA the two-place predicate $s \sqsubseteq t$ holding when s is the *tail* of a dyadic list t. The predicate has the following explicit definition:

$$\vdash_{\mathrm{PAx}} \ s \sqsubseteq t \leftrightarrow \exists u\, u \boxplus s = t\ . \tag{1}$$

with the properties:

$$\vdash_{\mathrm{PA}} \ s \sqsubseteq s \tag{2}$$
$$\vdash_{\mathrm{PA}} \ t \sqsubseteq s \wedge s \sqsubseteq r \rightarrow t \sqsubseteq r \tag{3}$$
$$\vdash_{\mathrm{PA}} \ Adj(s) = 0 \rightarrow t \sqsubseteq s \leftrightarrow t = s \tag{4}$$
$$\vdash_{\mathrm{PA}} \ t \sqsubseteq x;s \leftrightarrow t = x;s \vee t \sqsubseteq s\ . \tag{5}$$

(2): We have $0 \boxplus s$ by properties 5.2(4) and 5.6(1). Hence 0 witnesses $s \sqsubseteq s$.

(3): From the assumptions we have $u \boxplus t = s$ and $w \boxplus s = r$ for some u, w by the definition. Thus $(w \boxplus u) \boxplus t \overset{5.3(4)}{=} w \boxplus (u \boxplus t) = w \boxplus s = r$ and so $w \boxplus u$ witnesses $t \sqsubseteq r$.

(4): Assume $Adj(s) = 0$ and in the direction $(\rightarrow)$ also $t \sqsubseteq s$, i.e. $u \boxplus t = s$ for some u. We get $Adj(u) = 0$ from 5.3(5) and $t = s$ from 5.6(1). In the direction $(\leftarrow)$ we use (2).

(5): In the direction $(\rightarrow)$ assume $t \sqsubseteq x;s$, i.e. $u \boxplus t = x;s$ for some u and consider two cases by 5.4(4). If $Adj(u) = 0$ then $t = x;s$ by 5.6(1). If $u = y;w$ for some y and w then we get $y;(w \boxplus t) = x;s$ by 5.6(2), $w \boxplus t = s$ by 5.4(3), and hence $t \sqsubseteq s$ from the definition.

In the direction $(\leftarrow)$ we first assume $t = x;s$ and get $t \sqsubseteq x;s$ by (2). We then assume $t \sqsubseteq s$, i.e. $u \boxplus t = s$ for some u. We have $(x;u) \boxplus t \overset{5.6(2)}{=} x;(u \boxplus t) = x;s$ and so $x;u$ witnesses $t \sqsubseteq x;s$.

5.8 Membership in dyadic lists. We now introduce into PA the two-place predicate $x \varepsilon t$ of *membership in dyadic lists*:

$$\vdash_{\mathrm{PAx}} x \varepsilon t \leftrightarrow \exists s\, x; s \sqsubseteq t \tag{1}$$

with the properties:

$$\vdash_{\mathrm{PA}} x \varepsilon x; s \tag{2}$$
$$\vdash_{\mathrm{PA}} x \varepsilon s \rightarrow x \varepsilon s \boxplus t \wedge x \in t \boxplus s \;. \tag{3}$$

(2): We have $x; s \sqsubseteq x; s$ by 5.7(2). We now use the definition of membership.

(3): From $x \varepsilon s$ we get $x; u \sqsubseteq s$ for some u by the definition of membership and $w \boxplus (x; u) = s$ for some w by the definition of tails. We have

$$w \boxplus (x; (u \boxplus t)) \overset{5.6(2)}{=} w \boxplus ((x; u) \boxplus t) \overset{5.3(4)}{=} (w \boxplus (x; u)) \boxplus t = s \boxplus t \;.$$

Hence $x; (u \boxplus t) \sqsubseteq s \boxplus t$ and then $x \varepsilon s \boxplus t$ by the definitions of tails and membership. We also have $(t \boxplus w) \boxplus (x; u) \overset{5.3(4)}{=} t \boxplus (w \boxplus (x; u)) = t \boxplus s$ and so $x \varepsilon t \boxplus s$ similarly as above.

6 Closure of PA under a Schema of Nested Iteration

We will see in Sect. 7 that we can introduce into PA functions and predicates satisfying recursive clauses of CL provided that we can show PA to be closed under a *schema of nested iteration* presented in Par. 6.1.

6.1 Schema of nested iteration. Suppose that a three-place function g, unary **measure** function μ, and a constant C giving a **recursion count** have been introduced into PA such that

$$\vdash_{\mathrm{PA}} g(x, n, a) = v\mathbf{1} \rightarrow \mu(v) < \mu(x) \tag{1}$$
$$\vdash_{\mathrm{PA}} \exists v\, g(x, 0, a) = v\mathbf{0} \;. \tag{2}$$

We then wish to introduce into PA a three-place **nested iteration** function g^* such that:

$$\vdash_{\mathrm{PA}} g^*(x, n, a) = v \leftarrow g(x, n, a) = v\mathbf{0} \tag{3}$$
$$\vdash_{\mathrm{PA}} g^*(x, n, a) = y \leftarrow g(x, n, a) = v\mathbf{1} \wedge n = m + 1 \wedge$$
$$g^*(v, C, 0) = w \wedge g^*(x, m, a \boxplus (w; 0)) = y \;. \tag{4}$$

Note that the measure of this recursion is $\mu(x){\cdot}C + n$ because we have $\mu(x){\cdot}C + n > \mu(x){\cdot}C + m$ for the second (outer) recursive call and $\mu(x){\cdot}C + n \overset{(1),(2)}{>} (\mu(v) + 1){\cdot}C = \mu(v){\cdot}C + C$ for the first (inner) recursive call.

The remainder of this section will be devoted to extensions by definitions of PA culminating in the introduction of the function g^* and in the proofs of recurrences (3) and (4) in Par. 6.5. The development will be under the assumption that g, μ, and C have been introduced into PA such that (1) and (2) hold.

6.2 Example: Fibonacci sequence. UNFINISHED: (this was explained in the class).

$F_0 = F_1 = 1$ and $F_{x+2} = F_x + F_{x+1}$. For this **explicitly** define $C = 2$, $\mu(x) = x$, and

$$g(x,n,a) = \begin{cases} (x \dot{-} 2)\mathbf{1} & \text{if } x \geq 2 \wedge n = 2 \\ (x \dot{-} 1)\mathbf{1} & \text{if } x \geq 2 \wedge n = 1 \wedge a = v;b \\ (v+w)\mathbf{0} & \text{if } x \geq 2 \wedge a = v;w;b \\ 1\mathbf{0} & \text{otherwise} \end{cases}$$

Since PA proves $2 \mid g(x,0,a)$ and $g(x,n,a) = v\mathbf{1} \rightarrow v < x$ we can use the schema of iteration and explicitly define $F_x = g^*(x,C,0)$ and prove in PA the **recurrences** for F.

6.3 Arithmetization of computation trees. The example from the preceding paragraph shows that computation trees for the nested iteration function g^* consist of two kinds of nodes:

$$\frac{g^*(\underline{x},\underline{n},\underline{a}) = \underline{y}}{0 \mid 0} \qquad \text{if } g(x,n,a) = y\mathbf{0}$$

$$\frac{g^*(\underline{x},\underline{n+1},\underline{a}) = \underline{y}}{g^*(\underline{v},C,0) = \underline{w} \mid g^*(\underline{x},\underline{n},\underline{a \boxplus (w;0)}) = \underline{y}} \quad \text{if } g(x,n+1,a) = v\mathbf{1}\ .$$

The two 'rules' for the construction of computation trees give *local conditions* which must be satisfied at every node of a computation tree.

We will *arithmetize* (encode into natural numbers) the symbolic identities $g^*(x,n,a) = y$ as $Lb(x,n,a,y)$ where the four-place function $Lb(x,n,a,y) = x;n;a;y$ yields the code of the identity as the *label* in a node of a computation tree We will abbreviate $Lb(x,n,a,y)$ to $(\mathbf{g}^*(x,n,a){=}^\bullet y)$. We will *flatten* the computation trees into lists containing the labels $(\mathbf{g}^*(x,n,a){=}^\bullet y)$ as elements in such a way that if the list s codes a computation tree then for every its tail $(\mathbf{g}^*(x,n,a){=}^\bullet y);t \sqsubseteq s$ either $g(n,x,a) = y\mathbf{0}$ or $g(n,x,a)$ is odd and the list t contains the labels of sons of the node $(\mathbf{g}^*(x,n,a){=}^\bullet y)$.

We are thus led to the introduction of a five-place predicate *Lcond* arithmetizing the local conditions and of a unary predicate *Ct* holding of computation trees:

$$\begin{aligned} \vdash_{\text{PAx}}\ & Lcond(x,n,a,y,t) \leftrightarrow \exists v(g(x,n,a) = v\mathbf{0} \wedge v = y \vee \\ & \quad \exists m \exists w(g(x,n,a) = v\mathbf{1} \wedge n = m+1 \wedge \\ & \qquad (\mathbf{g}^*(v,C,0){=}^\bullet w)\ \varepsilon\ t \wedge (\mathbf{g}^*(x,m,a \boxplus (w;0)){=}^\bullet y)\ \varepsilon\ t)) && (1) \\ \vdash_{\text{PAx}}\ & Ct(s) \leftrightarrow \forall x \forall n \forall a \forall y \forall t((\mathbf{g}^*(x,n,a){=}^\bullet y);t \sqsubseteq s \rightarrow Lcond(x,n,a,y,t))\ . && (2) \end{aligned}$$

The predicate *Lcond* satisfies the following:

$$\vdash_{\text{PA}} Lcond(x,n,a,y,s) \rightarrow Lcond(x,n,a,y,s \boxplus t) \qquad (3)$$

(3): Assume $Lcond(x,n,a,y,s)$ and for some v we consider two cases by (1). If $g(x,n,a) = v\mathbf{0}$ and $v = y$ then $Lcond(x,n,a,y,s \boxplus t)$ by (1) again.

If $g(x,n,a) = v\mathbf{1}$, $n = m+1$, $(\mathbf{g}^*(v,C,0){=}^\bullet w)\ \varepsilon\ s$, and $(\mathbf{g}^*(x,m,a \boxplus (w;0)){=}^\bullet y)\ \varepsilon\ s$ for some m and w then we get $(\mathbf{g}^*(v,C,0){=}^\bullet w)\ \varepsilon\ s \boxplus t$, and $(\mathbf{g}^*(x,m,a \boxplus (w;0)){=}^\bullet y)\ \varepsilon\ s \boxplus t$ by two applications of 5.8(3). We now get $Lcond(x,n,a,y,s \boxplus t)$ by (1).

Tails of computation trees are computation trees again:

$$\vdash_{\mathrm{PA}}\ Ct(s) \wedge t \sqsubseteq s \to Ct(t)\ . \tag{4}$$

(4): Assume $Ct(s)$ and $t \sqsubseteq s$. We wish to prove $Ct(s)$ so we take any x, n, a, y, and u such that $(\mathbf{g}^*(x,n,a){=}^\bullet y); u \sqsubseteq t$. By 5.7(3) we have $(\mathbf{g}^*(x,n,a){=}^\bullet y); u \sqsubseteq s$ and from the definition of $Ct(s)$ we get the desired $Lcond(x,n,a,y,u)$.

The following properties give recurrent clauses for Ct:

$$\vdash_{\mathrm{PA}}\ Adj(s) = 0 \to Ct(s) \tag{5}$$

$$\vdash_{\mathrm{PA}}\ \forall x \forall n \forall a \forall y\, b \neq (\mathbf{g}^*(x,n,a){=}^\bullet y) \to Ct(b;s) \leftrightarrow Ct(s) \tag{6}$$

$$\vdash_{\mathrm{PA}}\ Ct((\mathbf{g}^*(x,n,a){=}^\bullet y);s) \leftrightarrow Lcond((x,n,a,y,s) \wedge Ct(s)\ . \tag{7}$$

(5): Assume $Adj(s) = 0$ and take any take any x, n, a, y, and t such that $(\mathbf{g}^*(x,n,a){=}^\bullet y); t \sqsubseteq s$. By 5.7(4) we have $(\mathbf{g}^*(x,n,a){=}^\bullet y); t = s$ contradicting 5.4(5). Hence $Lcond(x,n,a,y,t)$ holds trivially.

(6): Assume not $\forall x \forall n \forall a \forall y\, b \neq (\mathbf{g}^*(x,n,a){=}^\bullet y)$ and in the direction $(\to)$ also $Ct(b;s)$. We have $s \sqsubseteq s$ by 5.7(2) and $s \sqsubseteq b;s$ by 5.7(5). Hence $Ct(s)$ by (4).

In the direction $(\leftarrow)$ assume $Ct(s)$ and for the proof of $Ct(b;s)$ take any x, n, a, y, and t such that $(\mathbf{g}^*(x,n,a){=}^\bullet y); t \sqsubseteq b;s$. By 5.7(5) we consider two cases. If $(\mathbf{g}^*(x,n,a){=}^\bullet y); t = b;s$ then $(\mathbf{g}^*(x,n,a){=}^\bullet y) = b$ by 5.4(3) contradicting the assumption about b and so $Lcond(x,n,a,y,t)$ holds trivially. If $(\mathbf{g}^*(x,n,a){=}^\bullet y); t \sqsubseteq s$ we get $Lcond(x,n,a,y,t)$ from the definition of $Ct(s)$.

(7): In the direction $(\to)$ assume $Ct((\mathbf{g}^*(x,n,a){=}^\bullet y);s)$. By 5.7(2) we have $(\mathbf{g}^*(x,n,a){=}^\bullet y);s \sqsubseteq (\mathbf{g}^*(x,n,a){=}^\bullet y);s$ and we get $Lcond(x,n,a,y,s)$ from (2). We also have $s \sqsubseteq s$ by 5.7(2) and $s \sqsubseteq (\mathbf{g}^*(x,n,a){=}^\bullet y);s$ by 5.7(5). Hence $Ct(s)$ by (4).

In the direction $(\leftarrow)$ assume $Lcond((x,n,a,y,s)$ and $Ct(s)$. For the proof of $Ct((\mathbf{g}^*(x,n,a){=}^\bullet y);s)$ take any take any x_1, n_1, a_1, y_1, and t such that $(\mathbf{g}^*(x_1,n_1,a_1){=}^\bullet y_1); t \sqsubseteq (\mathbf{g}^*(x,n,a){=}^\bullet y);s$. By 5.7(5) we consider two cases. If $(\mathbf{g}^*(x_1,n_1,a_1){=}^\bullet y_1); t = (\mathbf{g}^*(x,n,a){=}^\bullet y);s$ then $x_1 = x$, $n_1 = n$, $a_1 = a$, $y_1 = y$, and $t = s$ by several applications of 5.4(3) and so $Lcond(x_1,n_1,a_1,y_1,t_1)$ holds trivially. If $(\mathbf{g}^*(x_1,n_1,a_1){=}^\bullet y_1); t \sqsubseteq s$ we get $Lcond(x_1,n_1,a_1,y_1,t)$ from the definition of $Ct(s)$.

We will also need the following property:

$$\vdash_{\mathrm{PA}}\ Ct(s) \wedge Ct(t) \to Ct(s \boxplus t)\ . \tag{8}$$

(8): By complete induction on s. We assume $Ct(s)$ and by 5.4(4) we consider two cases. If $Adj(s) = 0$ then $Ct(s \boxplus t)$ holds by 5.6(1).

If $s = b;u$ from some b and u then, since $u < s$ by 5.5(1), we get $Ct(u \boxplus t)$ from IH. We also have $s \boxplus t \overset{5.6(2)}{=} b;(u \boxplus t)$ and we consider two cases. If $b \neq (\mathbf{g}^*(x,n,a) {=}^\bullet y)$ for all x, n, a, and y we get $Ct(b;(u \boxplus t))$ from (6). If $b = (\mathbf{g}^*(x,n,a) {=}^\bullet y)$ for some x, n, a, and y then, since $b;u \overset{5.7(2)}{\sqsubseteq} s$, we have $Lcond(x,n,a,y,u)$ from the definition of $Ct(s)$ and $Lcond(x,n,a,y,u \boxplus t)$ by (3). We now get $Ct(b;(u \boxplus t))$ from (7).

6.4 Introduction of graph of the nested iteration function into PA. We can now introduce into PA a four-place predicate $G\_gnit(x,n,a,y)$, abbreviated as $\mathbf{g}^*(x,n,a) \doteq y$, about which we will prove in Par. 6.5 that it is the graph of the nested iteration function g^*. The predicate is introduced as follows:

$$\vdash_{\text{PAx}} \mathbf{g}^*(x,n,a) \doteq y \leftrightarrow \exists t\, Ct((\mathbf{g}^*(x,n,a) {=}^\bullet y);t) \ . \tag{1}$$

We will need the following auxiliary property:

$$\vdash_{\text{PA}} Ct(s) \land (\mathbf{g}^*(x,n,a) {=}^\bullet y) \ \varepsilon \ s \rightarrow \mathbf{g}^*(x,n,a) \doteq y \tag{2}$$

which is proved by assumming $Ct(s)$ and $(\mathbf{g}^*(x,n,a) {=}^\bullet y) \ \varepsilon \ s$. From 5.8(1) we get $(\mathbf{g}^*(x,n,a) {=}^\bullet y);u \sqsubseteq s$ for some u and then $Ct((\mathbf{g}^*(x,n,a) {=}^\bullet y);u)$ from 6.3(4). We now use (1).

The predicate G_gnit satisfies following recurrences:

$$\vdash_{\text{PA}} g(x,n,a) = v\mathbf{0} \rightarrow \mathbf{g}^*(x,n,a) \doteq y \leftrightarrow y = v \tag{3}$$

$$\vdash_{\text{PA}} g(x,n+1,a) = v\mathbf{1} \rightarrow \mathbf{g}^*(x,n+1,a) \doteq y \leftrightarrow$$
$$\exists w (\mathbf{g}^*(v,C,0) \doteq w \land \mathbf{g}^*(x,n,a \boxplus (w;0)) \doteq y) \ . \tag{4}$$

(3): Assume $g(x,n,a) = v\mathbf{0}$ and in the direction $(\rightarrow)$ also $\mathbf{g}^*(x,n,a) \doteq y$. Hence $Ct((\mathbf{g}^*(x,n,a) {=}^\bullet y);t)$ for some t by (1) and $Lcond(x,n,a,y,t)$ by 6.3(7). We now obtain $y = v$ from 6.3(1).

In the direction $(\leftarrow)$ we wish to get $\mathbf{g}^*(x,n,a) \doteq v$. Towards that end we get $Lcond(x,n,a,v,0)$ from 6.3(1). Since $Adj(0)$ by 5.2(4) and $Ct(0)$ by 6.3(5), we get $Ct((\mathbf{g}^*(x,n,a) {=}^\bullet v);0)$ from 6.3(7) and $\mathbf{g}^*(x,n,a) \doteq v$ by (1).

(4): Assume $g(x,n+1,a) = v\mathbf{1}$ and in the direction $(\rightarrow)$ also $\mathbf{g}^*(x,n+1,a) \doteq y$. Thus $Ct((\mathbf{g}^*(x,n+1,a) {=}^\bullet y);s)$ for some s by (1). We use 6.3(7) to get $Lcond(x,n+1,a,y,s)$ and $Ct(s)$. By 6.3(1) we get $(\mathbf{g}^*(v,C,0) {=}^\bullet w) \ \varepsilon \ s$ and $(\mathbf{g}^*(x,n,a \boxplus (w;0)) {=}^\bullet y) \ \varepsilon \ s$ for some w. We now use (2) twice to get the desired conclusion.

In the direction $(\leftarrow)$ take any y and for some w assume $\mathbf{g}^*(v,C,0) \doteq w$ and $\mathbf{g}^*(x,n,a \boxplus (w;0)) \doteq y$. By a two-fold use of (1) we get $Ct((\mathbf{g}^*(v,C,0) {=}^\bullet w);s)$ and $Ct((\mathbf{g}^*(x,n,a \boxplus (w;0)) {=}^\bullet y);t)$ for some s, and t . By 6.3(8) we get $Ct(u)$ where we abbreviate $((\mathbf{g}^*(v,C,0) {=}^\bullet w);s) \boxplus ((\mathbf{g}^*(x,n,a \boxplus (w;0)) {=}^\bullet y);t)$ by u. Using both 5.8(2) and 5.8(3) yields $(\mathbf{g}^*(v,C,0) {=}^\bullet w) \ \varepsilon \ u$ and $(\mathbf{g}^*(x,n,a \boxplus (w;0)) {=}^\bullet y) \ \varepsilon \ u$. Since now $Lcond(x,n{+}1,a,y,u)$ by 6.3(1), we obtain $Ct((\mathbf{g}^*(x,n{+}1,a) {=}^\bullet y),u)$ by 6.3(7) and then $\mathbf{g}^*(x,n+1,a) \doteq y$ by (1).

6.5 Introduction of the nested iteration function into PA. The predicate G_gnit defined in Par. 6.4 is the graph of a function because it satisfies the following existence and uniqueness conditions:

$$\vdash_{\text{PA}} \exists y\, \mathbf{g}^*(x,n,a) \doteq y \tag{1}$$

$$\vdash_{\text{PA}} \mathbf{g}^*(x,n,a) \doteq y_1 \wedge \mathbf{g}^*(x,n,a) \doteq y_2 \rightarrow y_1 = y_2\ . \tag{2}$$

(1): By measure induction with the measure $\mu(x){\cdot}C + n$ and with the induction formula $\forall a(1)$. We take any a and consider two cases by 4.3(3). If $g(x,n,a) = v\mathbf{0}$ for some v we get $\mathbf{g}^*(x,n,a) \doteq v$ from 6.4(3). The goal is thus witnessed by v. If $g(x,n,a) = v\mathbf{1}$ for some v then $\mu(v) < \mu(x)$ by 6.1(1) and $n \neq 0$ by 6.1(2). Thus $n = m+1$ and $\mu(v)+d+1 = \mu(x)$ for some m and d. Since then $\mu(v){\cdot}C+C = (\mu(v)+1){\cdot}C < \mu(x){\cdot}C+m+1$ and $\mu(x){\cdot}C+m < \mu(x){\cdot}C+m+1$, we apply IH twice to get $\mathbf{g}^*(v,C,0) \doteq y$ for some w and then $\mathbf{g}^*(x,m,a \boxplus (w;0)) \doteq y$ for some y. Applying 6.4(4) now yields $\mathbf{g}^*(x,n,a) \doteq y$. The goal is thus witnessed by y.

(2): By measure induction with the measure $\mu(x){\cdot}C + n$ and with the induction formula $\forall a \forall y_1 \forall y_2(1)$. We take any a, y_1, y_2, assume $\mathbf{g}^*(x,n,a) \doteq y_1$, $\mathbf{g}^*(x,n,a) \doteq y_2$ and consider two cases by 4.3(3). If $g(x,n,a) = v\mathbf{0}$ for some v then $y_1 \overset{6.4(3)}{=} v \overset{6.4(3)}{=} y_2$. If $g(x,n,a) = v\mathbf{1}$ for some v then $\mu(v) < \mu(x)$ by 6.1(1) and $n \neq 0$ by 6.1(2). Thus $n = m+1$ and $\mu(v)+d+1 = \mu(x)$ for some m and d. We obtain $\mathbf{g}^*(v,C,0) \doteq w_1$ and $\mathbf{g}^*(x,m,a \boxplus (w_1;0)) \doteq y_1$ for some w_1 by 6.4(4). We similarly get $\mathbf{g}^*(v,C,0) \doteq w_2$ and $\mathbf{g}^*(x,m,a \boxplus (w_2;0)) \doteq y_2$ for some w_2. Since then $\mu(v){\cdot}C + C = (\mu(v)+1){\cdot}C < \mu(x){\cdot}C + m + 1$, we get $w_1 = w_2$ from IH. Since also and $\mu(x){\cdot}C + m < \mu(x){\cdot}C + m + 1$ we get $y_1 = y_2$ from another IH.

The property (1) is the existence condition for the introduction by minimization of the function g^*:

$$\vdash_{\text{PAx}} g^*(x,n,a) = \mu_y[\mathbf{g}^*(x,n,a) \doteq y] \tag{3}$$

We are now ready to prove the recurrences for g^* from Par. 6.1:

$$\vdash_{\text{PA}} g^*(x,n,a) = v \leftarrow g(x,n,a) = v\mathbf{0} \tag{4}$$

$$\vdash_{\text{PA}} g^*(x,n,a) = y \leftarrow g(x,n,a) = v\mathbf{1} \wedge n = m+1 \wedge$$
$$g^*(v,C,0) = w \wedge g^*(x,m,a \boxplus (w;0)) = y\ . \tag{5}$$

(4): Assume $g(x,n,a) = v\mathbf{0}$. Since $\mathbf{g}^*(x,n,a) \doteq g^*(x,n,a)$ by (3) and $\mathbf{g}^*(x,n,a) \doteq v$ by 6.4(3), we obtain $g^*(x,n,a) = v$ by (2).

(5): Assume $g(x,n,a) = v\mathbf{1}$, $n = m+1$, $g^*(v,C,0) = w$, and $g^*(x,m,a \boxplus (w;0)) = y$. We have $\mathbf{g}^*(v,C,0) \doteq g^*(v,C,0)$ by (3), $\mathbf{g}^*(x,m,a \boxplus (w;0)) \doteq g^*(x,m,a \boxplus (w;0))$ is obtained similarly. Using 6.4(4) then yields $\mathbf{g}^*(x,n,a) \doteq y$ and, since $\mathbf{g}^*(x,n,a) \doteq g^*(x,n,a)$ by (3), we have $g^*(x,n,a) = y$ by (2).

7 Clausal Definitions

UNFINISHED: (see the slides).