A Note on the Exponential Relation in Peano Arithmetic

Paul J. Voda
Institute of Informatics, Comenius University Bratislava,
Mlynská dolina, 842 15 Bratislava, Slovakia,
email: voda@fmph.uniba.sk
homepage: www.fmph.uniba.sk/∼voda

December 1998

The development of Peano arithmetic or of μ-recursive functions proceeds smoothly once the graph of the exponentiation function $2^x = y$ is defined as a Σ_1-predicate because one can code finite sequences as digits of 2^k-ary representation of numbers. Gödel did the development with the help of his β-function using the Chinese remainder theorem (see [Sho67]). A slightly simpler development is possible via p-adic concatenation (p is a prime) as suggested by Kripke (see [BJ80]). Smullyan in [Smu92] uses an idea of Quine and derives $2^x = y$ as a Σ_1-predicate by a detour through the general relation $x^y = z$. He poses as a problem a direct definition of $2^x = y$.

That the relation $x^y = z$ is even a Σ_0-predicate was proved by Bennett [Ben62]. For a formal proof of this in the fragment $I\Sigma_0$ of Peano arithmetic see [HP93]. All approaches require an auxiliary pairing function and in $I\Sigma_0$ also difficult estimates of quantifier bounds.

We present a simple derivation of the relation $2^x = y$ as a Σ_0-predicate which extends to $p^x = y$ for any prime p in a straightforward way. The derivation is based on elementary facts about binary representation of numbers without any recourse to pairing, p-adic concatenation, or β functions. We think that we have largely succeeded in supressing the metamathematical character of the coding by expressing it in purely arithmetical terms. Our derivation easily formalizes in $I\Sigma_0$-arithmetic.

0.1 Σ_0-predicates. Σ_0-predicates are defined by formulas constructed from 0, 1, $+$, $\cdot$, $=$, propositional connectives, and bounded quantifiers. The last are $\exists x{\le}\tau\,\phi$ and $\forall x{\le}\tau\,\phi$ where τ is a term. We permit also sharp bounds in quantifiers, for instance, $\exists x{<}\tau\,\phi$ as abbreviation for $\exists x{\le}\tau\,(x \neq \tau \wedge \phi)$.

0.2 Some Σ_0-predicates. The predicate $x \mid y$ of *divisibility* holding if x divides y is a Σ_0-predicate by:

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

The relation $<$ is Σ_0 by:

$$x < y \leftrightarrow \exists z{\leq}y\, y = x + z + 1$$

Myhill was probably first to notice that a positive number x is a power of two, in symbols $\exists n\, x = 2^n$, iff all its divisors $d > 1$ are themselves divisible by 2. This is captured by the following Σ_0-definition of the predicate:

$$\exists n\, x = 2^n \leftrightarrow 0 < x \land \forall d{\leq}x\, (d \mid x \rightarrow d = 1 \lor 2 \mid d) \ .$$

0.3 Graph of exponentiation $2^x = y$ is a Σ_0-predicate. Consider the following derivation of the exponentiation function 2^x by recursion on notation:

$$\begin{aligned} 2^0 &= 1 \\ 2^{2\cdot x+0} &= (2^x)^2 \qquad\qquad \text{if } x > 0 \\ 2^{2\cdot x+1} &= 2{\cdot}(2^x)^2 \ . \end{aligned}$$

For a given x let us define the numbers $x_i = x \div 2^i$ for all $i = 0, 1, \ldots, l$ where 2^l is the smallest number such that $2^l > x$. Note that we have $x_0 = x$, $x_l = 0$, and for every $i < l$ we have $x_{i+1} = x_i \div 2$. The computation of 2^x goes through the recursive arguments x_0, x_1, $\ldots$, until for $x_l = 0$ we can compute $2^{x_l} = 1$ directly.

We first derive an auxiliary binary predicate $Prn(p, y)$ holding of the *predecessor p of y in recursion on notation*, i.e. such that for $y = 2^x$ we have $Prn(p, y)$ iff $p = 2^{x_j}$ for some $j \leq l$. The predicate can be introduced with the help of course of values sequences $y + s$ satisfying

$$\exists j\, (p = 2^{x_j} \land y + s = \sum_{i\leq j} 2^{x_i})$$

where $s < y$, the smallest power in the sum is $p = 2^{x_j}$, and for every two 'neighboring' powers $p_1 = 2^{x_i}$ and $p_2 = 2^{x_{i+1}}$ in the sum we have $p_1 = p_2^2$ or $p_1 = 2{\cdot}p_2^2$. This fact is used in the following Σ_0-derivation of the predicate Prn:

$$\begin{aligned} &Prn(p, y) \leftrightarrow p \geq 1 \land \exists n\, y = 2^n \land \exists s{<}y \forall p_1{\leq}y \forall a{<}y{+}s \forall b{<}p_1\, (\\ &\quad \exists n\, p_1 = 2^n \land y + s = a{\cdot}2{\cdot}p_1 + p_1 + b \rightarrow p_1 = p \land b = 0 \lor \\ &\qquad p_1 > p \land \exists p_2{\leq}b \exists c{<}p_2\, (b = p_2 + c \land (p_1 = p_2{\cdot}p_2 \lor p_1 = 2{\cdot}p_2{\cdot}p_2)))\ . \end{aligned}$$

With the help of Prn we can 'store' and recover the recursive arguments x_i needed in the computation of $y = 2^x$ in a course of values sequence: $x{\cdot}y + s = \sum_{i\leq l} x_i{\cdot}2^{x_i}$ with $s < y$. Every argument in the sequence $x{\cdot}y + s$ can be located at some power p for which $Prn(p, y)$ holds. The arguments x_i cannot run into each other because $x_i < 2^{x_i}$ and the next higher bit set in $x{\cdot}y + s$ cannot come sooner than at the power $(2^{x_i})^2$ and so we have space for at least x_i bits. Of course, we do not know which argument x_i is at a power p but we know the relation between the arguments at two neighboring powers. This leads to a Σ_0-derivation of the graph of exponentiation:

$$
\begin{aligned}
2^x = y \leftrightarrow x < y \wedge \exists n\, y = 2^n \wedge \exists s{<}y \forall p{\le}y \forall a{\le}x{\cdot}y{+}s \forall b{<}p \forall c{<}p\, (\\
\quad Prn(p,y) \wedge x{\cdot}y + s = a{\cdot}p{\cdot}p + b{\cdot}p + c \rightarrow p = 1 \wedge b = 0 \vee p > 1 \wedge \\
\quad\quad \exists q{<}p \exists d{<}q \exists e{<}q\, (c = d{\cdot}q + e \wedge (\, p = q{\cdot}q \wedge b = 2{\cdot}d \vee \\
p = 2{\cdot}q{\cdot}q \wedge b = 2{\cdot}d + 1)))\ .
\end{aligned}
$$

References

[Ben62] J. H. Bennett. *On Spectra.* Ph.D. dissertation. Princeton, 1962.

[BJ80] G. Boolos, R. Jeffrey. *Computability and Logic.* Cambridge Univ. Press, 1980.

[HP93] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic.* Springer Verlag, 1993.

[Sho67] J. R. Shoenfield. *Mathematical Logic.* Addison-Wesley, 1967.

[Smu92] R. M. Smullyan. *Gödel's Incompleteness Theorem.* Oxford University Press, 1992.