Bulletin of the **S**ection of **L**ogic
Volume 8/3 (1979), pp. 148–152

reedition 2010 [original edition, pp. 148–153]

László Csirmaz

ON DEFINABILITY IN PEANO ARITHMETIC

We give here a rigorous proof of the existence of a Peano-definable coding function in the Peano-arithmetic (with + and · only). This is a well-known result among the logicians but we could not find it in the literature. This answers the question of Andréka and Németi [1] whether the axiom of the existence of a coding function should be added to PA in the proof of the completeness of Floyd Logic.

The letters, with or without indices, small and capital ones denote variables and all the formulas below belong to the set of the classical first order formulas of type t, where t is the similarity type of arithmetic, i.e. it consists of "$+, \cdot, 0, 1$" with arities "$2, 2, 0, 0$". PA denotes the following (infinite) set of axioms:

$P1$ $x + 1 \neq 0$
$P2$ $x + 1 = y + 1 \ \leftrightarrow \ x = y$
$P3$ $x + 0 = x$
$P4$ $x + (y + 1) = (x + y) + 1$
$P5$ $x \cdot 0 = 0$
$P6$ $x \cdot (y + 1) = (x \cdot y) + x$
$P7$ for all formulas φ of PA with x as free variable

$$[\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(x + 1))] \rightarrow \forall x \varphi(x).$$

$P7$ is the axiom of induction, φ may contain free variables other than x, which are parameters [2]. We will use other function and relation symbols as abbreviations without mentioning them, as e.g. $x < y$, $x \geqq y$, $x|y$ (x is a divisor of y) or $rem(x, y)$ (the remainder when x is divided by y). We

introduce the bounded quantifiers $(\forall x < y)\varphi(x) \leftrightarrow \forall x(x < y \rightarrow \varphi(x))$, etc. too.

One can easily prove from PA the following formulas:

$$x + y = y + x,\ (x + y) + z = x + (y + z),\ x \cdot y = y \cdot x,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

i.e. that the edition and the multiplication are commutative and associative;
that they are distributive;
that if $y > 0$ then the remainder $rem(x, y)$ exists and is unique (by induction on x);
that the subtraction has all its usual properties;
that the relation $<$ is a linear ordering (i.e. is transitive antisymmetric, irreflexive and trichotom) and
that any actual instance of the following theorem is valid (substituting $\varphi(x)$ in $P7$ by $(\forall y < x)\varphi(y)$)

$$P8\ [(\forall y < x)\varphi(y) \rightarrow \varphi(x)] \rightarrow \forall x\varphi(x).$$

The positive numbers x and y are relatively primes if they have no common divisior other than 1:

$$(x, y) = 1\ \leftrightarrow\ x > 0 \wedge y > 0 \wedge \forall z(z|x \wedge z|y\ \rightarrow\ z = 1).$$

LEMMA 1. $PA \vdash (x, y) = 1\ \rightarrow\ \exists u, v(x \cdot u - y \cdot v = 1)$.

PROOF. We will use induction of type $P8$ on $x + y$. First if $x + y \leqq 2$ then $(x, y) = 1$ implies $x = y = 1$ and in this case $x \cdot 2 - y \cdot 1 = 1$. If $x + y > 2$ then either $x > y$ or $x > y$. If $x > y$ then $(x - y, y) = 1$, $(x - y) + y < x + y$ so, by the induction hypothesis, $\exists u, v$ such that $(x - y) \cdot u - y \cdot v = 1$, i.e. $x \cdot u - y \cdot (u + v) = 1$. The case $x < y$ is similar. □

LEMMA 2. $PA \vdash (y, x) = 1 \wedge (z, x) = 1\ \rightarrow\ (y \cdot z, x) = 1$.

PROOF. By the previous lemma, there are u, v, w, t such that

$$y \cdot u = 1 + x \cdot v \qquad z \cdot w = 1 + x \cdot t.$$

Multiplying these equations we get

$$(y \cdot z) \cdot (u \cdot w) = 1 + x \cdot (v + t + v \cdot t).$$

If d is a common divisor of $y \cdot z$ and x then $d|l$. It is easy to check that it means $d = 1$. □

LEMMA 3. $PA \vdash x > y \wedge (x-y)|z \ \rightarrow \ (1+x\cdot z, 1+y\cdot z) = 1$.

PROOF. If d is a common divisor of $1+x\cdot z$ and $1+y\cdot z$ then d is a divisor of $x\cdot(1+x\cdot z) - y\cdot(1+x\cdot z) = x-y$, so d is a divisor of z. Then $d|(1+x\cdot z) - x\cdot z = 1$, i.e. $d=1$. □

LEMMA 4. $PA \vdash z > t \wedge (y,z) = 1 \ \rightarrow \ \forall x \exists u[rem(x+u\cdot y, z) = t]$.

PROOF. We distinguish three cases. If $x = t$, put simply $u = z$. If $x < t$ then, by Lemma 1, there are u_1, v_1 such that $y\cdot u_1 - z\cdot v_1 = 1$. Put $u = u_1\cdot(t-x)$, $v = v_1\cdot(t-x)$, then

$$x + u\cdot y = t + v\cdot z.$$

as required. The case $x > t$ is similar. □

THEOREM. $PA \vdash \forall m,b,n,z,x > 0 \ \exists M,B,C$

(i) $\{(\forall i < n)((i+1)|B) \wedge x|B \wedge$
(ii) $(\forall i \leqq n)(1+(i+1)\cdot B|C) \wedge$
(iii) $(\forall i > n)[(\forall j < i)(j+1|B) \rightarrow (1+(i+1)\cdot B, C) = 1] \wedge$
(iv) $(\forall i < n)[rem(m, 1+(i+1)\cdot b) = rem(M, 1+(i+1)\cdot B)] \wedge$
(v) $rem(M, 1+(n+1)\cdot B) = z\}$.

PROOF. Denote this formula by $\varphi(n)$, the proof will go by induction on n. First, we have to prove $\varphi(0)$, i.e. we are given the values of m, b, z and x and we look for M, B, and C. Let

$$M = z, B = x\cdot(z+1) \text{ and } C = 1+B.$$

For (i), (ii) and (iv) there is nothing to prove. For (v) observe that $1+B > z$ (because $x > 0$) so $rem(z, 1+B) = z$. For (iii) use Lemma 3:

$$PA \vdash i+1 > 1 \wedge i|B \ \rightarrow \ (1+(i+1)\cdot B, 1+B) = 1.$$

What has remained is to prove $\varphi(n) \rightarrow \varphi(n+1)$ from PA. Instead of this we will prove $\varphi(n+1)$ from $PA \cup \{\varphi(n)\}$. To avoid confusion of variables of the two instances of φ, we use asterisk to indicate the variables of $\varphi(n)$. Again, we are given the values of m, b, z and x and we look for M, B and C. First we use $\varphi(n)$ with the cast

This is a correct cast because $x^* > 0$. By $\varphi(n)$, we get M^*, B^*, C^* satisfying (i)* – (v)*, in particular, combining (iv)* and (v)*

(vi) $(\forall i < n+1)[rem(m, 1+(i+1)\cdot b) = rem(M^*, 1+(i+1)\cdot B^*)]$.

Let $B = B^*$ and $C = (1+(n+2)\cdot B)\cdot C^*$. (i) of $\varphi(n+1)$ is satisfied because of (i)* (of $\varphi(n)$) and the definition of x^*. As for (ii), $1+(i+1)\cdot B$ is a factor of C^* for $i \leqq n$, and $1+(n+2)\cdot B$ is a factor of C.

To prove (iii), if $i > n+1$ and $(\forall j < i)(j+1|B)$ then by (iii)*, $(1+(i+1)\cdot B, C^*) = 1$. We know, however, that $(i+1)-(n+2)|B$, so, by Lemma 3,

$$(1+(i+1)\cdot B, 1+(n+2)\cdot B) = 1.$$

Combining these equations as in Lemma 2, we get (iii).

From (i) we know that $(\forall j < n+1)(j+1|B)$, i.e. from (iii)* we get $(1+(n+2)\cdot B^*, C^*) = 1$. On the other hand $(1+(n+2)\cdot B^*) > B^* \geqq x^* > z$ so we can use Lemma 4 and get $M = M^* + u\cdot C^*$ for which $rem(M, 1+(n+2)\cdot B) = z$. This means that (v) is fulfilled.

As for (iv), we remark that $1+(i+1)\cdot B$ is a divisor of C^* for every $i \leqq n$ so $rem(M, 1+(i+1)\cdot B) = rem(M^*, 1+(i+1)\cdot B) = rem(m, 1+(i+1)\cdot b)$ by (vi). □

Corollary 1. $PA \vdash \forall m, b, n, z \exists M, B$
$\{(\forall i < n)[rem(m, 1+(i+1)\cdot b) = rem(M, 1+(i+1)\cdot B)] \wedge$
$rem(M, 1+(n+1)\cdot B) = z\}$. □

Define an ordered pair $\langle x, y\rangle$ as $(x+y)^2 + x$ and let $pair(z)$ be the following formulas with the only free variable z

$$\forall u(u\cdot u \leqq z \wedge (u+1)\cdot(u+1) > z \;\rightarrow\; z - u\cdot u \leqq u).$$

One can easily prove in PA that $pair(\langle x, y\rangle)$ and

$$pair(z) \;\rightarrow\; \exists! x \exists! y(z = \langle x, y\rangle).$$

(here "$\exists!$" means that there exists exactly one.) Let more the triplet $\langle x, y, z\rangle = \langle x, \langle y, z\rangle\rangle$ and define the formula seq and the functions $length$ and $elem$ as follows.

$$seq(u) = pair(u) \wedge \forall x \forall v(z = \langle x, v\rangle \rightarrow pair(v)),$$
$$length(u) = \begin{cases} n \text{ if } seq(u) \wedge u = \langle x, y, n\rangle \\ 0 \text{ otherwise} \end{cases}$$

$$elem(u,i) = \begin{cases} rem(m, 1+(i+1)\cdot b) \text{ if } seq(u) \wedge u = \langle m,b,n\rangle \wedge i < n \\ 0 \text{ otherwise.} \end{cases}$$

A straightforward proof shows that
$PA \vdash \forall u \exists! x(x = length(u))$
$PA \vdash \forall u \forall i \exists! x(x = elem(u,i))$.
From Corollary 1 we get

COROLLARY 2. $PA \vdash \forall u \forall z \exists v(seq(u) \rightarrow$
$\{seq(v) \wedge length(v) = length(u) + 1 \wedge$
$(\forall i < length(u))(elem(u,i) = elem(v,i)) \wedge$
$elem(v, length(u)) = z\})$. □

From Corollary 2 it follows immediately that every primitive recursive function f is PA-definable, i.e. there exists a formula φ_f of PA for which $PA \vdash \forall x \exists! y \varphi_f(x,y)$ and $PA \vdash$ "the function defined by φ_f satisfies the defining schemata of f".

References

[1] H. Anfréka and I. Németi, *Completeness of Floyd Logic*, **Bull. of Section of Logic** 7 (1978), pp. 115–121.

[2] C. C. Chang and H. J. Keisler, **Model Theory**, North Holland, 1973.

Mathematical Institute of the
Hungarian Academy of Sciences