Representing recursive (computable) functions in PA

Chinese remainder theorem (Sun Tzu [300 AD])

Theorem. Let $n_0, \ldots, n_{k-1}$ be pairwise coprime. $[\forall i \neq j. \gcd(n_i, n_j) = 1]$
Then for every sequence $x_0, \ldots, x_{k-1}$ there exists an a such that

$$\begin{aligned} a &\equiv x_0 \pmod{n_0} \\ &\ldots \\ a &\equiv x_{k-1} \pmod{n_{k-1}} \end{aligned}$$

[E.g. let $\vec{n} = \langle 3, 4, 5 \rangle$ and $\vec{a} = \langle 2, 3, 1 \rangle$. Then we can take $a = 191$.]

Proof. Define $N = n_0 n_1 \ldots n_{k-1}$ and $N_i = N/n_i$.

Note that $\gcd(n_i, N_i) = 1$. By Bézout there are p_i, q_i such that

$$q_i N_i = p_i n_i + 1$$

Define $e_i = q_i N_i$. Then $e_i \equiv 1 \pmod{n_i}$ and $e_i \equiv 0 \pmod{n_j}$ for $i \neq j$

Then take ('as in linear algebra')

$$a = \Sigma_{n=0}^{k-1} x_i e_i. \blacksquare$$

Coding sequences

Given $x_0, \ldots, x_{k-1}$ we want to code this as one number

As we do not know yet how to describe recursive functions in PA

our previous coding $\langle x_0, \ldots, x_{k-1} \rangle$ will not do

Define $m = \max(x_0, \ldots, x_{k-1}, k)!$ and $n_i = m(i+1)+1$

Then the $n_0, \ldots, n_{k-1}$ are mutually coprime

By the Chinese remainder theorem one has for some a

$$\forall i{<}k . a \equiv x_i \pmod{n_i}$$

Every number y can be written in a unique way as $y = \langle a, m \rangle$

Define Gödel's beta function $\beta(y, i) = (y)_i = rm(a, m(i+1)+1)$.
Theorem (i) PA $\vdash \forall x \exists y . y_0 = x$

(ii) PA $\vdash \forall x, y, k \exists y^1 [\forall i{<}k . y^1_i = y_i] \;\wedge\; y^1_k = x \quad [y^1 = x : y]$

(iii) PA $\vdash \forall a, m, i . [(\langle a, m \rangle)_i < a]$

Representing relations in PA

Definition. (i) Let $A \subseteq \mathbb{N}^k$. Then $\varphi = \varphi(x_1, \ldots, x_k)$ *represents* A if for all $n_1, \ldots, n_k \in \mathbb{N}^k$ one has

$$\begin{aligned} \vec{n} \in A \quad &\Rightarrow \quad \mathsf{PA} \vdash \varphi(\underline{n}_1, \ldots, \underline{n}_k) \\ \vec{n} \notin A \quad &\Rightarrow \quad \mathsf{PA} \vdash \neg\varphi(\underline{n}_1, \ldots, \underline{n}_k) \end{aligned}$$

where $\underline{0} = 0$, $\underline{n+1} = S(\underline{n})$

(ii) Let $F : \mathbb{N}^k \to \mathbb{N}$. Then $\varphi = \varphi(\vec{x}, y)$ represents f if it represents the graph of f:

$$\begin{aligned} f(\vec{n}) = m \quad &\Rightarrow \quad \mathsf{PA} \vdash \varphi(\underline{\vec{n}}, \underline{m}) \\ f(\vec{n}) \neq m \quad &\Rightarrow \quad \mathsf{PA} \vdash \neg\varphi(\underline{\vec{n}}, \underline{m}) \end{aligned}$$

Σ_1-formulae

Definition. Let φ be a formula of PA.

(i) φ is called a *Δ_0-formula* if all quantifiers in φ are *bounded* i.e. of the form $\forall x{<}t.\psi$ or $\exists x{<}t.\psi$, with $x \notin \mathrm{FV}(t)$

(ii) $\varphi = \varphi(\vec{x})$ is called a *Σ_1-formula* if there is a Δ_0-formula ψ s.t.

$$\text{PA} \vdash \varphi(\vec{x}) \;\leftrightarrow\; \exists \vec{y}.\psi(\vec{x}, \vec{y})$$

(iii) A relation $R \subseteq \mathbb{N}^k$ is called Σ_1 or Δ_0 if R is representable by respectively a Σ_1 or Δ_0 formula

Using the β-function

Lemma. Define $R(x, d, r) \Leftrightarrow r$ is the remainder after dividing x by d

Then R is Δ_0.

Proof. Indeed, R is represented by

$$\varphi(x, d, r) \equiv \exists q{<}(x + 1).x = qd + r. \blacksquare$$

Lemma. The relation $\beta(x, i) = y$ is Δ_0.

Proof. This is because

$$\beta(x, i) = y \;\Leftrightarrow\; \exists a{<}x, m{<}x.\langle a, m\rangle = x \;\wedge\; R(a, m(i + 1) + 1, y),$$

while $\langle a, m\rangle = x \;\Leftrightarrow\; 2x = (a + m)(a + m + 1) + 2a. \blacksquare$

Lemma. (i) PA $\vdash \forall x{<}t\exists y.\psi(x, y) \rightarrow \exists y\forall x{<}t\exists u{<}y.\psi(x, u)$

(ii) Σ_1 formulae are closed under $\forall x{<}t$ and $\exists x{<}t$ and even $\exists y$

Provably recursive functions

Definition. A function $F : \mathbb{N}^k \longrightarrow \mathbb{N}$ is *provably recursive* if there it is represented by a Σ_1-formula $\varphi(\vec{x}, z)$ such that

$$\mathsf{PA} \vdash \forall \vec{x}\, \exists ! z . \varphi(\vec{x}, z)$$

Recursive functions are Σ_1-representable

Theorem *Every total recursive function is Σ_1-representable in* PA

Proof. For the initial functions this is easy. The Σ_1-representable functions are closed under substitution. To show that they are closed under primitive recursion, consider e.g.

$$\begin{aligned} f(x,0) &= n \\ f(x,k+1) &= g(f(x,k),x,k) \end{aligned}$$

We may suppose that g is represented by the Σ_1-formula ψ_g. Then $f(x,y) = z$ iff there exists a sequence $x_0,\ldots,x_{k-1}$ such that

$$\forall i{\leq}y . x_i = f(x,i) \ \wedge \ x_y = z.$$

This is equivalent to

$$x_0 = n \ \wedge \ \forall i{<}k . \varphi_g(x_i,x,i,x_{i+1}) \ \wedge \ x_k = z.$$

All this can be expressed via the β-function.

Primitive recursive functions are provably total

Theorem *Every primitive recursive function is provably recursive in PA*

[But not all recursive funcions are provably recursive functions!]