The Definability of the P.R. Functions in $\mathfrak{N}$

Robert Rynasiewicz
Mathematical Logic II

Spring 2022

Definability of Functions

Defn. Recall that an $n+1$-ary relation R is definable in $\mathfrak{N}$ iff there is a wff $\rho(v_0, \ldots, v_n)$ s.t. for all $k_0, \ldots, k_n \in \mathbb{N}$

$$\langle k_0, \ldots, k_n \rangle \in R \quad \text{iff} \quad \models_{\mathfrak{N}} \rho(v_0, \ldots, v_n) \, [\![k_0, \ldots, k_n]\!]$$

Defn. An n-ary function just is an $n+1$-ary relation of a particular type, and to say that a function is definable just is to say that it is definable as a relation.[1]

---

[1] Smith talks instead about expressibility in the language of arithmetic, but by the language of arithmetic, he means the *interpreted* language, i.e., the language together with the structure $\mathfrak{N}$. His definition of expressibility in the language of arithmetic coincides with our definition of definability in $\mathfrak{N}$.

Definability of the Base Functions

- The 0-ary zero function $\{k_0 \mid k_0 = 0\}$ is defined by the wff $v_0 = 0$.
- The successor function $\{\langle k_0, k_1\rangle \mid S(k_0) = k_1\}$ is defined by the wff $Sv_0 = v_1$.
- The mth n-ary projection function I^n_m as a relation is:

  $$\{\langle k_0, \ldots, k_{m-1}, \ldots, k_n\rangle \mid k_n = k_{m-1}\}$$

  and is defined by the wff

  $$((v_0 = v_0) \wedge \cdots \wedge (v_{m-1} = v_n) \wedge (v_{n-1} = v_{n-1})).$$

Definability of the Base Functions (cont.)

For example,

$$\begin{aligned} I^3_2 &= \{\langle k_0, k_1, k_2, k_3\rangle \mid k_3 = k_1\} \\ &= \{\langle k_0, k_1, k_2, k_3\rangle \mid k_3 = I^3_2(k_0, k_1, k_2)\} \end{aligned}$$

is defined by

$$((v_0 = v_0) \wedge (v_1 = v_3) \wedge (v_2 = v_2)).$$

Definability of the Composition of Functions

Composition of Functions of One Variable.

$$\begin{array}{rcl} f = h \circ g & = & \{\langle x, z\rangle \mid z = h(g(x))\} \\ & = & \{\langle x, z\rangle \mid \exists y(g(x) = y \wedge h(y) = z)\} \\ & = & \{\langle x, z\rangle \mid \exists y(\langle x, y\rangle \in g \wedge \langle y, z\rangle \in h)\} \end{array}$$

If $\gamma(v_0, v_1)$ defines g in $\mathfrak{N}$ and $\eta(v_0, v_1)$ defines h in $\mathfrak{N}$, then

$$\exists y(\gamma(v_0, y) \wedge \eta(y, v_1))$$

defines $f = h \circ g$ in $\mathfrak{N}$.

N.B. This works even if f, g, and h are relations that are not functions.

Definability of the Composition of Functions (cont.)

Composition of Functions of Several Variables. Before stating the solution for the general case, consider a particular example where

$$f(x) = h(g_1(x), g_2(x)).$$

Then f, as a set of ordered pairs, is just

$$f = \{\langle x, z\rangle \mid \exists y_1 \exists y_2 (g_1(x) = y_1 \wedge g_2(x) = y_2 \wedge h(y_1, y_2) = z)\}.$$

So, if

- $\gamma_1(v_0, v_1)$ defines g_1,
- $\gamma_2(v_0, v_1)$ defines g_2, and
- $\eta(v_0, v_1, v_2)$ defines h,

then f is defined by:

$$\exists y_1 \exists y_2 (\gamma_1(v_0, y_1) \wedge \gamma_2(v_0, y_2) \wedge \eta(y_1, y_2, v_1)).$$

Definability of the Composition of Functions (cont.)

Composition of Functions of Several Variables. Suppose

$$f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_k(\vec{x})),$$

where $\vec{x} = (x_1, \ldots, x_n)$. Then

$$f = \{\langle \vec{x}, z \rangle \mid \exists y_1 \cdots \exists y_k (g_1(\vec{x}) = y_1 \wedge \cdots \wedge g_k(\vec{x}) = y_k \wedge h(y_1, \ldots, y_k) = z)\}.$$

So, if $\gamma_1(\vec{v}, v_n), \ldots, \gamma_k(\vec{v}, v_n)$ define $g_1, \ldots, g_k$ and η defines h, where $\vec{v} = (v_0, \ldots, v_{n-1})$, then

$$\exists y_1 \cdots \exists y_k (\gamma_1(\vec{v}, y_1) \wedge \cdots \wedge \gamma_k(\vec{v}, y_k) \wedge \eta(\vec{y}, v_n))$$

defines f, where $\vec{y} = (y_1, \ldots, y_k)$.

Heuristics for Defining a Primitive Recursive Function

Consider a simple case such as the factorial function $f(n) = n!$ which, recall, was defined by recursion:

$$\begin{aligned} f(0) &= 1 \\ f(S(n)) &= f(n) \cdot S(n). \end{aligned}$$

The idea behind defining in $\mathfrak{N}$ the factorial function (and primitive recursion in general) is to existentially quantify over the whole sequence of intermediate values. For factorial, we have: $\langle n, m \rangle \in f$ just in case there exist numbers $k_0, \ldots, k_n$ s.t.

- $k_0 = 1$,
- for all $j < n$, $k_{S(j)} = k_j \cdot S(j)$, and
- $k_n = m$.

Heuristics for Defining a Primitive Recursive FunctionI(cont.)

However, in the object language we don't have wffs that quantify over indices. So, we need some sort of trick for encoding a finite sequence of numbers uniquely as a natural number. So, e.g., for the sequence of numbers $k_0, \ldots, k_n$, let

$$c = \pi_0^{k_0} \cdot \pi_1^{k_1} \cdots \pi_n^{k_n}.$$

Then we have a p.r. function *exf* s.t. $exf(c, i) = k_i$ for each $i \leq n$, thus allowing us to "decode" c into the sequence $k_0, \ldots, k_n$.

The Idea of a β-Function

Defn. A 2-place β-function is a function $\beta(c, i)$ such that for any sequence of numbers $k_0, \ldots, k_n$, and for each $i \leq n$, there is a number c s.t. $\beta(c, i) = k_i$.

Example. $exf(c, i)$ from before. However, we can't use this directly since exponentiation isn't a primitive in the language of Peano arithmetic and we were able to define it only by using primitive recursion. So, we need:

Defn. A 3-place β-function is a function $\beta(c, d, i)$ such that for any sequence of numbers $k_0, \ldots, k_n$, and for each $i \leq n$, there exists a pair of numbers c, d s.t. $\beta(c, d, i) = k_i$.

Excursion into Number Theory

To secure such a β we need to engage in a bit of number theory. Let $rm(c, d)$ be the remainder of dividing c by d, i.e., $rm(c, d) = c \bmod d$.

Lemma. Suppose x and y are relatively prime. Then there exists a $b < y$ s.t. $rm(bx, y) = 1$.

Proof. Suppose that x and y are relatively prime. Suppose also that $b_1 < b_2 < y$ and $rm(b_1x, y) = rm(b_2x, y)$. Then, $\exists c_1, c_2$ s.t. for some d:

$$\begin{aligned} b_1x &= c_1y + d \\ b_2x &= c_2y + d. \end{aligned}$$

Excursion into Number Theory (cont.)

Thus, subtracting the first equation from the 2nd,

$$\frac{(b_2 - b_1)x}{y} = c_2 - c_1,$$

where, of course, $c_2 - c_1$ is a whole number. Since $b_2 - b_1 < y$, y must factorize into $y = y_1 \cdot y_2$ s.t.

- $y_1 \mid (b_2 - b_1)$,
- $y_2 \mid x$, *but*
- $y_2 \neq 1$.

Thus x and y have the common factor y_2, violating the assumption that x and y are relatively prime.

Excursion into Number Theory (cont.)

Thus, for any $b_1, b_2 < y$, $rm(b_1x, y) \neq rm(b_2x, y)$. Hence there are is a 1-1 correspondence between the b's less than y and the remainders of bx/y. Consequently, one of the remainders must be 1. ■

This lemma is useful in proving an ancient theorem.

The Chinese Remainder Theorem

Chinese Remainder Theorem. Suppose that $m_0, \ldots, m_n$ are pairwise relatively prime and $k_0, \ldots, k_n$ are s.t. $k_i \leq m_i$ for all $i \leq n$. Then there is a number c s.t. $k_i = rm(c, m_i)$ for all $i \leq n$.

Proof. For each i, let M_i be the product of all the m_j, $j \neq i$. Since m_i is prime relative to each of the m_j's, m_i and M_i are relatively prime. Now, for each i, there exists a $b_i < m_i$ s.t. $rm(b_i M_i, m_i) = 1$. For each i, choose such a b_i. Let

$$c = \sum_{i=0}^{n} k_i b_i M_i.$$

The Chinese Remainder Theorem (cont.)

Since, for $i \neq j$, m_i divides M_j exactly,

$$\begin{aligned}
rm(c, m_i) &= rm\left(\sum_{i=0}^{n} k_i b_i M_i, m_i\right) \\
&= rm(k_i b_i M_i, m_i) + \sum_{j \neq i} rm(k_j b_j M_j, m_i) \\
&= rm(k_i b_i M_i, m_i) + 0 \\
&= rm(k_i b_i M_i, m_i).
\end{aligned}$$

Now

$$\frac{k_i b_i M_i}{m_i} = k_i(a + \frac{1}{m_i}) = k_i a + \frac{k_i}{m_i}$$

for some $a \in \mathbb{N}$. Hence, since $k_i \leq m_i$, it follows that $rm(c, m_i) = k_i$. This leads to our main result ...

Gödel's β-Function Lemma

Gödel's β-Function Lemma. For any sequence of numbers $k_0, \ldots, k_n$, there exist numbers c and d s.t. $rm(c, d(i+1)+1) = k_i$.

Proof. The strategy is to choose d so that for different values of i the terms $d(i+1)+1$ are relatively prime and then to apply the Chinese Remainder Theorem. Let u be the maximum of the sequence $k_0, \ldots, k_n, n+1$, and let $d = u!$, i.e.,

$$d = \max\{k_0, \ldots, k_n, n+1\}!.$$

Contrary to what we want to show, suppose that, for some pair of distinct $i, j \leq n$, some prime p divides both $d(i+1)+1$ and $d(j+1)+1$. Let $a = i+1$ and $b = j+1$, and w/o loss of generality suppose that $a < b$.

Gödel's β-Function Lemma (cont.)

Then there exists ℓ, m such that

$$\begin{aligned} \ell p &= da + 1 \\ mp &= db + 1. \end{aligned}$$

Hence

$$(m - \ell)p = (b - a)d.$$

- But since $b - a \leq n + 1$, $b - a$ is a factor of $d = \max\{k_0, \ldots, k_n, n + 1\}!$.
- Thus p divides d.
- Then p is not a divisor of $da + 1$ or $db + 1$, contrary to supposition. ■

The Gödel β-Function.

Def. $\beta(c, d, i) =_{df} rm(c, d(i+1)+1)$ is the *Gödel β-function*.

β has the property that for any sequence of numbers $k_0, \ldots, k_n$, there exists numbers c and d s.t. $\beta(c, d, i) = k_i$ for all $i \leq n$.
Now it's easy to define β in $\mathfrak{N}$. In the **metalanguage** we have that $\beta(c, d, i) = k_i$ iff

$$\exists x[(c = x \cdot (d(i+1)+1) + k_i) \wedge (k_i \leq d \cdot (i+1))].$$

So, let $B(v_0, v_1, v_2, v_3)$ be the **object language** wff

$$(\exists x \leq v_0)((v_0 = x \cdot S(v_1 \cdot Sv_2) + v_3) \wedge (v_3 \leq v_1 \cdot Sv_2)).$$

Then B defines β in $\mathfrak{N}$.[2]

---

[2] Note, by the way, that B is Δ_0.

Defining Factorial with the β-Function

We began the investigation into defining primitive recursion in $\mathfrak{N}$ by noting that for the factorial function f defined recursively:

$\langle n, m\rangle \in f$ iff there exist numbers $k_0, \ldots, k_n$ s.t.

- $k_0 = 1$,
- *for all* $j < n$, $k_{S(j)} = k_j \cdot S(j)$, *and*
- $k_n = m$.

Using the β function, we can replace quantification over indices of a sequence of length n with quantification over a pair of numbers c, d:

$\langle n, m\rangle \in f$ iff there exist numbers c, d s.t.

- $\beta(c, d, 0) = 1$,
- *for all* $j < n$, $\beta(c, d, S(j)) = \beta(c, d, j) \cdot S(j)$, *and*
- $\beta(c, d, n) = m$.

Defining Factorial with the β-Function (cont.)

In order to define factorial f in $\mathfrak{N}$, we cast this in the object language. Call the resulting formula $F(v_0, v_1)$. Using periods for conjunction and double colons with indenting to indicate the scope of quantifiers, here is $F(v_0, v_1)$:

$\exists x \exists y$::

- $B(x, y, 0, 1)$.
- $(\forall z < v_0)\exists u \exists v$::
  - $B(x, y, Sz, u)$.
  - $u = v \cdot Sz$.
  - $B(x, y, z, v)$.
- $B(x, y, v_0, v_1)$

Taking on the General Case

Recall the general form of primitive recursion:

$$\begin{aligned} f(\vec{x}, 0) &= g(\vec{x}) \\ f(\vec{x}, S(n)) &= h(\vec{x}, n, f(\vec{x}, n)) \end{aligned}$$

Following the pattern we did with factorial, this can be re-expressed:

$\langle \vec{x}, n, m \rangle \in f$ iff there exists a sequence $k_0, \ldots, k_n$ s.t.

- $k_0 = g(\vec{x})$,
- for all $j < n$, $k_{S(j)} = h(\vec{x}, j, k_j)$, and
- $k_n = m$.

Taking on the General Case (cont.)

Using the β-function, this becomes:

$\langle \vec{x}, n, m \rangle \in f$ iff there exist numbers c, d s.t.

- $\beta(c, d, 0) = g(\vec{x})$,
- for all $j < n$, $\beta(c, d, S(j)) = h(\vec{x}, j, \beta(c, d, j))$, and
- $\beta(c, d, n) = m$.

Now suppose $G(\vec{v}, v_{n+1})$ defines g in $\mathfrak{N}$ and $H(\vec{v}, v_{n+1}, v_{n+2}, v_{n+3})$ defines h in $\mathfrak{N}$, where $\vec{v} = (v_0, \ldots, v_n)$. Then we can translate into the object language to get a wff $F(\vec{v}, v_{n+1}, v_{n+2})$ that defines f in $\mathfrak{N}$ as follows.

Taking on the General Case (cont.)

$\exists x \exists y$::

- $\exists z (B(x, y, 0, z) \wedge G(\vec{v}, z))$.
- $(\forall z < v_{n+1}) \exists u \exists v$::
  - $B(x, y, Sz, u)$.
  - $H(\vec{v}, z, v, u)$.
  - $B(x, y, z, v)$.
- $B(x, y, v_{n+1}, v_{n+2})$

Definability Theorem for P.R. Functions

Theorem. Any p.r. function is definable in $\mathfrak{N}$, in fact by a Σ_1 wff.

Pf. The set of p.r. functions is just the closure of the base set under composition and primitive recursion.

- 0, S, and the projection functions are all definable by Δ_0 wffs.
- Composition uses only existential quantification, so if $g_1, \ldots, g_k$ and h are all definable by Σ_1 wffs, then so is $h(g_1(\vec{x}), \ldots, g_k(\vec{x}))$.
- The β-function is definable by a Δ_0 wff. If f is defined from g and h by primitive recursion and g and h are definable by Σ_1 wffs, then so is f. ■

The Definability of P.R. Properties and Relations

Theorem. Any p.r. property or relation is definable in $\mathfrak{N}$ by a Σ_1 wff.

Pf. Recall that a p.r. property or relation is one whose characteristic function is p.r. If the characteristic function χ_R of an $(n+1)$-ary relation R is definable by the wff $\rho(v_0, \ldots, v_n, v_{n+1})$, then $\rho(v_0, \ldots, v_n, 1)$ defines R. ■