Representability

Let $f : \mathbb{N}^k \to \mathbb{N}$ be a function.
We say that <u>f is represented by the formula $F(x_1, \ldots, x_k, y) \in L_A$</u> if for all $n_1, \ldots, n_k \in \mathbb{N}$,

$$\mathcal{P} \vdash \forall y \left(F(\underline{n}_1, \ldots, \underline{n}_k, y) \leftrightarrow y = \underline{f(n_1, \ldots, n_k)} \right).$$

We say that f is <u>representable</u> if f is represented by some formula in L_A.

Let $R \subseteq \mathbb{N}^k$. We say that <u>R is represented by the formula $\varphi(x_1, \ldots, x_k)$</u> $\in L_A$ if for all $n_1, \ldots, n_k \in \mathbb{N}$:

(i) if $(n_1, \ldots, n_k) \in R$ then $\mathcal{P} \vdash \varphi(\underline{n}_1, \ldots, \underline{n}_k)$

(ii) if $(n_1, \ldots, n_k) \notin R$ then $\mathcal{P} \vdash \neg\varphi(\underline{n}_1, \ldots, \underline{n}_k)$

We say that R is representable if R is represented by some formula in L_A.

Proposition 2.1 Let $R \subseteq \mathbb{N}^k$.

Then R is representable if and only if its characteristic function C_R is representable.

Proof. If R is represented by $\varphi(x_1,\ldots,x_k)$ then C_R is represented by

$$(\varphi(x_1,\ldots,x_k) \wedge y=\underline{0}) \vee (\neg\varphi(x_1,\ldots,x_k) \wedge y=\underline{1}).$$

If C_R is represented by $F(x_1,\ldots,x_k,y)$ then R is represented by $F(x_1,\ldots,x_k,\underline{0})$.

(We need to use $\mathcal{P} \vdash \underline{0} \neq \underline{1}$, which follows from (29), to prove this) $\square$

Examples 2.2 It is easy to see that:

1. The zero function $z(n)=0$, for all $n\in\mathbb{N}$, is represented by the formula

$$x_1 = x_1 \wedge y = \underline{0}.$$

2. the successor function $s(n)=n+1$, for all $n\in\mathbb{N}$, is represented by the formula

$$s(x_1) = y$$

3. The projection function $P_i^k(n_1, \dots, n_k) = n_i$, for all $n_1, \dots, n_k \in \mathbb{N}$, is represented by

$$x_1 = x_1 \wedge x_2 = x_2 \wedge \dots \wedge x_k = x_k \wedge y = x_i$$

<u>Lemma 2.2</u> Suppose that $f(x_1, \dots, x_k)$ is defined from $g, h_1, \dots, h_m$ by substitution.
If $g, h_1, \dots, h_m$ are representable then f is representable.

Proof. Let g be represented by $G(x_1, \dots, x_m, y)$ and let h_i be represented by $H_i(x_1, \dots, x_k, y)$, for $1 \le i \le m$,
Then f is represented by

$$\exists z_1, \dots, z_m \Big[G(z_1, \dots, z_m, y) \wedge \bigwedge_{1 \le i \le m} H_i(x_1, \dots, x_k, z_i) \Big].$$

(exercise to show this!) □

<u>Lemma 2.3</u> Suppose that $f(x_1, \dots, x_k)$ is defined from $g(x_1, \dots, x_k, x_{k+1})$ by the μ-operator.
If g is representable then f is representable.

Proof. Let g be represented by $G(x_1, \dots, x_k, x_{k+1}, y)$
Let $F(x_1, \dots, x_k, y)$ be the following formula
$G(x_1, \dots, x_k, y, \underline{0}) \wedge \forall z (z < y \rightarrow \neg G(x_1, \dots, x_k, z, \underline{0}))$.

We show that F represents f.

Let $n_1, \dots, n_k \in \mathbb{N}$ and $f(n_1, \dots, n_k) = n$.

Then n is the least natural number such that $g(n_1, \dots, n_k, n) = 0$. Since g is represented by G, it follows that

(a) $\mathcal{P} \vdash G(\underline{n}_1, \dots, \underline{n}_k, \underline{n}, \underline{0})$

and for all $m \leq n-1$

(b) $\mathcal{P} \vdash \neg G(\underline{n}_1, \dots, \underline{n}_k, \underline{m}, \underline{0})$.

By (30) we get

(c) $\mathcal{P} \vdash y = \underline{n} \rightarrow F(\underline{n}_1, \dots, \underline{n}_k, y)$.

By (30),

(d) $\mathcal{P}, F(\underline{n}_1, \dots, \underline{n}_k, y), y < \underline{n} \vdash \bigvee_{1 \leq m \leq n-1} G(\underline{n}_1, \dots, \underline{n}_k, \underline{m}, \underline{0})$

and we also have

(e) $\mathcal{P}, F(\underline{n}_1, \dots, \underline{n}_k, y), \underline{n} < y \vdash \neg G(\underline{n}_1, \dots, \underline{n}_k, \underline{n}, \underline{0})$.

By (a), (b), (d) and (e) we get

$\mathcal{P} \vdash F(\underline{n}_1, \dots, \underline{n}_k, y) \rightarrow \neg y < \underline{n} \wedge \neg \underline{n} < y$

which by (20) gives

$\mathcal{P} \vdash F(\underline{n}_1, \dots, \underline{n}_k, y) \rightarrow y = \underline{n}$.

The last line and (c) shows that f is represented by F. $\square$

Chinese Remainder Theorem

If $m_1, m_2, \ldots, m_k \in \mathbb{N}^+$ are relatively prime and $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ then there exists a such that $a \equiv n_i \ (m_i)$ for $1 \le i \le k$.

Proof. Let $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ and let $l_i = \frac{m}{m_i}$.

If l_i and m_i are not relatively prime then there exists a prime p such that $p \mid l_i$ and $p \mid m_i$, but if $p \mid l_i$ then $p \mid m_j$ for some $j \neq i$, contradicting that m_i and m_j are relatively prime. Hence l_i and m_i are relatively prime for all $1 \le i \le k$. Hence there are r_i, s_i, $1 \le i \le k$ such that $r_i m_i + s_i l_i = 1$. Then $s_i l_i \equiv 1 \ (m_i)$ (because $s_i l_i = r_i m_i + 1$) and $s_i l_i \equiv 0 \ (m_j)$ for every $j \neq i$ (because $m_j \mid l_i$).

By the multiplication rule for congruences

$n_i s_i l_i \equiv n_i \ (m_i)$ and

$n_i s_i l_i \equiv 0 \ (m_j)$ for $i \neq j$

By the addition rule for congruences

$$\left(\sum_{i=1}^{k} n_i s_i l_i \right) \equiv n_i \ (m_i) \text{ for } 1 \le i \le k.$$

So if we let $a = \sum_{i=1}^{k} n_i s_i l_i$ then

$a \equiv n_i \ (m_i)$ for $1 \le i \le k$. $\square$

Define a function $\beta(x_1, x_2, x_3)$ by

$\beta(x_1, x_2, x_3) = rm(1+(x_3+1)\cdot x_2, x_1)$.

This function is called <u>Gödel's β-function</u>.

<u>Lemma 2.4</u> β is primitive recursive and representable.

Proof. β is primitive recursive by Proposition 1.3.

Let $B(x_1, x_2, x_3, y)$ be the formula

$\exists z\,[x_1 = (1+(x_3+1)\cdot x_2)\cdot z + y \wedge y < 1+(x_3+1)\cdot x_2]$.

Let $n_1, n_2, n_3 \in \mathbb{N}$ and let $r = \beta(n_1, n_2, n_3)$.

Then there is $q \in \mathbb{N}$ such that

$n_1 = (1+(n_3+1)\cdot n_2)\cdot q + r$ and $r < 1+(n_3+1)\cdot n_2$.

Let $m \in \mathbb{N}$ be such that $m + r = 1+(n_3+1)\cdot n_2$.

By (26), (27), (29) and the definition of $<$ we get

$P \vdash (\underline{1} + (\underline{n}_3 + \underline{1})\cdot \underline{n}_2)\cdot \underline{q} + \underline{r} \wedge \underline{r} < \underline{1} + (\underline{n}_3 + \underline{1})\cdot \underline{n}_2$

which gives

(a) $P \vdash y = \underline{r} \rightarrow B(\underline{n}_1, \underline{n}_2, \underline{n}_3, y)$.

Combining $P \vdash B(\underline{n}_1, \underline{n}_2, \underline{n}_3, \underline{r})$ and (32) gives

(b) $P \vdash B(\underline{n}_1, \underline{n}_2, \underline{n}_3, y) \rightarrow y = \underline{r}$,

Now (a) and (b) shows that β is represented by B $\square$

Lemma 2.5 For any sequence $n_0, n_1, \ldots, n_k \in \mathbb{N}$ there are $b, c \in \mathbb{N}$ such that $\beta(b,c,i) = n_i$ for $0 \leq i \leq k$.

Proof. Let $m = \max(k, n_0, n_1, \ldots, n_k)$ and let $c = m!$.

Claim: The numbers $u_i = 1 + (i+1) \cdot c$, $0 \leq i \leq k$ are relatively prime.

Proof of Claim. Suppose for a contradiction that some $p \neq 1$ divides u_i and u_j where $0 \leq i < j \leq k$. We may assume that p is prime. Then $p \mid (u_j - u_i) = (j-i) \cdot c$ so $p \mid (j-i)$ or $p \mid c$. Since $j - i \leq k \leq m$ it follows that $(j-i) \mid m! = c$ Hence, we must have $p \mid c$.
But then $p \mid (i+1) \cdot c$ and $p \mid 1 + (i+1) \cdot c$ so $p \mid 1 + (i+1) \cdot c - (i+1) \cdot c = 1$, which implies $p = 1$, a contradiction. Now the claim is proved.

By the Chinese Remainder Theorem there is a number b such that for every $0 \leq i \leq k$ $b \equiv n_i \ (u_i)$, and since $n_i < u_i$ we get $rm(u_i, b) = n_i$. By definition of β,

$$\beta(b,c,i) = rm(1 + (i+1) \cdot c, b) = rm(u_i, b) = n_i$$

$\square$

Lemma 2.6 Suppose that $f(x_1,\dots,x_k,x_{k+1})$ is defined by recursion from $g(x_1,\dots,x_k)$ and $h(x_1,\dots,x_k,x_{k+1},x_{k+2})$. If g and h are representable then f is representable.

Proof. Suppose that g is represented by $G(x_1,\dots,x_k,y)$ and h is represented by $H(x_1,\dots,x_k,x_{k+1},x_{k+2},y)$. Let $B(x_1,x_2,x_3,y)$ be a formula that represents β (by Lemma 2.4 such formula exists). Let $B'(x_1,x_2,x_3,y)$ be the formula

$$B(x_1,x_2,x_3,y) \wedge \forall z(z<y \rightarrow \neg B(x_1,x_2,x_3,z)).$$

Then B' represents β and from (20) it follows that

$$(\bullet)\quad P \vdash \forall x_1 x_2 x_3 y_1 y_2 \big(B'(x_1,x_2,x_3,y_1) \wedge B'(x_1,x_2,x_3,y_2) \rightarrow y_1 = y_2\big).$$

Since f is defined by recursion from g and h it follows (using Lemma 2.5) that:

$$(*)\quad \left\{\begin{array}{l} f(n_1,\dots,n_k)=m \text{ if and only if there are } b,c\in\mathbb{N} \\ \text{such that } \beta(b,c,0)=g(n_1,\dots,n_k) \text{ and} \\ \beta(b,c,i+1)=h(n_1,\dots,n_k,i,\beta(b,c,i)) \text{ for } 0\le i<n \\ \text{and } \beta(b,c,n)=m \text{ (so } \beta(b,c,i)=f(n_1,\dots,n_k,i) \\ \text{for } 0\le i\le n). \end{array}\right.$$

We express (*) by a formula F.
Let $F(x_1, \ldots, x_k, x_{k+1}, y)$ be

$$\exists uv\Big[\exists z\big[B'(u,v,\underline{0},z) \wedge G(x_1,\ldots,x_k,z)\big]$$
$$\wedge \forall z\big[z < x_{k+1} \to \exists z_1 z_2\big(B'(u,v,z,z_1) \wedge B'(u,v,S(z),z_2)$$
$$\wedge H(x_1,\ldots,x_k,z,z_1,z_2)\big)\big]$$
$$\wedge B'(u,v,x_{k+1},y)\Big].$$

Note that u, v corresponds to a, b in (*).
We will show that f is represented by F.

Suppose that $f(n_1, \ldots, n_k, n) = m$.
Then there are $b, c \in \mathbb{N}$ which satisfy the conditions in (*). Let $p = g(n_1, \ldots, n_k)$ and $r_i = \beta(b, c, i)$, for $0 \leq i \leq n$. Since g and β are represented by G and B' we get

(a) $\mathcal{P} \vdash B'(\underline{b}, \underline{c}, \underline{0}, \underline{p}) \wedge G(\underline{n}_1, \ldots, \underline{n}_k, \underline{p}) \wedge B'(\underline{b}, \underline{c}, \underline{n}, \underline{m})$

and (if $n > 0$)

(b) for all $0 \leq i < n$,

$$\mathcal{P} \vdash B'(\underline{b}, \underline{c}, \underline{i}, \underline{r}_i) \wedge B'(\underline{b}, \underline{c}, S(\underline{i}), \underline{r}_{i+1})$$
$$\wedge H(\underline{n}_1, \ldots, \underline{n}_k, \underline{i}, \underline{r}_i, \underline{r}_{i+1})$$

By (30) and (b) it follows that

(c) $\mathcal{P} \vdash \forall z \left[z < \underline{n} \to \exists z_1 z_2 \left(B'(\underline{b}, \underline{c}, z, z_1) \wedge B'(\underline{b}, \underline{c}, s(z), z_2) \wedge H(\underline{n}_1, \dots, \underline{n}_k, z, z_1, z_2) \right) \right]$

By (a) and (c) we get

(d) $\mathcal{P} \vdash F(\underline{n}_1, \dots, \underline{n}_k, \underline{n}, \underline{m})$, for all $n_1, \dots, n_k, n, m \in \mathbb{N}$ such that $f(n_1, \dots, n_k, n) = m$.

We will now show, by induction on n, that if $f(n_1, \dots, n_k) = m$ then

(e) $\mathcal{P} \vdash \forall y \left(F(\underline{n}_1, \dots, \underline{n}_k, \underline{n}, y) \to y = \underline{m} \right)$.

Then the theorem will follow from (d) and (e).

Base: Suppose that $f(n_1, \dots, n_k, 0) = m$. Then $m = g(n_1, \dots, n_k)$. From (•) and the assumption that g is represented by G it follows that

$\mathcal{P} \vdash \forall y \left(F(\underline{n}_1, \dots, \underline{n}_k, \underline{0}, y) \to y = \underline{m} \right)$.

Induction step: Suppose that $f(n_1, \dots, n_k, n) = \ell$, $f(n_1, \dots, n_k, n+1) = m$ and

(f) $\mathcal{P} \vdash \forall y \left(F(\underline{n}_1, \dots, \underline{n}_k, \underline{n}, y) \to y = \underline{\ell} \right)$.

We will now that we can formaly derive $y = \underline{m}$ from $\mathcal{P}$ and the hypotheses (g), (h) and (i) given below

(g) $\exists z [B'(u,v,\underline{0},z) \wedge G(\underline{n}_1,\dots,\underline{n}_k,z)]$

(h) $\forall z [z < \underline{n+1} \to \exists z_1 z_2 (B'(u,v,z,z_1) \wedge B'(u,v,s(z),z_2) \wedge H(\underline{n}_1,\dots,\underline{n}_k,z,z_1,z_2))]$

(i) $B'(u,v,\underline{n+1},y)$

From (h) we derive (using (17))

(j) $\forall z [z < \underline{n} \to \exists z_1 z_2 (B'(u,v,z,z_1) \wedge B'(u,v,s(z),z_2) \wedge H(\underline{n}_1,\dots,\underline{n}_k,z,z_1,z_2))]$

and

(k) $\exists z_1 z_2 (B'(u,v,\underline{n},z) \wedge B'(u,v,\underline{n+1},z_2) \wedge H(\underline{n}_1,\dots,\underline{n}_k,\underline{n},z_1,z_2))$.

If we add

(ℓ) $B'(u,v,\underline{n},z_1) \wedge B'(u,v,\underline{n+1},z_2) \wedge H(\underline{n}_1,\dots,\underline{n}_k,\underline{n},z_1,z_2)$

as a hypothesis then we can derive

$$F(\underline{n}_1,\dots,\underline{n}_k,\underline{n},z_1)$$

so by (f) we derive $z_1 = \underline{\ell}$, which (by (ℓ)) gives

$$H(\underline{n}_1,\dots,\underline{n}_k,\underline{n},\underline{\ell},z_2).$$

Since $m = f(n_1,\dots,n_k,n+1) = h(n_1,\dots,n_k,n,\ell)$ and h is represented by H we can derive $z_2 = \underline{m}$

which (by (ℓ)) gives $B'(u, v, \underline{n+1}, \underline{m})$, and by (i) and ($\bullet$) we get $y = \underline{m}$.

Since z_1 and z_2 do not occur free in (g), (h), (i) or $\mathcal{P}$ it follows that

$$\mathcal{P}, (g), (h), (i) \vdash y = \underline{m}$$

and since u and v do not occur free in $\mathcal{P}$ or $F(\underline{n}_1, \ldots, \underline{n}_k, \underline{n+1}, y)$ it follows that

$$\mathcal{P} \vdash F(\underline{n}_1, \ldots, \underline{n}_k, \underline{n+1}, y) \to y = \underline{m}.$$

The induction step is completed by introducing $\forall y$.

$\square$

Theorem 2.7 (Representation Theorem)
Every recursive function is representable.

Proof. In Examples 2.2 we showed that all initial functions are representable, so by the definition of recursive functions, Lemma 2.2, Lemma 2.3 and Lemma 2.6 the theorem follows. $\square$

Corollary 2.8 Every recursive relation is representable.

Proof. Let R be a recursive relation. Then its characteristic function C_R is recursive, and hence, by Theorem 2.7, representable. But then, by Proposition 2.1, R is representable. $\square$