Math Logic: Model Theory & Computability
Lecture 27

Recall that we call a relation $R \subseteq \mathbb{N}^k$ computable if $\mathbb{1}_R : \mathbb{N}^k \to \mathbb{N}$ is computable. We can also prove the converse (in some sense):

Graph property. A function $f: \mathbb{N}^k \to \mathbb{N}$ is computable iff its graph $G_f := \{(\vec{a}, b) \in \mathbb{N}^{k+1} : f(\vec{a}) = b\}$ is computable.

Proof. $\Rightarrow$: Suppose $f: \mathbb{N}^k \to \mathbb{N}$ is computable. Then for each $(\vec{a}, b) \in \mathbb{N}^{k+1}$,

$$(\vec{a}, b) \in G_f \text{ iff } f(\vec{a}) = b \text{ iff } f(P_1^{k+1}(\vec{a}, b), \dots, P_k^{k+1}(\vec{a}, b)) = P_{k+1}^{k+1}(\vec{a}, b)$$

so G_f is computable since $=$ is.

$\Leftarrow$. Suppose G_f is computable. Then $f(\vec{x}) := \mu_y\,(G_f(\vec{x}, y))$ is computable. □

We will show later that computable relations are not closed under quantifiers $\exists, \forall$. However:

Bounded quantification: The class of computable relations is closed under bounded quantification, i.e. for each computable relation $R \subseteq \mathbb{N}^k \times \mathbb{N}$, the relations $R_1, R_2 \subseteq \mathbb{N}^k \times \mathbb{N}$ defined by

$$R_1(\vec{x}, n) \;:\Leftrightarrow\; \exists y \le n \; R(\vec{x}, y)$$
$$R_2(\vec{x}, n) \;:\Leftrightarrow\; \forall y \le n \; R(\vec{x}, y)$$

are computable.

Proof. Since computable functions are closed under negation, it is enough to prove that R_1 is computable. For each $(\vec{a}, n) \in \mathbb{N}^{k+1}$,

$$R_1(\vec{a}, n) \;\Leftrightarrow\; \mu_x\,(R(\vec{a}, x) \vee x > n) \le n. \qquad \square$$

Prop. The following functions are computable:

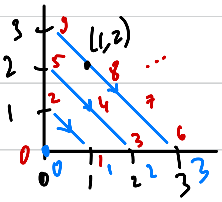
(a) Safe subtraction $\dot{-} : \mathbb{N}^2 \to \mathbb{N}$ defined by $(x,y) \mapsto \max\{0, x-y\}$.

(b) Division $: \mathbb{N}^2 \to \mathbb{N}$ defined by $(x,y) \mapsto \begin{cases} \lfloor \frac{x}{y} \rfloor & \text{if } y \neq 0 \\ 0 & \text{otherwise} \end{cases}$.

(c) Remainder $\text{Rem} : \mathbb{N}^2 \to \mathbb{N}$ defined by $(x,y) \mapsto \begin{cases} x - y \cdot \lfloor \frac{x}{y} \rfloor & \text{if } y \neq 0 \\ x & \text{if } y = 0 \end{cases}$.

(d) $\text{Pair} : \mathbb{N}^2 \to \mathbb{N}$ defined by

$$(x,y) \mapsto \underbrace{\frac{(x+y)(x+y+1)}{2}}_{\substack{\#\text{ of pairs on the diagonals before} \\ \text{the } (x+y)^{\text{th}} \text{ diagonal}}} + \underbrace{x}_{\substack{\text{the offset on the } (x+y)^{\text{th}} \\ \text{diagonal}}}.$$



(e) $\text{Left} : \mathbb{N} \to \mathbb{N}$ defined by $z \mapsto$ the unique x such that there is y such that $\text{Pair}(x,y) = z$.

$\text{Right} : \mathbb{N} \to \mathbb{N}$ defined by $z \mapsto$ the unique y such that there is x such that $\text{Pair}(x,y) = z$.

Proof. (a)–(c) is homework, (d) is clear, so we prove (e). Note that

$$\text{Left}(z) = \mu_x \left(\exists y \leq z \ \text{Pair}(x,y) = z \right)$$
$$\text{Right}(z) = \mu_y \left(\exists x \leq z \ \text{Pair}(x,y) = z \right).$$
$\square$

<u>Dedekind's analysis of recursion.</u> Suppose $f : \mathbb{N}^{k+1} \to \mathbb{N}$ is defined by primitive recursion from $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^{k+2} \to \mathbb{N}$, i.e. for all $(\vec{a}, n) \in \mathbb{N}^{k+1}$,

$$\begin{cases} f(\vec{a}, 0) = g(\vec{a}) \\ f(\vec{a}, n+1) = h(\vec{a}, n, f(\vec{a}, n)) \end{cases}.$$

Then for each $(\vec{a}, n) \in \mathbb{N}^{k+1}$ and $m \in \mathbb{N}$,

$$f(\vec{a}, n) = m \quad \text{iff} \quad \exists \vec{c} \in \mathbb{N}^{<\mathbb{N}} \ \text{lh}(\vec{c}) = n+1 \text{ and } c_0 = g(\vec{a}) \text{ and } c_n = m \text{ and } \forall i < n \ c_{i+1} = h(\vec{a}, i, c_i).$$

Proof. Follows by induction on i that $c_i = f(\vec{a}, i)$. $\square$

We will use Dedekind analysis to implement primitive recursion via successfull search, but for this we need to computable encode/decode tuples of natural numbers of arbitrary length. This is done by Gödel using:

Chinese Remainder Theorem. If $d_1, d_2, \ldots, d_n \in \mathbb{N}$ are pairwise coprime numbers > 1, then, putting $d := d_1 \cdot d_2 \cdot \ldots \cdot d_n$, the function $h : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$, $[a]_d \mapsto ([a]_{d_1}, [a]_{d_2}, \ldots, [a]_{d_n})$ is a well-defined group-isomorphism.

Proof. Well-definedness follows from the fact that if $a \equiv_d b$ then $a \equiv_{d_i} b$ for all i. That h is a group-homomorphism is because modding out respects addition. Because both groups $\mathbb{Z}/d\mathbb{Z}$ and $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n$ have d elements, it is enough to show (by the Pigeonhole Principle) that h is injective, for which we need to check that if $h([a]_d) = (0, 0, \ldots, 0)$ then $[a]_d = [0]_d$. Suppose $h([a]_d) = 0$, i.e. $[a]_{d_i} = [0]_{d_i}$ for all i, i.e. d_i divides a for all i. By the pairwise coprimeness of the d_i, $d = d_1 d_2 \cdots d_n$ divides a, so $[a]_d = [0]_d$. □

Gödel's β function. There is a computable function $\beta : \mathbb{N}^2 \to \mathbb{N}$, namely

$$\beta(w, i) := \mathrm{Rem}(\mathrm{Left}(w), 1 + (i+1)\,\mathrm{Right}(w))$$

such that for each $\vec{a} \in \mathbb{N}^{<\mathbb{N}}$ there is $w \in \mathbb{N}$ with $a_i = \beta(w, i)$ for all $i < \mathrm{lh}(\vec{a})$, where we write $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$.

Proof. Let $m := \max\{a_0, a_1, \ldots, a_n, n\}$ and put $d_i := 1 + (i+1)\cdot(m!)$ for each $i = 0, \ldots, n-1$. The d_i are pairwise coprime because for any $i \leq j < n$, if a prime p divides both d_i and d_j then p divides $d_j - d_i = (j-i)\cdot(m!)$. Since $(j-i) \mid m!$ if $j - i \neq 0$, we get that p divides $m!$, contradicting that $p \mid d_i = 1 + (i+1)(m!)$. Hence, $i = j$.
By the Chinese Remainder Theorem, there is $a < d$ such that $\mathrm{Rem}(a, d_i) = a_i$. Take $w := \mathrm{Pair}(a, m!)$, so $\mathrm{Rem}(\mathrm{Left}(w), 1 + (i+1)\,\mathrm{Right}(w)) = \mathrm{Rem}(a, 1 + (i+1)(m!)) = \mathrm{Rem}(a, d_i) = a_i$. □