# Coding sequences

We know (cf. the notes on $\Delta_0$-def functions) how to code $k$-tuples, any fixed $k \geq 2$. But we need to code finite seq's $a_0, \dots, a_{n-1}$ of arbitrary length $n$, i.e. $n$ is not known in advance.

For example, we could code it by

$$w := p_0^{1+a_0} p_1^{1+a_1} \cdot \ldots \cdot p_{n-1}^{1+a_{n-1}}$$

where $p_i$ is $(i+1)$-st prime. However, we need that the length function

$$len(w) = n$$

and the decoding

$$(w)_i := a_i$$

are $\Delta_0$-definable. To say "$q$ is $j$-th prime" in a $\Delta_0$-way is not easy and presupposes the ability to code sequences (first $j$ primes).

Fortunately Gödel (1931) invented in his proof a way how to do this. It uses the following number-theoretic statement.

# Chinese remainder theorem (~~~~300 B.C.)

Let $n \geq 0$, $m_0, \dots, m_{n-1} \geq 2$ and assume that all pairs $m_i, m_j$ for $i \neq j$, are coprime. Put $m := \prod_{i<n} m_i$.

Let $0 \leq a_i < m_i$, $i < n$, be arbitrary. Then there is $u < m$ s.t. for all $i < n$:

$$u \equiv a_i \pmod{m_i}$$

<u>Prf</u>: Put

$$D = \{0, \dots, m-1\}$$

$$R = \{0, \dots, m_0 - 1\} \times \dots \times \{0, \dots, m_{n-1} - 1\}$$

and define map $F : D \to R$ by

$$F(x) = (y_0, \dots, y_{n-1})$$

where $y_i = \mathrm{rem}(x, m_i)$ (cf. notes on $\Delta_0$-def fcn)

<u>Claim</u>: $F$ is 1-to-1 (i.e. injective).

Prf-claim: If not, then for some $0 \leq x < x' < m$

$$x \equiv x' \pmod{m_i}$$

i.e. $x' - x \equiv 0 \pmod{m_i}$. As $m_i$'s are coprime also $x' - x \equiv 0 \pmod{m}$. But $x' - x < m$, so $x = x'$. ↯

$\square_{\text{claim}}$.

The thm follows as $|D| = |R|$, so $F$ must be also surjective.

$\square_{\text{thm}}$.

Given $a_0, \ldots, a_{n-1}$ we will need to generate easily (i.e. $\Delta_0$-define) suitable $m_0, \ldots, m_{n-1}$.

Take:

$$d := (n!)(1 + \max_i a_i).$$

Clearly $a_i < d$, all $i$. Put:

$$m_i := (i+1) \cdot d + 1 .$$

__Claim:__ For $0 \leq i < j < n$, $m_i, m_j$ are coprime.

__Proof-claim__: Assume that $1 < p \mid m_i$ and $p \mid m_j$.

Then $p \mid (j-i)d$. As $j - i < n$, ~~also~~ and $n! \mid d$, also $p \mid d$. But that is impossible as $m_i \equiv 1 (d)$.

$\Box_{\text{claim}}$

__Gödel's $\beta$-function:__

$$\beta(x, y, z) := \operatorname{rem}(x, (z+1) \cdot y + 1).$$

Now we are ready to define the coding.

The code of sequence

$$a_0, \ldots, a_{n-1}$$

is

$$w := \langle m, d, n \rangle$$

where:

(a) $m := \prod_{i<n} m_i$, where $m_i := (i+1)\cdot d + 1$

(b) $d := (n!)(1 + \max_i a_i)$.

The $\Delta_0$-definitions of $\underline{len}(w)$ and $(w)_i$ are easy now:

$$len(w) = n \iff \exists u, v \leq w,\ w = \langle u, v, n \rangle$$

$$(w)_i = a \iff \exists u, v, n \leq w,\ w = \langle u, v, n \rangle \wedge a = rem(u, (i+1)\cdot v + 1).$$

//

<u>Summary:</u> For all sequences $a_0, \ldots, a_{n-1}$ there is $w$ s.t. $len(w) = n$ and for all $i < n$: $(w)_i = a_i$.

//