

Encoding Computations

We can represent a computation of M on an input as a sequence of configurations: every two consecutive integers are related by triple replacements, except for “padding” with blank (when the last digit is a state).

We encode a computation of M (on *empty* input) by juxtaposing consecutive configurations to form a single b -ary integer (followed by a 0, so that all configurations begin and end with a zero).

Lemma 1. *For each TM M we can construct a bounded expression $comp_M(x)$ in number theory satisfying the following: for all nonnegative integers n we have $N_{x=n} \models comp_M(x)$ iff the b -ary expansion of n is the juxtaposition of consecutive configurations of a halting computation of M , starting from the empty string.*

Details: Yields Relation

We express the “yields” relation $Y_M(m, n)$ as an expression in number theory.

$$yields_M(x, x') = pads_M(x, x') \vee$$

$$(\exists y < x)(\exists z_1 < x)(\exists z_2 < x)(\exists z'_2 < x)(\exists z_3 < x)(\exists z'_3 < x)(\exists z_4 < x)$$

$$(conf_M(x) \wedge conf_M(x'))$$

$$\wedge mod(x, b \uparrow y, z_1) \wedge div(x, b \uparrow y, z_2) \wedge mod(x', b \uparrow y, z_1) \wedge div(x', b \uparrow y, z'_2) \wedge$$

$$\wedge mod(z_2, b \uparrow 3, z_3) \wedge div(z_2, b \uparrow 3, z_4) \wedge mod(z'_2, b \uparrow 3, z'_3) \wedge div(z'_2, b \uparrow 3, z_4) \wedge localreplacement_M(z_3, z'_3)$$

$$pads_M(x, x') : (\forall y < x)(mod(x, b, y) \Rightarrow y \geq |\Sigma|) \wedge x' = x \times b + 1.$$

$$conf_M(x): \dots$$

$$localreplacement_M(x, y) : \forall_{a,b} \text{ are valid triples } (x = a_1 a_2 a_3 \wedge y = b_1 b_2 b_3)$$

Details: A whole computation

We can write an expression $comp_M(x)$ which states that x encodes a *halting computation* of M starting from the *empty string*:

1. Each configuration yields the next.
2. x starts with the 3 digits $0, |\Sigma|, 0$.
3. x ends with the two digits $|\Sigma| + 1, 0$ (“yes”) or $|\Sigma| + 2, 0$ (“no”).

Can be written as a bounded expression.

Undecidability and Incompleteness of Number Theory

Theorem 1. *The set of unsatisfiable sentences and the set of sentences provable from NT are recursively inseparable.*

Corollary 1. *The following problems are undecidable, given a sentence ϕ :*

(a) *Is ϕ VALID?*

(b) *Does $N \models \phi$?*

(c) *Does $NT \vdash \phi$?*

Corollary 2. [Godel's Incompleteness Theorem] *There is no recursively enumerable set of axioms Δ such that, for all expressions ϕ , $\Delta \vdash \phi$ iff $N \models \phi$.*