Incompleteness Theorem

Gödel's Incompleteness Theorem Any sound proof system for $Th(\mathbb{N}, 0, 1, +, \times, <)$ is incomplete i.e. $\exists$ sentences φ s.t.

$$(\mathbb{N}, 0, 1, +, \times, <) \models \varphi$$

and φ does not have a proof.

Gödel's (Alternate) Incompleteness Theorem

$Th(\mathbb{N}, 0, 1, +, \times, <)$ is not recursively enumerable.

Proof $HP = \{\langle M, w\rangle \mid M \text{ halts on } w\}$

$\overline{HP} = \{\langle M, w\rangle \mid M \text{ doesn't halt on } w\}$

is not recursively enumerable.

To show $\overline{HP} \leq_m Th(\mathbb{N}, 0, 1, +, \times, <)$

Given $\langle M, w\rangle$, we construct sentence $NotHalt_{\langle M, w\rangle}$ s.t.

$\langle M, w\rangle \in \overline{HP}$ iff $NotHalt_{\langle M, w\rangle} \in Th(\mathbb{N}, 0, 1, +, \times, <)$.

Without loss of generality, assume

- M is TM with only one read/write

tape. (There are no work-tapes and no special input tape.)

- Configuration

$$\triangleright\, a_1\, a_2 \begin{bmatrix} a_3 \\ q \end{bmatrix} \cdots\, a_k \sqcup \sqcup \sqcup \cdots$$

is string in $\Gamma^*(\Gamma \times Q)\,\Gamma^*$ where Γ is tape alphabet of M.

- enc : $\Gamma \cup (\Gamma \times Q) \to \{0, 1 \ldots p-1\}$ encodes symbols as numbers, where p is prime number.

- Halting Computation of M.

$$\underbrace{\overset{\text{Time } 0}{\triangleright a_1 a_2 \cdots}}_{c} \;\; \underbrace{\overset{\text{Time } 1}{\triangleright b_1 b_2 \cdots}}_{c} \;\; \underbrace{\overset{\text{Time } 2}{\qquad}}_{c} \cdots$$

Halting configuration

Configurations as number written out in base p.

Computions are also number written out in base p.

- Parameters

  p — the number used to encode symbols.

  c — length of one configuration

(in halting computation)

d – length of entire computation as string.

NotHalt – There is no halting computation

HaltComp(v) – Variable v encodes a halting computation of M on w.

- First configuration is initial config.
- Successive config follow the Transition function of M
- At some point M is in halting state.

Number – view as in base p

Auxilliary Formulas

- For $k \in \mathbb{N}$, $\underline{k} = \underbrace{1+1+1+\ldots+1}_{k}$
- Divides $(x, y) = \exists m \; y = x \times m$
- Prime $(x) = \big(((2 < x) \vee (2 = x)) \wedge \forall z\,(\text{Divides}(z, x) \to ((z=1) \vee (z=x)))\big)$
- $\text{Power}_p(x) = \big(\forall z\,(\text{Divides}(z, x) \wedge \text{Prime}(z)) \to (z = \underline{p})\big)$

$$a_0\, a_1\, a_2\, \dots\, a_k \dots$$

$\uparrow$

Digit at "position p^2".

— $\text{Symbol}(v, y, \underline{a})$ "The symbol at y in v is a"

$= \exists r.\, \exists u$

$$\left(v = u \times y \times \underline{p} + \underline{a} \times y + r\right) \wedge (r < y)$$

$\text{Start}(v, c)$ = "First c digits of v encodes starting configuration".

power p encoding length of one config.

Assume initial configuration $a_0, a_1, a_2 \dots a_n \sqcup^{c-n}$

$$\text{Start}(v,c) = \forall y \left[y < \underline{n} \rightarrow \text{Symbol}(v, y, \underline{a_y})\right]$$
$$\wedge \left[(\underline{n} < y+1 \wedge y < c) \rightarrow \text{Symbol}(v, y, \underline{\sqcup}) \right]$$

Suppose $H = \Gamma \times \{q_{acc}, q_{rej}\}$

$$\text{Halt}(v, d) = \exists y\, (y < d) \wedge \left(\bigvee_{a \in H} \text{Symbol}(v, y, \underline{a})\right)$$

Config 1 $\quad \boxed{a_0\ a_1\ a_2} \dots \boxed{a_c}$

Config 2 $\quad b_0\ b_1 \dots\dots b_c$

$\text{Mov} = \{ (a_0, a_1, a_2, b) \mid$ symbol b is the content of some cell if a_0, a_1, a_2 were the contents in the previous time step. }

$$\mathrm{ValidMove}(v, c, d)$$
$$= \forall y \Big((y \times c < d) \rightarrow$$
$$\Big(\bigvee_{(a_0, a_1, a_2, b) \in \mathrm{Mov}} \mathrm{Symbol}(v, y, \underline{a_0}) \wedge \mathrm{Symbol}(v, y\underline{p}, \underline{a_1}) \wedge$$
$$\mathrm{Symbol}(v, y\underline{p}\underline{p}, \underline{a_2}) \wedge$$
$$\mathrm{Symbol}(v, v \times c \times \underline{p}, \underline{b}) \Big) \Big)$$

$$\mathrm{HaltComp}(v) = \exists c \exists d \ \mathrm{power}_p(c) \wedge \mathrm{power}_p(d)$$
$$\wedge \ \mathrm{start}(v, c) \wedge \mathrm{Halt}(v, d) \wedge$$
$$\mathrm{ValidMove}(v, c, d)$$

$$\mathrm{Not}\ \underline{\mathrm{Halt} = \forall v}\ \neg \mathrm{HaltComp}(v)$$

Completeness Theorem If Γ is recursively enumerable then $Th(\Gamma)$ is recursively enumerable.

Corollary If $Th(\Gamma)$ is complete then $Th(\Gamma)$ is decidable.

Axiomatization of $\mathbb{N}$

A recursive set of sentences that characterizes $Th(\mathbb{N}, 0, 1, +, \times, <)$.

Is there a recursive axiomatization

is [illegible]

of $\mathbb{N}$?

No.

Peano's Axioms