

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

$\text{Not Halt}_{\langle M, w \rangle}$ s.t.

$$\langle M, w \rangle \in \overline{HP} \iff \text{Not Halt}_{\langle M, w \rangle} \in$$

$$Th(\mathbb{N}, 0, 1, +, \times, <).$$

Without loss of generality, assume

- M is TM with only one read/write

+ 1 1 π

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

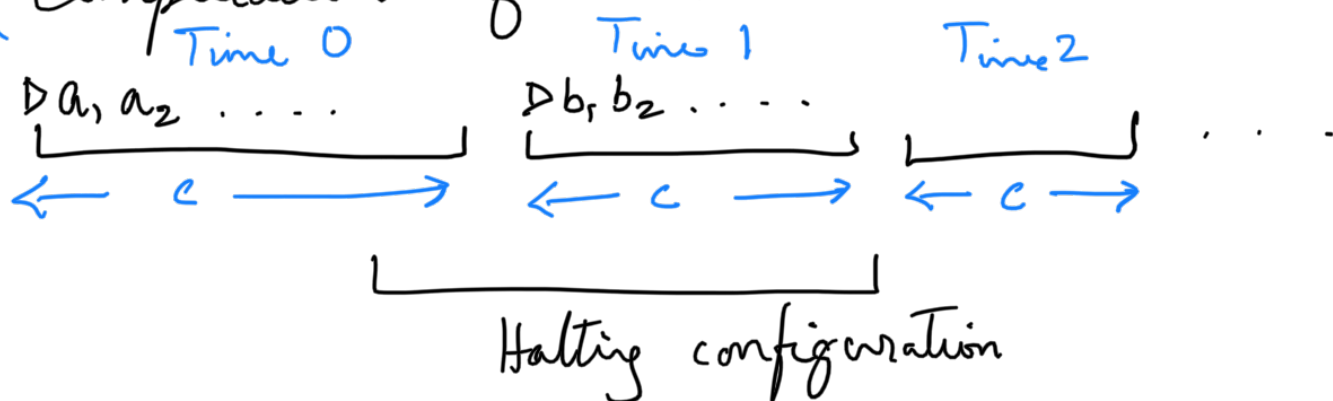
- Configuration

\downarrow
 $\triangleright a_1 a_2 \begin{bmatrix} a_3 \\ \vdots \\ q \end{bmatrix} \dots a_k \cup \cup \cup \dots$

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

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

- Computation of M .



Configurations as number written out in base p .

Computations 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.

Not Halt - There is no halting computation

Halt Comp (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

Auxiliary Formulas

- For $k \in \mathbb{N}$, $\underline{k} = \underbrace{1+1+1+\dots+1}_k$

- Divides $(x, y) = \exists m \ y = x \times m$

- Prime $(x) = ((2 < x) \vee (2 = x)) \wedge$

$\forall z \ (\text{Divides}(z, x) \rightarrow ((z = 1) \vee (z = x)))$

- Power _{p} $(x) = (\forall z \ (\text{Divides}(z, x) \wedge \text{Prime}(z)) \rightarrow (z = \underline{p}))$

$a_0 a_1 a_2 \dots a_k \dots$

↑
Digit at "position p^2 ".

- Symbol (v, y, \underline{a}) "the symbol at y in v is a "

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

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

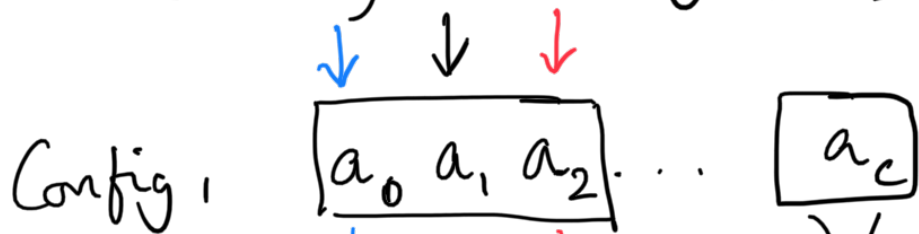
Start (v, c) = "First c digits of v encodes starting configuration".
power p
encoding length of one config.

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

$$\text{Start}(v, c) = \forall y [y < \underline{n} \rightarrow \text{Symbol}(v, y, \underline{a}_y)] \wedge [(\underline{n} < y+1 \wedge y < c) \rightarrow \text{Symbol}(v, y, \underline{\perp})]$$

Suppose $H = T^r \times \{q_{acc}, q_{rej}\}$

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



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

time step. $\{$

Valid Move (v, c, d)

$$= \exists y ((yxc < d) \rightarrow$$

$$\left(\bigvee_{(a_0, a_1, a_2, b) \in \text{Mov}} \text{Symbol}(v, y, \underline{a_0}) \wedge \text{Symbol}(v, \underline{y}, \underline{a_1}) \wedge \right. \\ \left. \text{Symbol}(v, \underline{y}, \underline{a_2}) \wedge \text{Symbol}(v, vxc \underline{y}, \underline{b}) \right)$$

$$\text{Halt Comp}(v) = \exists c \exists d \text{ power}_p(c) \wedge \text{power}_p(d)$$

$$\wedge \text{start}(v, c) \wedge \text{Halt}(v, d) \wedge$$

$$\text{Valid Move}(v, c, d)$$

$$\underline{\text{Not Halt}} = \forall v \neg \text{Halt Comp}(v)$$

Completeness Theorem If \mathcal{T} is recursively enumerable then $\text{Th}(\mathcal{T})$ is recursively enumerable.

Corollary If $\text{Th}(\mathcal{T})$ is complete then $\overline{\text{Th}(\mathcal{T})}$ is decidable.

Axiomatization of \mathbb{N}

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

↳ there is a recursive axiomatization

is there a successor of x ?

of \mathbb{N} ?

No.

Peano's Axioms