Gödel's Incompleteness Theorem

17^{th} century philosophy

Rationalists (Descartes, Spinoza, Leibniz) vs. Empiricists (Hobbes, Locke)

"all knowledge can be gained by reason alone."

"all knowledge has to come from experience through senses."

Math — Physics

Late 19^{th} - early 20^{th} century Math:

Foundations of Math

D. Hilbert asked for Axiomatization of Mathematics

1930's: Kurt Gödel proved that arithmetic cannot be axiomatized.

Informally, there is no

- finite set of axioms,
- finite derivation rules

so that every true arithmetic formula can be derived.

"There are true arithmetic sentences whose truth cannot be proved."

- arithmetic sentence ?
- truth ?
- provable ?

Arithmetic sentence:

a formula over vars $x, y, z, \ldots$

ar. opers $+, *$

$=, <$

constants $0, 1, 2, \ldots$

logical connectives $\wedge, \vee, \neg$
quantifiers $\forall, \exists$

Vars can be quantified (e.g., $\exists x \ldots$)
or not — free variables

Ex: $\exists x \, \forall y \, (x = 2 * y)$ false!

Sentence

$(1+1=2)$ true ✓

$\forall x \, \exists y \, (y = x+1)$ true ✓

A sentence = formula without free vars

- Truth: Sentence is either true or false over $\mathbb{N}$ with standard interpret. of all symbols with standard interpret. of such symbols.

provable: a proof system:

- set of axioms (truths)
- set of inference rules

A proof: sequence of statements where each st't is an axiom or is inferred from earlier statements by an infer. rule.

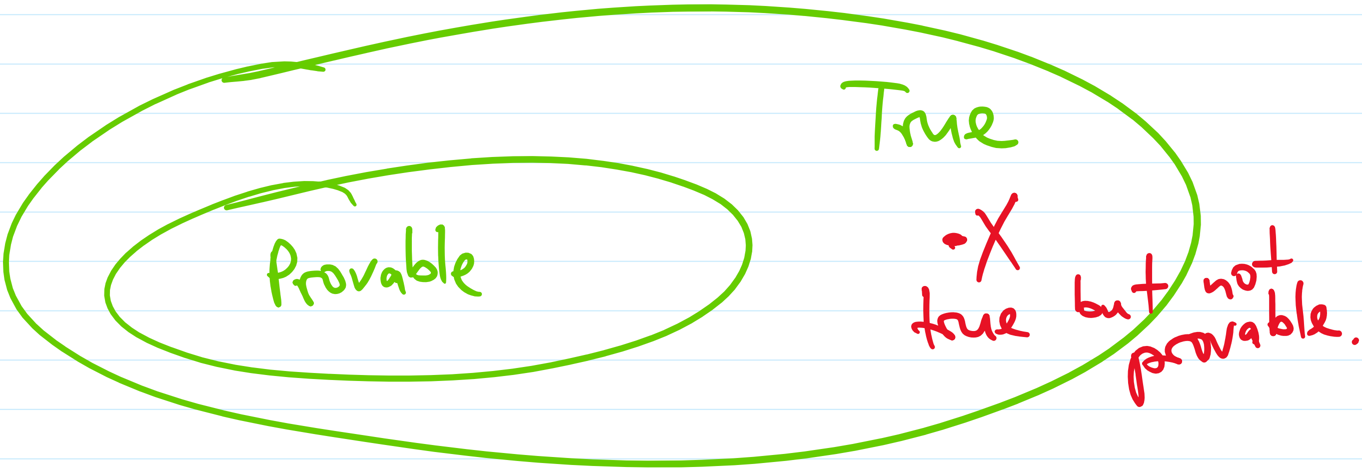
A standard proof system is s.t. one can check (easily) if a given string is a valid proof or not.

Proof System is called

- sound: every provable sentence is actually true is actually true

- completeness: every true sentence is provable in the proof system.

Want: proof system both Sound and Complete.



for sound proof systems

Thm (Gödel's 1^{st} Incompleteness Thm)

Fix any proof system $\mathcal{P}$ "powerful enough" (to reason about $+$ and $*$)

If $\mathcal{P}$ is sound,
then $\mathcal{P}$ is not complete.

<u>Proof:</u> Define

$\text{Provable} = \{\langle\varphi\rangle \mid \varphi \text{ is provable in } \mathcal{P}\}$

$\text{True} = \{\langle\varphi\rangle \mid \varphi \text{ is true}\}$

We'll show

$\text{Provable} \neq \text{True}$.

<u>Claim:</u> Provable is semi-decidable.

<u>Claim:</u> True is not semi-decidable.

<u>Proof:</u> $\overline{A_{TM}} \leq \text{True}$

Want $f : \langle M, w\rangle \longmapsto \varphi_{M,w}$

s.t.

M not acc $w \Rightarrow \varphi_{M,w}$ true

M not acc w $\Rightarrow$ $\neg_{M,w}$ true

M acc w $\Rightarrow$ $\varphi_{M,w}$ false

<u>Lemma:</u> $\exists$ an algorithm that given $\langle M, w \rangle$ outputs

$\psi_{M,w}$ s.t.

M acc w $\iff$ $\psi_{M,w}$ is true

Define $\varphi_{M,w} \equiv \neg \psi_{M,w}$

<u>Proof of Lemma: (Sketch):</u>

M accepts w :

$\exists\, c_0, c_1, c_2, \ldots, c_m$ s.t.

c_0 = init config of M on w

c_m = accepting config. of M

$\forall i,\quad c_i \overset{\delta}{\longmapsto} c_{i+1}$

$$\forall i, \quad c_i \vdash c_{i+1}$$

ar. formula

<u>Claim:</u> $\forall m \in \mathbb{N}$,
$\forall a_1, \dots, a_m \in \mathbb{N}$

$\exists A, B \in \mathbb{N}$ s.t.

$$\beta(A, B, i) = a_i \quad \forall i$$

where

$$\beta(x, y, i) = x \bmod (1 + y(i+1))$$