Given a language $\mathcal{L}$, is there a TM that decides it?

If not, $\mathcal{L}$ is undecidable.

Examples of undecidable languages:

- SELFREJECT = $\{\langle M \rangle : M \text{ rejects } \langle M \rangle\}$
- SELFHALT = $\{\langle M \rangle : M \text{ halts on } \langle M \rangle\}$
- SELFACCEPT = $\{\langle M \rangle : \underline{M} \text{ accept } \underline{\langle M \rangle}\}$
- ACCEPT = $\{\langle M, w \rangle : M \text{ accepts } w\}$

How do we prove a language is undecidable?

(1) Diagonalization — Cantor proved that $|\mathbb{R}| > |\mathbb{Z}|$

TM Y $\overline{\text{accept}}$ $\langle Y \rangle \iff$ TM not $\overline{\text{accept}}$ $\langle Y \rangle$

(2) Reduction from deciding a <u>known undecidable language</u>

Theorem HALT = $\{\langle M, w\rangle : M$ halts on $w\}$ is undecidable.

Proof We prove that HALT is undecidable by reduction from deciding SELFHALT.

Suppose HALT is decidable. Let H be the TM that decides HALT.

Now we can make a TM called SH that decides SELFHALT as follows:

SH($\langle M\rangle$):
  run H on $\langle M, \langle M\rangle\rangle$

data type check:

- SH is a TM that accepts $\langle M\rangle$ iff M halts on $\langle M\rangle$
- H is a TM that accepts $\langle M, w\rangle$ iff M halts on w
- M is a TM that is arbitrary

SH accepts $\langle M\rangle$ iff M halts on $\langle M\rangle$.

- SH accepts $\langle M\rangle$ if M halts on $\langle M\rangle$:

M halts on $\langle M\rangle$.
H accepts on $\langle M, \langle M\rangle\rangle$.
SH accepts on $\langle M\rangle$

- M halts on $\langle M \rangle$ if SH accepts $\langle M \rangle$:

SH rejects $\langle M \rangle$ if M does not halt on $\langle M \rangle$:

contrapositive
$p \Rightarrow q$
$\neg q \Rightarrow \neg p$

M does not halt on $\langle M \rangle$.
So H rejects $\langle M, \langle M \rangle \rangle$
so SH rejects $\langle M \rangle$.

But SH is undecidable!

So H cannot exist.

- most languages of form
"Given $\langle M \rangle$, does M accept ___?"
are undeciable

- are there undecidable problems that are not about TMs that are undecidable?

1) Diophantine Equations ~1970

Given a polynomial, does it have integer solution?

$a^2 + b^2 = c^2$ yes infinitely many

$a^n + b^n = c^n$ $n > 2$

2) Post Correspondence Problem