Undecidability

Rice's theorem:

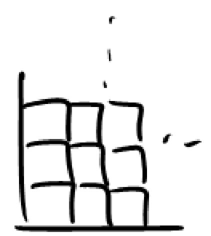
you can't decide anything that involves the language of a Turing machine

The implications of undecidability:

Software verification is not solvable.

Several problems are not solvable:

- Knot theory.
- PCP
- tiling
- Diophantine eq.



main
    n ← 4 ;
    while true
        call Percolate(n)
        n ← n+2;

percolate(n)
    for p < q < n do
        If p is prime & q is prime and p+q = n then return
    If you reach this point, halt!

Goldbach conjecture
Every even number can be written as the sum of two primes

Reduction to show L is undecidable.

A_{TM} reduces to L.

Known to be undec

Show $L_3 = \{ \langle M \rangle \mid M$ is a TM and $|L(M)| = 3 \}$

Proof: Show A_{TM} reduces to L_3

$A_{TM} = \{ \langle M, w \rangle \mid M$ is a TM that acc $w \}$

Build a decider for A_{TM}, given an oracle decider L_3.

Decider for A_{TM}:

- Input $\langle M, w \rangle$
- Construct a machine $M'_{\langle M, w \rangle}$.
- Feed M' to the oracle deciding L_3
- Depending on the answer, it will decide whether M acc w or not.

I want to reduce the problem of checking whether M acc w to the problem of checking whether $M' \in L_3$. (i.e. $|L(M')| = 3$?)

M':
for a particular $\langle M, w \rangle$

- Input x
- Simulate M on w.
- If M halts and rejects, reject
- If M halts and accepts, then accept provided $x =$ "UIUC", $x =$ "Michigan" or $x =$ "Iowa".

So

If M acc w, then $L(M') = \{$UIUC, Michigan, Iowa$\}$

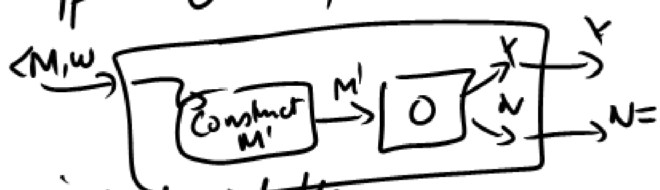
If M does not accept w,
(i.e. M halts and rejects w or
M does not halt on w)
$L(M') = \emptyset$

So M acc w iff $|L(M')| = 3$

So A_{TM} reduces to L_3.

Decider for A_{TM} using an oracle decider O for L_3:

1. Input $\langle M, w \rangle$.
2. Construct M' (as on prev. slides)
3. Feed M' to O
4. If O reports "Yes", halt and accept
5. If O reports "No", reject.



So L_3 is undecidable.

Rice's theorem.

Suppose L is a languages of Turing machine descriptions such that:

a) Membership of a $\langle M \rangle$ in L depends only on the <u>language</u> of L

If $\langle M \rangle$ and $\langle M' \rangle$ are such that $\mathcal{L}(M) = \mathcal{L}(M')$ then either ($\langle M \rangle \in L$ & $\langle M' \rangle \in L$) or ($\langle M \rangle \notin L$ & $\langle M' \rangle \notin L$)

b) L is not trivial (i.e. $L \neq \emptyset$ nor is L = all TMs)

Then L is undecidable.

Proof Let TM_ϕ be a TM that accepts nothing.

Assume that

$$\langle TM_\phi \rangle \notin L$$

Since L is non-trivial, there is a TM $\langle Z \rangle$ s.t. $\langle Z \rangle \in L$

We'll show A_{TM} reduces to L.

i.e. given an oracle for L, we will design a decider for A_{TM}.

The decider for A_{TM} gets input $\langle M, w \rangle$ and will construct a TM $\langle M' \rangle$.

This TM $\langle M' \rangle$ for a given $\langle M, w \rangle$ is:

- Input x
- Simulate M on w
- If simulation halts & reject, reject x.
- If M acc w, simulate Z on x
- If Z acc x, accept & if Z halts & rejects, reject

ensures $L(M') = L(Z)$

If M does not acc w, $L(M') = \phi$ and hence $\langle M' \rangle \notin L$.

If M acc w, $L(M') = L(Z)$ and hence $\langle M' \rangle \in L$.

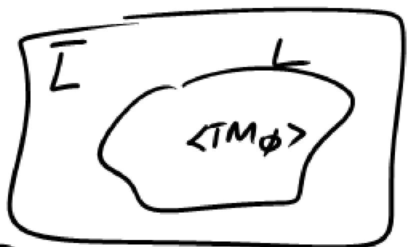
Decider for A_{TM}:

- Input $\langle M, w \rangle$.
- Construct M'
  (s.t. $L(M') = \phi$ if M does not acc w
  $L(M') = L(z)$ if M acc w
  i.e. M acc w iff $\langle M' \rangle \in L$)
- Feed M' to the oracle O decides L.
- If O says "yes", accept
  If O says "no", reject.

Hence L is undecidable.

Now, if $\langle TM_\phi \rangle \in L$.

Then consider $\overline{L}$



$\overline{L}$ satisfies the two conditions in the thm.
(it is a semantic property of TMs & is non-trivial)

& $\overline{L}$ does not contain $\langle TM_\phi \rangle$.

Hence $\overline{L}$ is undecidable.

Hence L is undecidable.

L reduces to $\overline{L}$:

Suppose

$$L_1 = \{ \langle M \rangle \mid |L(M)| = 3 \}$$

If $\langle TM_\phi \rangle \in L_1$? No!

$$L_2 = \{ \langle M \rangle \mid L(M) = \phi \}$$

Is $\langle TM_\phi \rangle \in L_2$. Yes.

L_1 & L_2 are both non-trivial