Limits of diagonalization

Diagonalization

1) $\forall$ TM has effective representation
2) Existence of universal machine that simulates any other machine without much overhead in time or space.

Diagonalization approach treat MT as a black box. The machine's internal working do not matter.

We provide an idea why P ? NP cannot be resolved using diagonalization.

Def An oracle Turing machine.

$\boxed{MT}$ + oracle tape and three special states q_{query}, q_{yes}, q_{no}. Specify language $O \in \{0,1\}^*$.
oracle.

$M^O(x)$ - output of M with oracle access to language O.

Non-deterministic oracle MTs are defined similarly.

Def P^O, NP^O.

Example (i) $\overline{SAT} \in P^{SAT}$.

(ii) $O \in P \Rightarrow P^O = P$

(iii) $EXPCOM = \{\langle M, x, 1^n \rangle : M$ outputs 1 on x within 2^n steps$\}$

$EXP \subseteq P^{EXPCOM}$

$NP^{EXPCOM} \subseteq EXP$ - simulate oracle requests in EXP time and enumerate all certificates in EXP time.

Theorem $\exists$ oracles A and B s.t.

$P^A = NP^A$ and $P^B \neq NP^B$.

Proof $A = EXPCOM$.

For any language B construct language

$$U_B = \{1^n : \exists x \in B \text{ and } |x| = n\}$$

construct desired B step by step.

Stage i ensures that M_i does not decide U_B in $\frac{2^n}{10}$ time

string represented by i

Choose n big enough s.t. its length exceed lengths of any string in B.

Run M_i on 1^n, answer oracle queries correctly, if value is not determined say the word do not belong B.

If M_i answer ~~yes~~ yes ~~exclude all strings o~~ assign all strings of length n to do not belong B.

If M_i answer no assign one string into B whose fate was not determined before.

Such string exists as $\frac{2^n}{10}$ ~~$+ \frac{2^{n-1}}{10} + \ldots < 2^n$~~.

$$\frac{2^n}{10} < 2^n.$$

Any $p(n) < \frac{2^n}{10}$ from some point as each M appear infinitely often.

Space complexity

Def Let $S: \mathbb{N} \to \mathbb{N}$ and $L \subseteq \{0,1\}^*$.

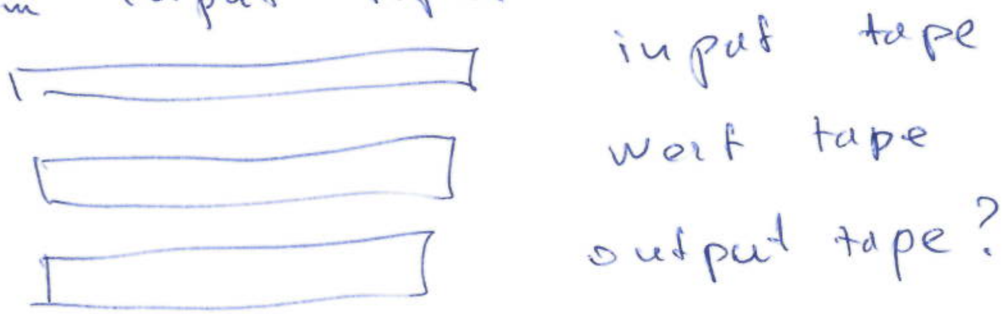
$L \in SPACE(S(n))$ if $\exists$ constant c and TM M deciding L such at most $c \cdot S(n)$ locations of M's work tapes (excluding input tape) are ever visited by M's head during its computation on every input of length n.

Similarly $L \in NSPACE(S(n))$.

Consider only space constructibe function here. I.e. $\exists$ TM M that computes $S(|x|)$ in $O(S(|x|))$ space given x as input.

$\log n$, n, 2^n are space constructible.

Here, we think that work tape is separated from input tape.



Reasonable to consider $S(n) \leq n$.

we require $S(n) \geq \log n$.

Note $DTime(S(n)) \subseteq SPACE(S(n))$.

Theorem

$$DTime(S(n)) \subseteq SPACE(S(n)) \subseteq NSPACE(S(n)) \subseteq$$
$$\subseteq DTime(2^{O(S(n))}).$$

<u>Def</u> Configuration of TM M consists of the contents of all non-blank enties of M's tapes, its state, and head position.

For every ~~$S(n)$~~ space $S(n)$ TM M and input $x \in \{0,1\}^*$ configuration graph — $G_{M,x}$

directed graph.

nodes - possible configurations of M on input x.

tapes have at most $S(|x|)$ nonblank cells.

$C \to C'$ if C' is reachable in one step.

M-deterministic outdeg $= 1$

M-non-deterministic outdeg ≤ 2.

$M \rightsquigarrow M'$ such that accept configuration contains empty working tape and 1 on output tape.

<u>Claim</u> Let $G_{M,x}$ configuration graph for $S(n)$ space MT M on some input x of length n.

1) Every vertex can be described in $cS(n)$ bits.

2) $\exists$ $O(S(n))$-size CNF $\varphi_{M,x}$ s.t.

$\varphi_{M,x}(C, C') = 1$ iff $C \to C'$.

$\hookrightarrow$ $\boxed{\text{As exercise}}$ ~~for~~ P

From Breadth-First-Search follows $NSPACE(S(n)) \subseteq DTime[2^{cS(n)}]$

Construct graph and run BFS.

<u>Def</u> $PSPACE = \bigcup_{c>0} SPACE(n^c)$

$NSPACE = \bigcup_{c>0} NSPACE(n^c)$

$L = SPACE(\log n)$

$NL = NSPACE(\log n)$

<u>Example</u> $3SAT \in PSPACE$.

<u>Example</u> EVEN, MULT in L.

<u>Open Question</u> $3SAT \overset{?}{\in} L$.

PSPACE COMPLETENESS

<u>Def</u> L' is PSPACE hard if $\forall L \in PSPACE$
$L \le_p L'$. if $L' \in PSPACE \Rightarrow L'$ is PSPACE-complete.

<u>Def</u> A quantified Boolean formula (QBF) is a formula of the form $Q_1 x_1 \dots Q_n x_n \varphi(x_1, \dots x_n)$
$\forall Q_i \in \{\forall, \exists\}$, $x_i \in \{0,1\}$, φ – Boolean formula

<u>Example</u> $\forall x \exists y \; (x \wedge y) \vee (\bar{x} \wedge \bar{y})$ – true
$\qquad\qquad\qquad \overset{\shortparallel}{\forall x \exists y \; x = y}$.
$\forall x \forall y \; (x \wedge y) \vee (\bar{x} \wedge \bar{y})$ – false

<u>Example</u> SAT is QBF: $\forall i \; Q_i = \exists$.
TAUTOLOGY is QBF: $\forall i \; Q_i = \forall$.

Theorem TQBF is PSPACE-complete.

Proof $\psi = Q_1 x_1 \ldots Q_n x_n \, \varphi(x_1, \ldots x_n)$

Membership

$S_{n,m}$ - space that algorithm uses on formulas with n variables and description size m.

Write $\psi|_{x_i=0}$, solve recursively

Save answer

Write $\psi|_{x_i=1}$ above $\psi|_{x_i=0}$, solve recursively

$S_{n,m} = S_{n-1,m} + O(m) \Rightarrow S_{n,m} = O(nm)$

TQBF $\in$ PSPACE.

completeness

let $L \in$ PSPACE, M decides L in $S(n)$ space.

We construct TQBF of size $O(S(n)^2)$

$m = O(S(n))$ number of bits in order to encode configuration of machine M.

$\exists\, \varphi_m$ s.t $\varphi_m(C, C') = 1$ iff $C \to C'$.

Goal to build ψ with two unquantified variables s.t. $\psi(C, C')$ if $\exists$ directed path from C to C'.

$\psi(C_{start}, C_{accept}) = 1$ iff M accepts x.

$\psi_0(C, C') = \varphi_{M,x}(C, C')$

$\psi_i(C, C')$ - distance between C and $C' \leq 2^i$.

$\psi_i(C, C') = \exists C'' \; \psi_{i-1}(C, C'') \wedge \psi_{i-1}(C'', C')$

Length is to big.

$$\exists C'' \forall D_1 \forall D_2 \left(\left(\left(D' = C \wedge D^2 = C'' \right) \vee \right.\right.$$

$$\left.\left. \vee \left(D' = C'' \wedge D'' = C' \right) \right) \Rightarrow \varphi_{i-1}(D', D^2) \right).$$

$$size(\varphi_i) \leq size(\varphi_{i-1}) + O(m)$$

$$\Rightarrow size(\varphi_m) \leq O(m^2).$$

$\boxtimes$

$x \to y$

$1 \quad 0$

$y \vee \bar{x}$