Time Complexity Classes, P, NP

Defn: Let $t(n)$ be a fn $\mathbb{N} \to \mathbb{N}$. A language $L \in DTIME(t(n))$ if $\exists$ a standard TM M and constant c s.t. M decides L and runs in $c \cdot t(n)$ time.

Q. Define $DTIME_\Sigma(t(n))$ using TMs over alphabet Σ. ($|\Sigma| > 2$)
What is the best statement?

A) $DTIME_\Sigma(t(n)) \subseteq DTIME(t(n))$

B) $DTIME(t(n)) \subseteq DTIME_\Sigma(t(n))$

✓C) $DTIME(t(n)) = DTIME_\Sigma(t(n))$

because TM over alphabet Σ can be simulated by TM over binary alphabet with $\log_2|\Sigma|$ overhead in running time

Q. Define $DTIME_k(t(n))$ using TMs with k tapes ($k > 1$)
What is the best statement?

A) $DTIME_k(t(n)) \subseteq DTIME(t(n))$

✓B) $DTIME(t(n)) \subseteq DTIME_k(t(n))$

C) $DTIME(t(n)) = DTIME_k(t(n))$

We prove that a k-tape TM running in $t(n)$ time can be simulated in $O(k\,t(n)^2)$ time by a standard TM.

[HS] efficient simulation $O(k\,t(n)\log t(n))$

$$\boxed{\mathrm{DTIME}_k(t(n)) \subseteq \mathrm{DTIME}(t(n)\log t(n))}$$

$$\subseteq \mathrm{DTIME}(t(n)^2)$$

Defn: $$\mathbb{P} = \bigcup_{c\in\mathbb{N}} \mathrm{DTIME}(n^c)$$

$\mathbb{P}$ does NOT depend on the # tapes or alphabet size.
on the specifics of the TM.

Strong CT Thesis: Every physically realizable model of computation can be simulated by standard TMs with polynomial overhead.

(1) $\mathbb{P}$ contains all languages that can be efficiently decided. [Cobham's thesis 62]

(2) $\mathbb{P}$ contains "closure" of efficient algorithms. An algorithm that invokes a poly-time algorithm polynomially many times is also polynomial.

(3) [Edmonds 64, Gödel 52, Trakhenbrot 50s, Cobham 62]

For many languages/problems, existence in P implied ~~an~~ a non-trivial algorithm that beat brute-force.

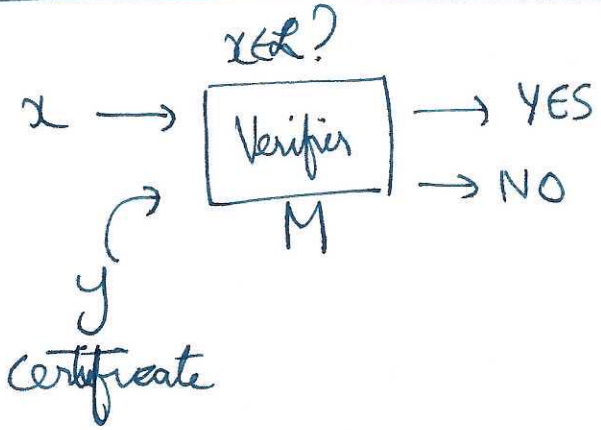
Defn [NP] $\mathcal{L} \in$ NP if $\mathcal{L}$ is "poly-time verifiable".

$\exists$ polynomials p and q ~~s.t.~~ and a TM M s.t.

$\forall\ x \in \mathcal{L}, |x|=n$ $\exists$ "certificate" y, $|y| \leq p(n)$ s.t.
$M(x,y)$ accepts in $q(n)$ time

AND

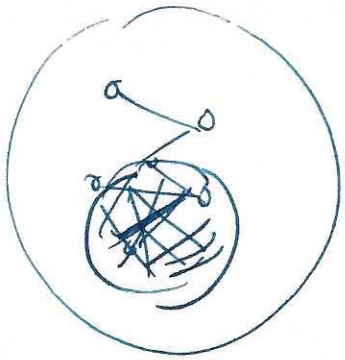
$\forall\ x \notin \mathcal{L}, |x|=n$ $\forall$ certificates y, $|y| \leq p(n)$
$M(x,y)$ rejects (in $q(n)$ time)



If $x \in \mathcal{L}$, there is a ~~certificate~~ certificate making M accept.

If $x \notin \mathcal{L}$, M will never accept.

In a simple graph $G=(V,E)$,
a clique C is a set of vertices
st. $\forall u,v \in C, (u,v) \in E$.



$L = \{ G \mid G$ has a clique of size $\geq |V|/2 \}$

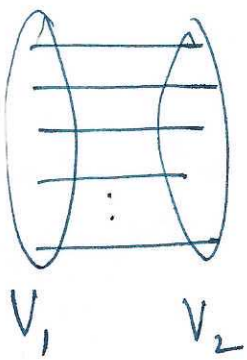
$L \in NP$. Certificate? Clique of size $\geq |V|/2$.

(0) Verifier takes G and a certificate (C subset of vertices ~~POTENTIAL clique~~ of size $\geq |V|/2$).

(1) Verifier checks if all edges in C are present.

(2) If yes, ACCEPT, else REJECT

$L = \{ $ ~~$G=(V,E)$~~, $G=(V_1, V_2, E)$ bipartite $\mid$ G has a perfect matching $\}$



$L \in NP$

Q. Hilbert's 10th problem. Given a set S of Diophantine equations, does there exist an integer solution?

$L = \{\langle S \rangle \mid S \text{ has integer soln}\}$

$x^2+y^2=z^2$ 3,4,5 $x^3+y^3=z^3$

$x^2+y^2=2z^2$
1 7 5

NO! Fermat's Last Theorem

The certificate may not have a polynomial size.

Q. Set of linear equations

$Ax = b$, $x \in \mathbb{R}^d$ Does there exist of solution this linear system?

(For square A) By Cramer's rule, for any solution $\bar{x}$, entries can be represented as ratios of determinants.

In general The bit complexity of $\bar{x}$ is polynomial in bit complexities of entries of A and b. $\in NP$

Gaussian Elimination

$L = \{ G \mid G$ does NOT have a clique of size $\geq |V|/2 \}$

$$\binom{|V|}{|V|/2} = \Theta\left(\frac{2^{|V|}}{\sqrt{|V|}}\right)$$

Is there a smaller certificate? BIG OPEN PROBLEM

Obvious certificate: all subsets of size $\geq |V|/2$.

But this has exponential size.

~~If~~ There is a small (poly) ~~cert~~ certificate of NOT being in language.

Thm: $P \subseteq NP$.

Q. What is certificate for a language $L \in P$?

(A) Everything

(B) Nothing

~~(C)~~ Whatever you want

Verifier: $L \in P$, decided by poly-time TM M'

(1) Runs $M'(x)$. If $x \notin L$, reject.

(2) If y is a certificate of my choice, accept. Else reject.

Def: A non-deterministic TM has a non-deterministic transition fn. $\delta : Q \times (\Sigma \cup \{\sqcup\}) \to 2^{(Q \times (\Sigma \cup \{\sqcup\}) \times \{\leftarrow, \rightarrow\})}$.

The running time is an upper bound on all computational paths.

M runs in $t(n)$ time $\Rightarrow$: $\forall x, |x| = n$, all computations of $M(x)$ run in $t(n)$ time.

Def: $L \in \text{NTIME}(t(n))$, if $\exists$ a standard NTM and constant α s.t. M decides L and runs in $\alpha t(n)$ time

Thm: $\text{NP} = \bigcup_{c \in \mathbb{N}} \text{NTIME}(n^c)$

Proof sketch: Suppose $L \in \text{NP}$.

We need to show $\exists c$ s.t. $L \in \text{NTIME}(n^c)$

(Non-deterministically guess certificate)

Suppose $L \in \text{NTIME}(n^c)$ (for $c \in \mathbb{N}$)

We need to show $L \in \text{NP}$.

(Certificate is the non-deterministic computational path.)