CSE322 Theory of Comput. (L25)

$P(k) = TIME(n^k)$

$P = P(0) \cup P(1) \cup P(2) \cup \ldots$

$EXP(k) = TIME(2^{(n^k)})$

$EXP = EXP(0) \cup EXP(1) \cup EXP(2) \cup \ldots$

$NP(k) = NTIME(n^k)$

$NP = NP(0) \cup NP(1) \cup NP(2) \cup \ldots$

If $A \leq_m \overline{A}$ then $\overline{A} \leq_m A$.

$A = \emptyset$ $\overline{A} = \Sigma^*$

$A \leq_m \overline{A}$ by definition?

$\boxed{f(x) = x}$

$x \in \emptyset$ iff $f(x) \in \Sigma^*$

$\Rightarrow x \in \emptyset$ iff $x \in \Sigma^*$

$A \leq_m \overline{A}$

$x \in A$ iff $f(x) \in \overline{A}$

$\Rightarrow x \notin A$ iff $f(x) \notin \overline{A}$

$\Rightarrow x \in \overline{A}$ iff $f(x) \in A$

$\Rightarrow \overline{A} \leq_m^f A$

$f(x) = x$

Claim :- $y \in \overline{A}$ iff $f(y) \in A$

$\Rightarrow$ Let $y \in \overline{A}$. $f(y) =$

$\bigcup_{k>0} \text{DTIME}(n^k)$ Since $\text{DTIME}(n^k) \subseteq \text{NTIME}(n^k)$

$\subseteq \bigcup_{k\geq 0} \text{NTIME}(n^k)$

Show that P is a subset of NP

Show that NP is a subset of EXP

$c = \lceil \log_2 b \rceil$

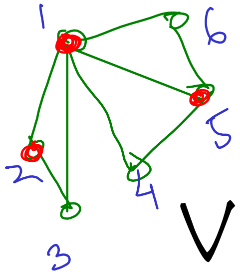
$\text{NTIME}(t) \subseteq \text{DTIME}(b^t) \subseteq \text{DTIME}(2^{ct})$

$\text{NTIME}(n^k) \subseteq \text{DTIME}(2^{cn^k})$

$c\, n^k <<< n^{2k}$

$\subseteq \text{DTIME}(2^{n^{2k}})$

$NP \subseteq EXP$



$K = 1$ $\quad (G,1) \notin VC \quad (G,3) \in VC$

$(G,2) \notin VC$

VERTEX-COVER $= \{ \langle G, K \rangle$: Graph G has a vertex cover with at most K vertices $\}$

$VC \in NP$ def VCNDTM(G,K):

$O(m)$ non-deterministically choose a subset V' of vertices

if $|V'| > K$: goto q_{rej}

for every edge $(u,v) \in E$:

$O(m)$ if $u \notin V'$ and $v \notin V'$:

goto q_{rej}

goto q_{acc}.

AVC: decider for VC

find MinVC(G):

for $k = 1 \ldots |V|$:

if AVC$(G,k) \rightarrow$ true

return k

Claim 1: halts on all nondet. branch

Claim 2 & 3: correctness w.r.t. VC

Claim 4: running time

SUBSETSUM

$\{ \langle$Array A, target int $T \rangle$: A has a subarray of sum $T \}$

$O(m)$

$O(m^2)$

3COLOR

$\{ \langle G \rangle$: G can be coloured using ≤ 3 colours$\}$

CHROMATIC

$\{ \langle G, K \rangle$: G can be coloured using at most K colours $\}$

G: m vertex graph.

$|G| = m^2 \qquad n = m^2 + \lg m$

$|K| = \lg m$

running time should be $poly(n) = poly(m)$

$O(m^3)$

TSP

$\{ \langle G, T \rangle$: G is a complete wtd graph & has a tour of cost at most $T \}$

3SAT

$\{ \langle F \rangle$: F is a Boolean 3CNF formula & F is satisfiable$\}$

$F = (x_1 \vee x_2) \wedge (x_3 \vee x_4 \vee \bar{x}_1) \wedge (x_2 \vee \bar{x}_3)$ is satisfiable if some truth value assignment so that F is true

variable literals

$F' = (x_1 \vee x_2) \wedge (x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2)$ not satisfiable

3CNF : Conjunctive normal form

And of ORs $\quad (\cdot \vee \cdot \vee \cdot) \wedge (\cdot \vee \cdot \vee \cdot) \wedge (- - -)$

clause

3 literals in each clause

---

coNP = { L : complement(L) is in NP }

Co P $= \{ L : \bar{L} \in P \}$

Co EXP

Claim:- $CoP = P$?

$CoEXP = EXP$

P is included in both NP and coNP. Both NP and coNP are included in EXP.

Open: Is P = NP?

Open: Is NP = coNP?

$P \subseteq NP$

$P = NP$
$P \neq NP$

$NP \subseteq P$

$P \not\subseteq NP$

RELPRIME = $\{ \langle x,y \rangle$: x, y prime to each oth.$\}$

Show that RELPRIME belongs to P. Euclid's GCD

PRIMES = $\{ \langle x \rangle$: x is prime $\}$ $\in NP$

Agarwal Kayal Saxena

Open for a long time. In 2002, PRIMES was shown to belong to P.

COMPOSITES = $\{ \langle x \rangle$: x is not a prime number $\}$ $\in NP$

What is the complexity of PRIMES & COMPOSITES ?

$\in NP \cap CoNP$

$= \{ \langle D_1, D_2 \rangle : L(D_1) = L(D_2) \}$

Show that EQ-DFA is in P. How to calculate input length?

(EQ-NFA is not known to be in P.)

Q. Show that 2SAT is in P.

(3SAT is not known to be in P.)

Can you solve them ? (and get A+)

$P \subseteq NP \subseteq EXP$

Thm: P is a subset of NP is a subset of EXP.

$P \subsetneq EXP$

(Not proved) Thm: P is a strict subset of EXP.

Open: Either P is not equal to NP or NP is not equal to EXP.

Prove whichever is true.

$L1 \leq^{p}_{m} L2$: poly-time many-one redn.

L1 <=mp L2 (L1 is polynomial-time many-one reducible to L2) if ...

there exists a many-one reduction from L1 to L2 that is polynomial-time.

Prove: L1 <=mp L2 and L2 $\leq^{p}_{m}$ L3 implies L1 <=mp L3.

R12 n^{k_1} R23 n^{k_2} R13

$x \in L1$ iff $z \in L3$

def R13(x):

$y \in L2$ iff $x \in L1$ y = R12(x) // $|x|^{k_1}$

$z \in L3$ iff $y \in L2$ z = R23(y) // $|y|^{k_2}$

return z

Is R13 poly time?

Total: $|x|^{k_1} + |y|^{k_2}$

$\because |y| \leq |x|^{k_1}$

$\Rightarrow$ Total $\leq |x|^{k_1} + |x|^{k_1 k_2}$

$= O(|x|^{k_1 k_2})$

L is NP-hard if for EVERY H in NP, H <=mp L.

L is NP-complete if (a) L is in NP, and (b) L is NP-hard.

Suppose H is NP-complete. If H <=mp L, then L is NP-hard.

How to prove that L is NP-complete?

1. Prove L is in NP
2. Prove L is NP-hard by reducing FROM some NP-complete H.

First NP-complete problem: SAT