Announcements

- HW6 due today as usual
- HW7 single question, due Tuesday March 17th max 1 late day

- Prelim 2: Tuesday March 24th
  - The conflicts survey is open, due on Monday, March 16th
  - Topics: stable matching, flows and applications and NP-completeness
  - Information sheet on topics and sample question in canvas

Thank you for all who responded to the survey (147)

Final announced: May 9 at 9am

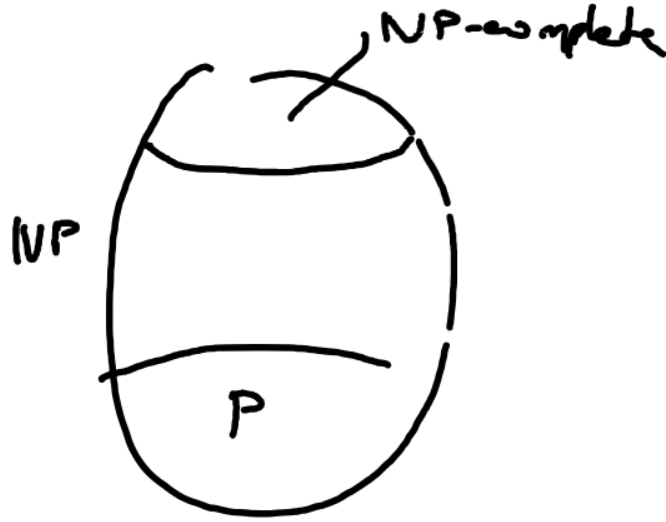
P, NP and NP-complete summary

All decision problems

P = solable in polynomial time

NP = yes answer with hint/help veriable in poly time

NP-complete : hardest in NP



P = NP? 1M $

Proving new problem X NP-complete

1. $X \in NP$
2. pick an NP-complete problem Y
   & prove $Y \leq_p X$

NP-complete summary

HW7

which problem to pick?

find at least k ...

find at most k ....

- Independent Set : packing
  very indep set, set packing
- Vertex Cover : covering
  cycle cover
- Hamiltonian Cycle and Hamiltonian Path sequencing
  & TSP
- Subset Sum & Knapsack problems hard due to huge numbers
- SAT and 3-SAT constraint satisfaction

Asymmetry of NP and co-NP

NP = yes verifiable in polynomial time with a hint

co-NP = no verifiable in polynomial time with a hint

Examples

1. Given $G = (V, E)$ are all independent set size $\leq k$

   if no: given indep set $I \subseteq V$ $|I| > k$ easy to verify

2. tautology $\overline{\emptyset} = (x_1 \wedge x_2 \wedge \bar{x}_3) \vee (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3) \vee \cdots$

   ($\wedge$: and; $\vee$: or)

   is $\overline{\emptyset}$ always true on any setting of variable

   clearly in co-NP

   reverse from SAT

Note $\emptyset$ SAT formula

$(x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2) \cdots$

$\neg\emptyset = \neg[(x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2) \wedge \cdots]$

$= (\neg(x_1 \vee x_2 \vee x_3) \vee \neg(\bar{x}_1 \vee x_2) \vee \cdots)$

$= (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3) \vee (x_1 \wedge \bar{x}_2) \vee \cdots)$

More examples of problems in co-NP

p integer is p a prime: PRIME

Claim: PRIME $\in$ co-NP

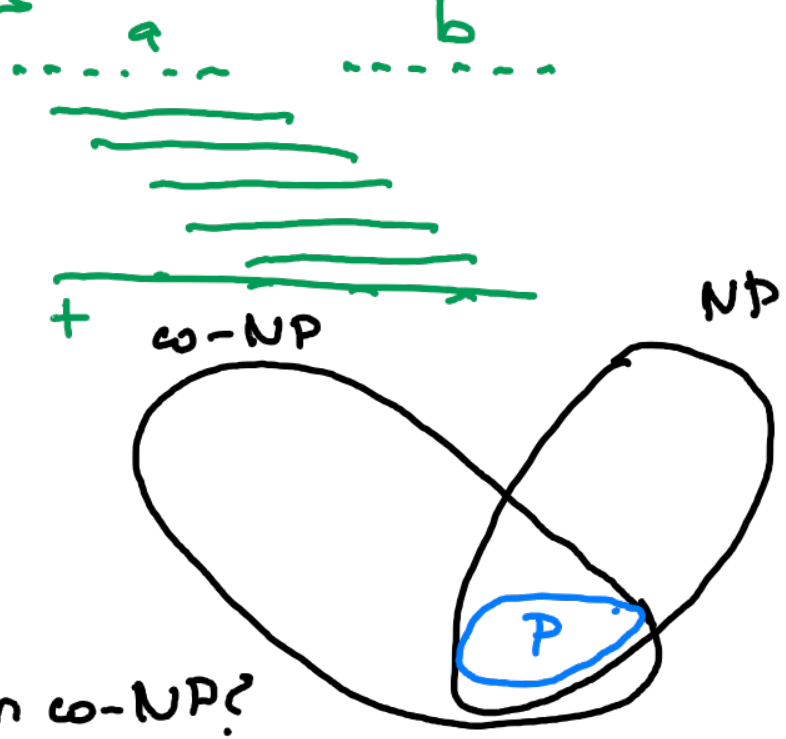
Proof: p not prime $p = a \cdot b$ a, b integers $< p$

time to verify this

$\leq \log p$ # digits

time $O(\log^2 p)$

input length $\log p$



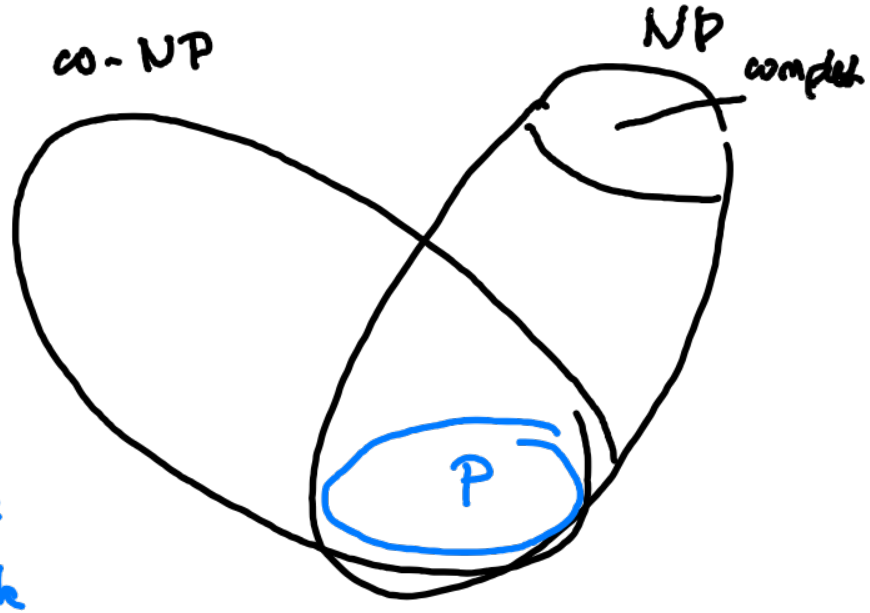
Actually PRIME $\in$ P

Agrawal - Kayal - Saxena 2002

Claim $P \subseteq NP \cap$ co-NP

Open $P = NP \cap$ co-NP?

NP ∩ co-NP examples



$P = ? \; NP \cap co\text{-}NP$

1. given network & capacities, target value v
   is max flow value $\geq v$

   in NP : given flow, easy to check

   in co-NP: given s-t cut, easy to check
   cut value $< v$

2. In fact $P \subseteq NP \cap co\text{-}NP$

3. DIVISER given two integers n & m
   does n have a divisor $\leq m$
   $\exists \; n = ab$ with $1 < a \leq m$

   Example
   $n = 49$ $m = 6$
   no

decision version of given n
write as a product of primes

Join by Web PollEv.com/evatardos772

Does DIVISER belong to P, NP, co-NP...

given n & m
$\exists\ a, b$ integers $n = ab$
$1 < a \leq m$
input length $2 \log n$

A. DIVISER is in NP ✓ given a : alg divide
- B. DIVISER is in co-NP
- C. DIVISER is in NP ∩ c-NP

hint: $n = p_1 \cdots p_k$ primes
checking equation $O(k \log^2 n) \leq O(\log^2 n)$
one product $O(\log^2 n)$
& run AKS to check each are primes

D. DIVISER is in P

open

method 1:
* test all $a = 1 \ldots, m$ if $a \cdot b = n$, time $O(m \cdot \log n)$ exponential

poly time testable on quantum computers, see CS 4813

How efficiently can we solve NP-complete problems (or co-NP-complete problems)

Observe: SAT solvable in time 2^n polynomial

n = # variables