A Panaroma of "Computational" Problems"

✓ (1) MULTIPLICATION: Given two nos. a, b (n-digit) compute $a \times b$.

✓ (2) PRIMES: Given an $n \geq 2$, test if n is prime or not.

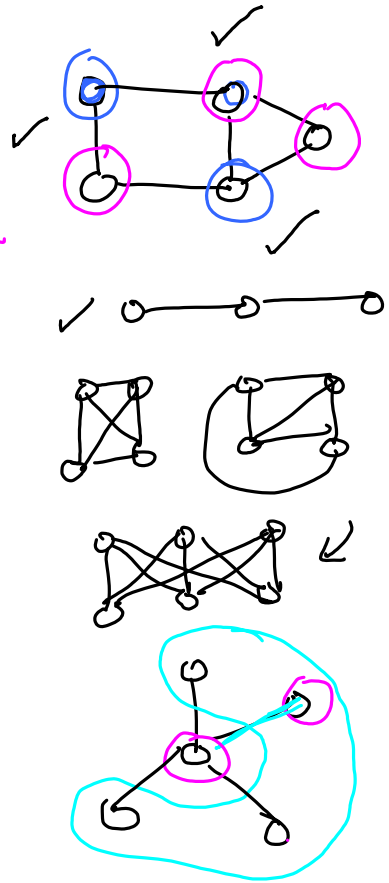
✓ (3) GCD: "Given" $a, b \geq 0$, compute $\gcd(a,b)$ Euclid's algorithm

(4) ODD CYCLE: Given graph G, test if G has odd cycle or not.

(5) PLANARITY: Given graph G, test if G is planar or not.

✓ (6) MAX-CUT: Given a graph G, find a partition $S, T \subset V$ s.t. $|\{(u,v) \mid u \in S, v \in T\}|$ is maximized.

cut



✓ (7) **SATISFIABILITY**: Given a boolean formula $\varphi(x_1, \ldots, x_n)$, decide if it is satisfiable or not

↳ $\{\wedge, \vee, \neg\}$

$\varphi_1 = x_1 \wedge \neg x_1$

$\varphi_2 = x_1 \vee x_2$

? $\exists\ a_1, \ldots, a_n \in \{0,1\}^n$ s.t $\varphi(a_1, \ldots, a_n) = 1$

(8) COUNT-ASSIGN : Given φ, count the no of satisfying assignments.

(9) SEARCH-ASSIGN: Given φ (satisfiable) search / op that satisfying assign

Comp Problems : Decision, Search, Counting, Optimization

↓

Yes / NO

Primes, Planarity

"Algorithm": step-by-step proc. to solve a problem

How is the i/p gn?

PRIMES: n for all $a \in \{2, \ldots, \sqrt{n}\}$ test $a \mid n$.

"Given n" #steps $= \sqrt{n}$

↓ ||

"in binary $\log n$" exp in the i/p representation

"Exponential" vs. poly run times (2^x, x^{100})

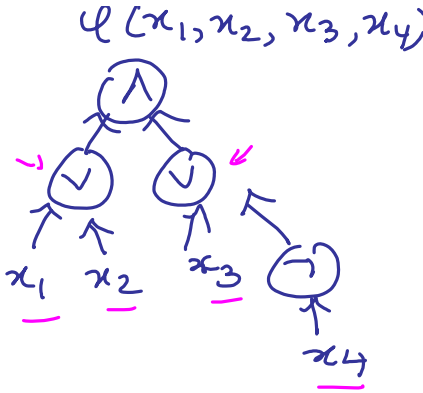
An algo. is said to be "efficient" if it runs in time poly in the i/p $\text{poly}(|x|)$ for all i/p x

"Class P": Decision problems for which an efficient algo is known.

[Agrawal, Kayal, Saxena '04] PRIMES $\in$ P, PLANARITY $\in$ P [Hopcroft, Tarjan '74]

$O(2^n \cdot |\varphi|)$ time algo.

Give me an assign $\bar{a} = (a_1, \ldots, a_n) \in \{0,1\}^n$ can decide if $\varphi(\bar{a}) = 1$ efficiently.



ANSWER is YES

If the formula φ is satisfiable, then there exist a short proof that is efficiently verifiable

If the fomula φ is unsatisfiable then no such proof exists.

"assignment"

NO

Class NP : Decision problem where the "YES" instance has a short certificate that is eff. verifiable. ↙ $A(x, c)$

"NO" instance no such certificate exists.

SATISFIABILITY $\in$ NP. , COMPOSITES $\in$ NP

Observe: $P \subseteq NP$

Open: $P \stackrel{?}{=} NP$

Suppose SATISFIABILITY $\in P$, $A(\varphi)$ can I obtain the assignment?

$\varphi(x_1, \ldots, x_n)$ → $\{0,1\}$

If φ is unsatisfiable, then say "no":

$A(\varphi) = NO$

If $A(\varphi) = YES$: For every $i \in [n]$

if " $A(\varphi(x_1 = 0, \underbrace{x_2, \ldots, x_n}_{X \setminus \{x_i\}})) = YES$ " $\alpha_1 = 0$

else $\alpha_1 = 1$

MAX-CUT in GRAPH:

G (without loops) $S, T \subset V$ $|cut| = |\{(u,v) \mid u \in S, v \in T\}|$ is max.

Brute-force: lot of time!

MAX-CUT is "NP-hard".

Given a coin (H, T)

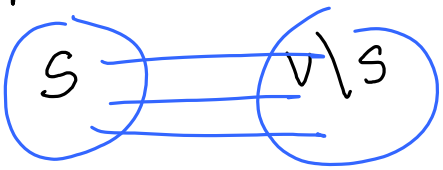
"Toss the coin" for every vertex $v \in V(G)$

if heads $v \in S$ else $v \in V \setminus S$.

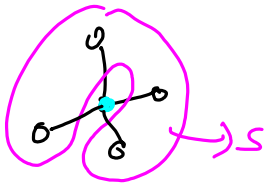
$$\mathbb{E}[|cut(S)|] = \sum_{e \in E} Pr[e \text{ is in the cut}]$$

$$= \frac{|E|}{2} \geq \frac{OPT\text{-}CUT}{2}$$

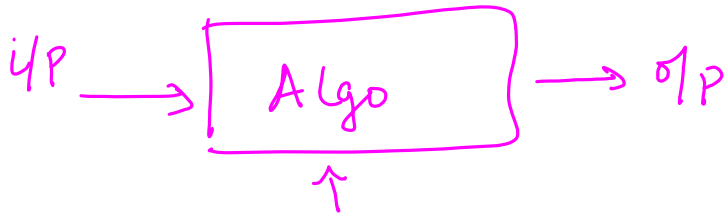
$V(G) = \{v_1, \ldots, v_n\}$



MAX-CUT $\leq |E|$



Randomized Algo



- There could be errors
- Same i/p given several times could produce diff. answers.

POLYNOMIAL IDENTITY TESTING: p, q, decide if $p - q \equiv 0$?

Given $p(x_1, \ldots, x_n)$ deg d decide if $p \equiv 0$?

$(a+b)^2 = a^2 + 2ab - b^2$

[Schwartz – Zippel, Demillo, Lipton] Given $p(x_1, \ldots, x_n)$. deg d . Let $r_i \in_R \{1, \ldots, 3d\}$

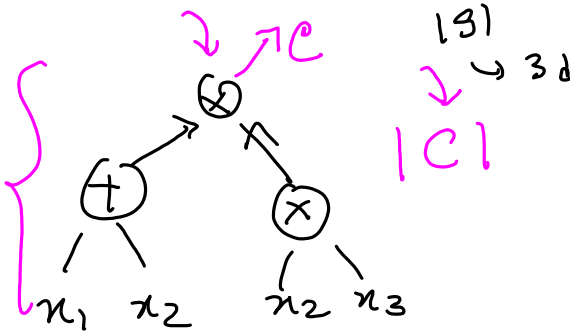
$$\Pr_{\underline{r}} \left[p(r_1, \ldots, r_n) = 0 \right] \leq \frac{1}{3}$$

i/p: $p(x_1, \ldots, x_n)$ deg d

$p \equiv 0 \Rightarrow \Pr[\text{Alg} = \text{YES}] = 1$

$p \not\equiv 0 \Rightarrow \Pr[\text{Alg} = \text{NO}] \geq 2/3$

} Probabilistic algo. poly-time



- Error reduction by repetition

Class BPP : Decision problems (poly-time) for which there is a prob. poly. time algo A

bounded error, probabilistic

s.t. $\forall$ i/p x :

x is YES instance : $Pr[A \text{ o/p's } YES] \geq 2/3$ (= 1)

x is NO instance : $Pr[A \text{ o/p's } YES] \leq 1/3$ (= 0)

$P_{IT} \in BPP$.

$P \subseteq BPP$

Open: $P \stackrel{?}{=} BPP$

ramyac@imsc.res.in