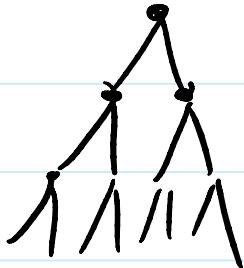


Alg. PROBABILISTIMonte Carlo

$$x \in L \rightarrow \Pr \{ A(x) = \text{YES} \} \geq 2/3$$

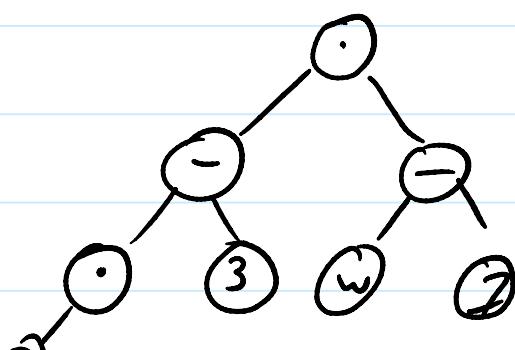
$$x \notin L \rightarrow \Pr \{ A(x) = \text{YES} \} \leq 1/3$$

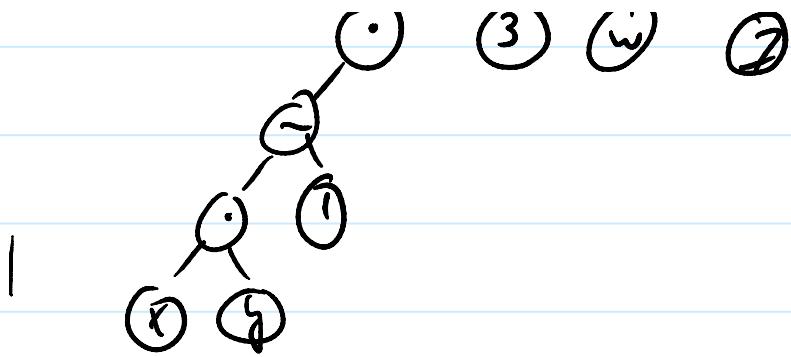
NP $x \in L \Leftrightarrow \Pr \{ A(x) = \text{YES} \} > 0$

Example Polynomial Identity Testing

So far Non-polynomial P, Q .

$$P = ((xy - 1) \cdot (zt + 1)) - 5 \cdot (vw - 7)$$





De obig Este $P = Q$?

LEMA LUI SCHWARTZ - ZIPPEL

Fie $p(x_1, \dots, x_n)$ un polinom de grad $\leq d$

Fie S o multime cu m elemente

Dacă $p(x_1, \dots, x_n) \neq 0 \Rightarrow \Pr_{z \in S} \{ p(z) = 0 \} \leq \frac{d}{m}$

$BPP = \{ L \mid \text{existe o Mașină Turing probabilistică cu complexitate polinomială}$

$$\left(\#x \mid T_M(x) \leq g(|x|) \right)$$

polinom

$x \in L \Rightarrow \Pr_M \{ M(x) \text{ acceptă} \} \geq 2/3$

$x \notin L \Rightarrow \Pr_M \{ M(x) \text{ acceptă} \} \leq 1/3$

(1) a/j. probabilități folositorii

(2) $P \subset BPP$

... 1 ... 0 1 0 1 0 1 0 1

(2) $P \subset BPP$

Probabil $BPP \not\subset NP$

Probabil $SAT \not\subset BPP$

$BPP \subset Z_2^P$

Alg. approximation $A \rightarrow f \geq 1 \quad f \in \sup_x \frac{C_A(x)}{C_{OPT}(x)}$

Exemplu VC are alg 2-approxim.

Teorema PCP

probabilistically checkable proofs

IDEE NP

G graf Hamiltonian $\rightarrow \exists C$ un circuit Hamiltonian
 $\in G$

" C este circuit Hamiltonian în G " $\rightarrow P$

Vizionare foarte încărcată de certificat pt x
care să răspundă numărul de toti hotărîrii lui y .

$L \in NP \Leftrightarrow$ există un predicat $f(., .)$

calculabil de o masină Turing
probabilistică care răspunde
în timp polynomial.

(1) y este pt $x \Rightarrow \Pr \{ M(x, y) \text{ accepte} \} = 1$

(2) y nu este multă pt $x \Rightarrow \Pr \{ M(x, y) \text{ accepte} \} \leq 1/3$

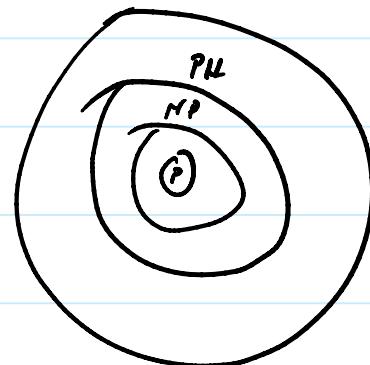
(3) M folosește $O(\log n)$ spațiu $n = |x| + |y|$

și acceptă $O(1)$ h.f.t. și încă y

Clasă de complexitate în P

PSPACE

NL (nondeterministic logspace)



Probleme Se dă $G = (V, E)$

graf orientat

Să dan $s, t \in V$

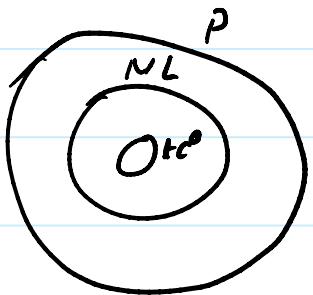
De decis $s \xrightarrow{*} t$ în G

Alg care ghiceste în drum de la s la t

și verifică dacă $s \in S_i \rightarrow S_i \ni t$

pot fi implementat ca să folosească spațiu $O(\log(n))$

$NL = \{ A \mid \text{există o mașină Turing nondeterministică cu spațiu } O(\log(n)) \text{ care decide pe } A \}$



STCONN cea mai grea
problemă NL

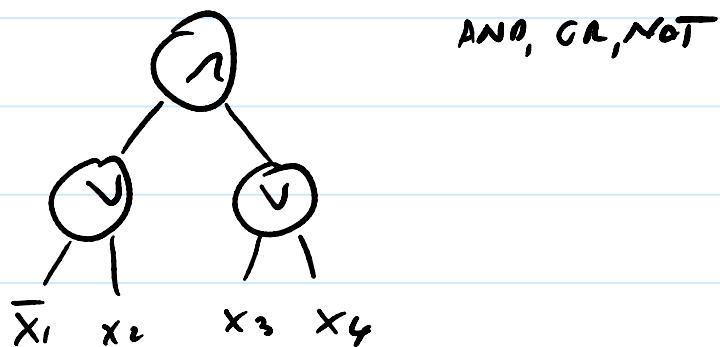
\leq_m^L , completă pt NL

COMPLEXITATEA CIRCUITELOR BOOLEENE

$$f: \{0,1\}^n \rightarrow \{0,1\}$$

Ex $f(x_1, \dots, x_n) = x_1 \oplus x_2 \oplus \dots \oplus x_n$ paritate

Circuit Boolean

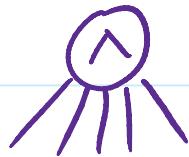


$$c(f) = \# \text{ pari}$$

(T) SHANNON Aproxima toate funcțiile booleene $f: \{0,1\}^n \rightarrow \{0,1\}$
nu pot fi calculate de circuite
 $c_n \leq 2^n / n$ pari

Nu stiu niciun exemplu concret de functie booleană care să necesite $\geq \ln$ parti (3.017)

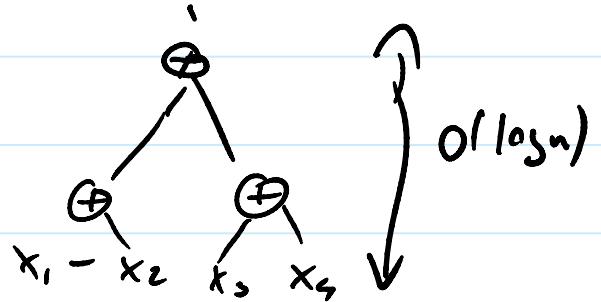
Constrângeri înaltine circuitului să fie $\Omega(1)$
Suplimentare din vîrte AND_n , OR_n



$AC^0 = \{ f \mid f \text{ calcolată de circuit boolean}$
 cu - adâncime $O(1)$
 - #parti poly(n) }

$\bigoplus_{(H, S, A)} \text{PARITY} \notin AC^0$

$x_1 \oplus \dots \oplus x_n$



UNDE E IMPORTANȚA COMPLEXITATEA?

1. Criptografie

Functii one way si criptosisteme cu chei publice

functie one way

functie one way

f waar de calmet
geen die inverset

$$x \rightarrow f(x) = y \text{ waar}$$

$$y \rightarrow x \text{ geen'}$$

Exp p_1, p_2 nr prime $\rightarrow n = p_1 \cdot p_2$

$n \rightarrow p_1$ geun (FACTORING)

CRIPTATE aan novele de n

DECRYPTATE aan novele de p_1, p_2

ZERO KNOWLEDGE

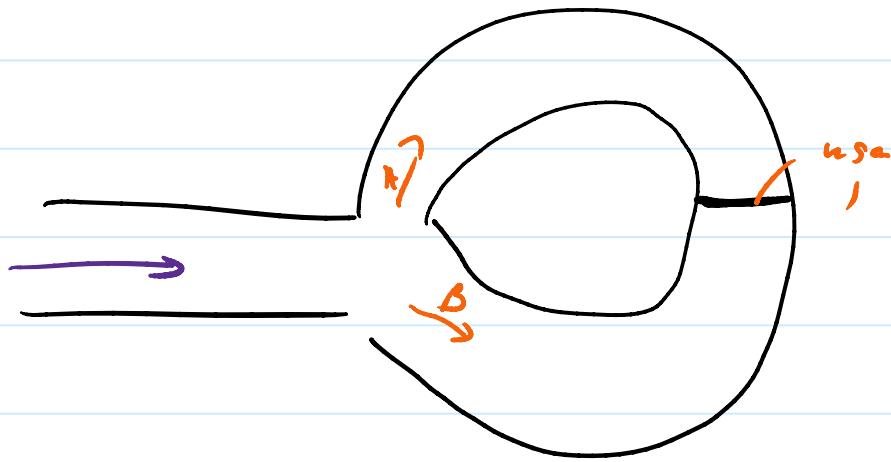
Protocol case

- converge un verifice că ştiu un secret

- VERIFIER 'n / un invito numic

din secretele mea urind protocolele

Pp există o năjă pt ca ce să o deschid am novele
să ştiu un secret.



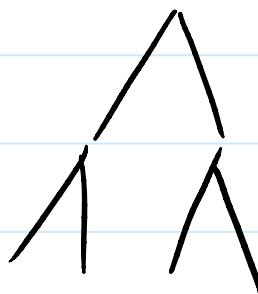
- introducă probabilitatea de intereseaza A sau B
- verificați dacă este la distanță de A sau B

Differential Privacy

În vrem ce datele noastre să potă fi revelate
facând calculări bazate pe atributări ale unui grup cunoscut
în apărare

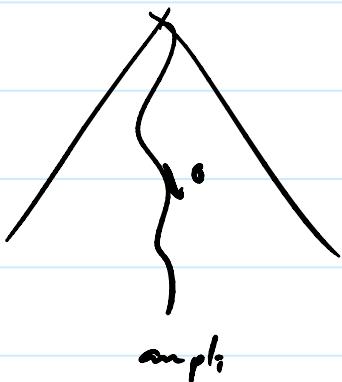
CALCUL QUANTIC

probabilități
calculare ușoară



"dăunătorii" cu amplitudini complexe

$$\alpha \sigma + \beta \Rightarrow \alpha, \beta \in \mathbb{C}$$



$$\Pr \{ \text{event} \} = \| \cdot \| ^2$$

\mathbb{T} (shor) FACTOLING

paste fi rezolvate
în timp polynomial
pe un calculator cuantic.

\mathbb{T} (error)



CUANTIC $x \rightarrow O(\sqrt{n})$ operatii

REALITATE 1000 hrti

$n = \text{echilibrul sodecăză}$

evidență pt faptul că NL putem rezolva pb NP-complet în timp polynomial cu alg. cuantici