CURS 11

UNDE SUNTEM ▯ IND. SET NP-completă

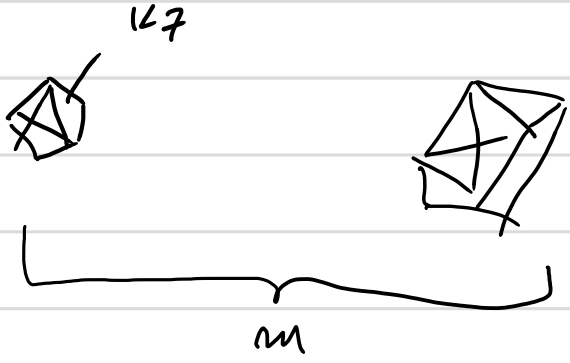
IS Se dau $G=(V,E)$, $1 \le k \le n$

DECIDE există k vf $v_1, \dots v_k$

$v_i \neq v_j$

$3\text{-SAT} \le^P_m IS$

$\phi = \bigwedge_{j=1}^{m} C_j$ m variabile



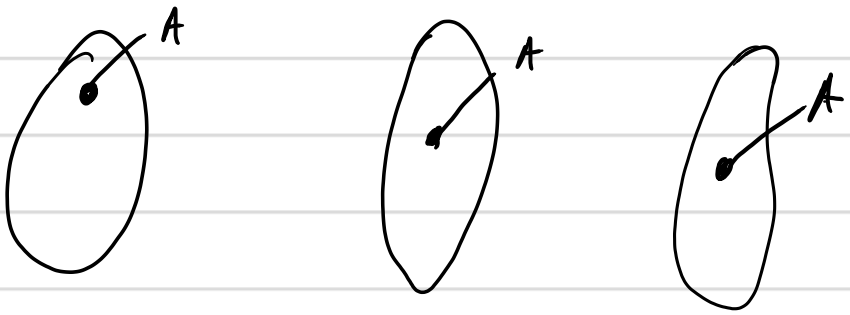
$C = x \vee y \vee z$

$(x=0, y=1, z=1)$

G_ϕ

$\phi \in SAT \iff G_\phi$ are un IS cu m vf.

$\Rightarrow$) $A \models \phi$



$\Leftarrow$) IS cu m vf ia exact 1 vf din fiecare cluster.

CLIQUE NP-complete

Se dau $G = (V, E)$ $1 \leq k \in \mathbb{N}$

De dacă Conține G o clică cu k vf?

$v_1, \ldots v_k$

$\forall i, j \; v_i \sim v_j$

VERTEX COVER NP-complete

Se dau $G = (V, E)$, $1 \leq k \in \mathbb{N}$

De dacă există k vf $v_1, \ldots v_k$

a.î. $\forall e \in E$ $left(e) \in \{v_1 \ldots v_k\}$ sau $right(e) \in \{v_1, \ldots v_k\}$

$IS \leq_m^P VC$

$(G, k) \longrightarrow (G', k')$

$G' = G$

$k' = n - k$

$S \subseteq V$ este IS in G

$\Updownarrow$

$V \setminus S$ este VC in G

⊠

retrospectivă

P (alg. eficienți)

2-SAT

G are un cuplaj perfect

PRIMES

NP-complete zeci de mii

SAT, 3-SAT, etc

Ham Cycle, TSP

neaunoscut GI $O(n^{\lg n})$

FACTORING

Primes Se dă: întreg X în binar.

De decis Este X prim sau nu?

$n = |X|$ Alg ușual → EXPONENȚIAL!

(2002) AGRAWAL, SAXENA, KAYAL (?)

CRIPTOGRAFIE — FUNCTII ONE WAY

$x \longrightarrow f(x)$ usor

$\longleftarrow$ greu

WORST CASE $\longrightarrow$ MURPHY'S LAW

- usor din p.d.v matematic. ✓
- alg eficient $\Rightarrow$ eficient în practică ✓

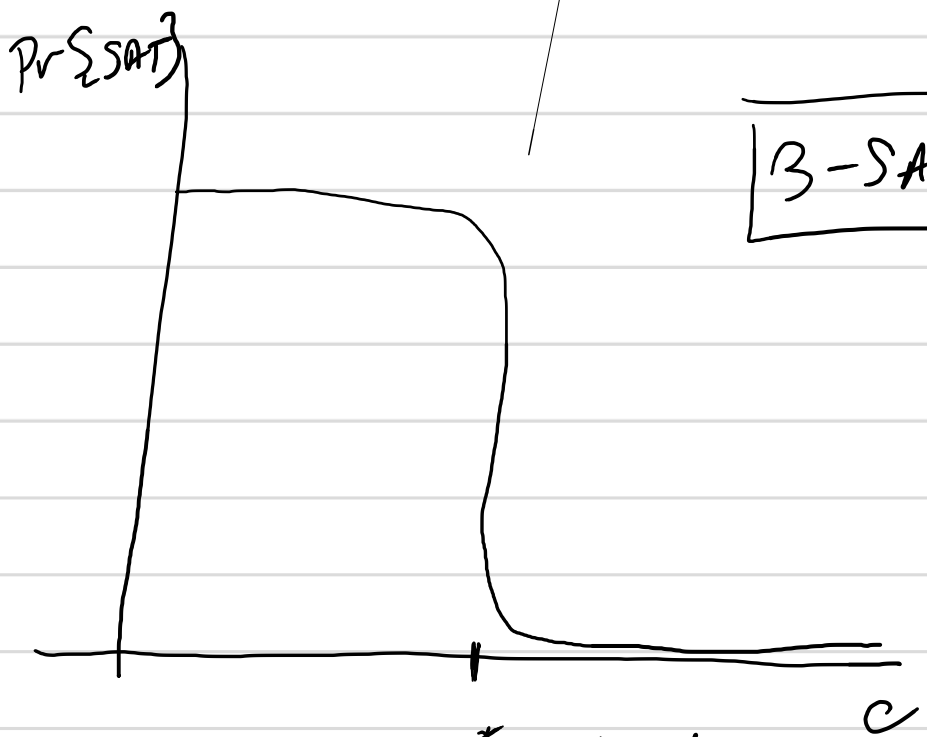
DEZAVANTAJ Pb grea în teorie $\not\Rightarrow$ Pb grea în practică

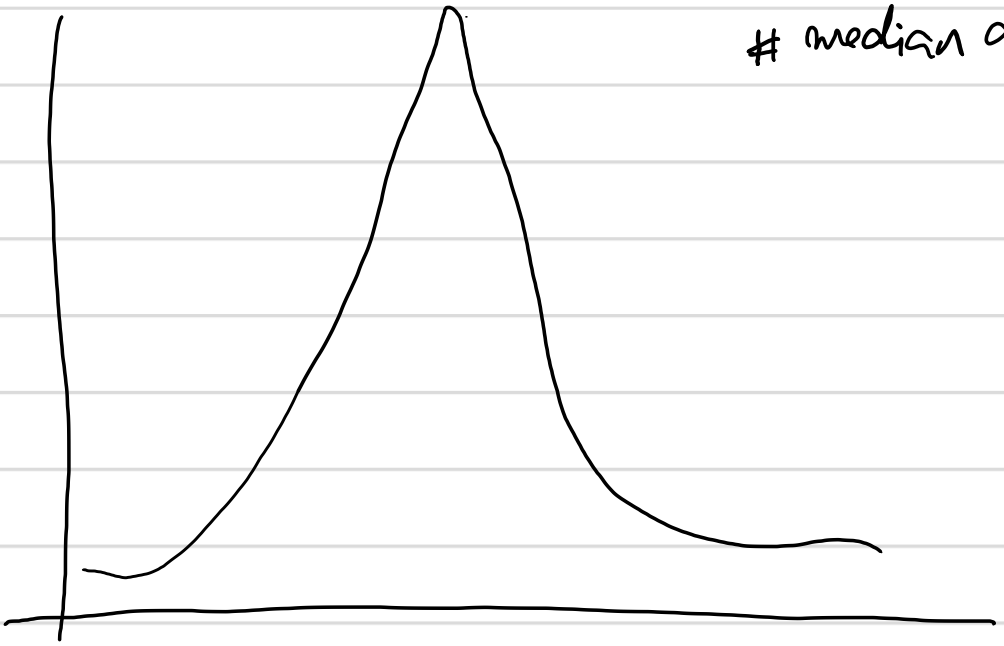
Pb NP-completă $\rightarrow$ unele instanțe sunt dificile.

3-SAT generez formule la întâmplare.

$$c = \frac{\#\text{ clauze}}{\#\text{ variabile.}}$$

$c \nearrow \Rightarrow$ Pr{SAT} $\searrow$

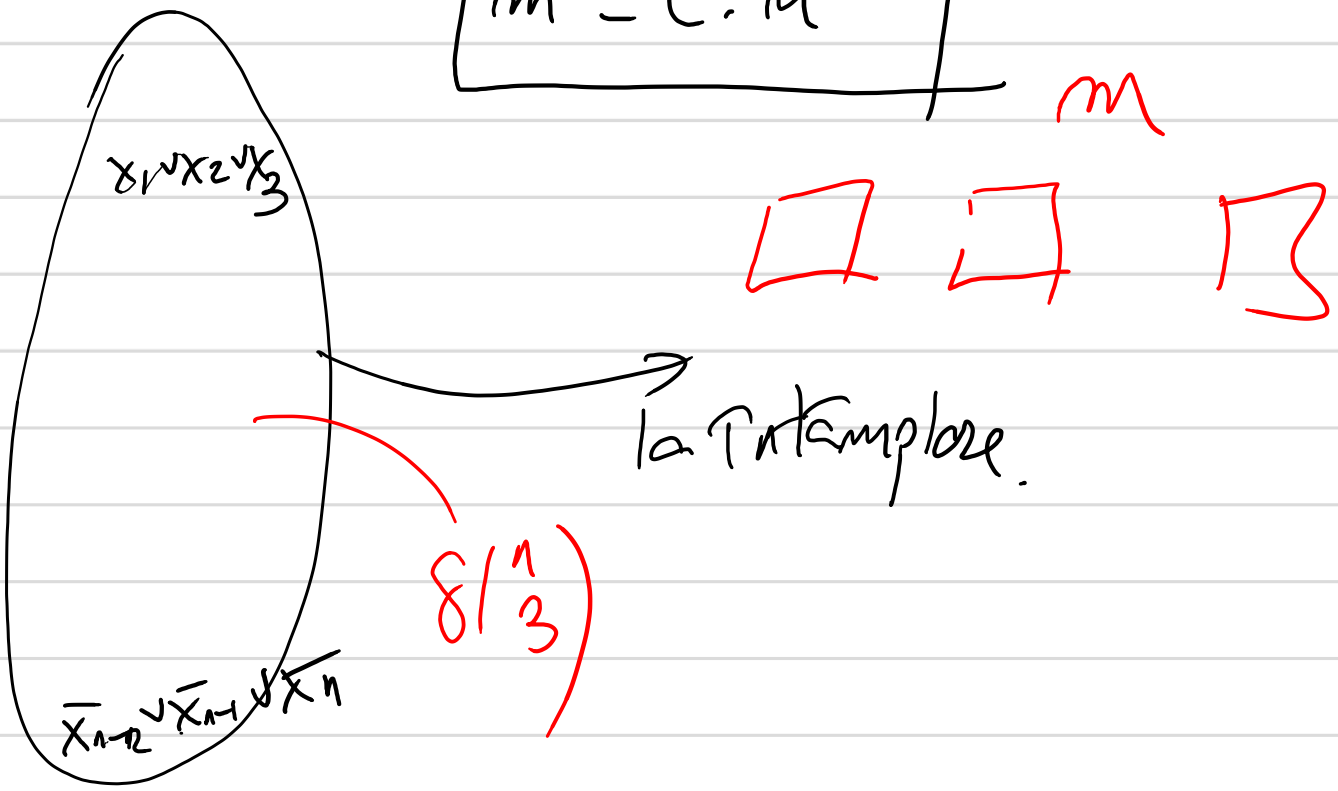




C

n = nr variabile $\quad \phi = \bigwedge_{i=1}^{m} C_i$

$m = C \cdot n$



DPLL — Davis Putnam

backtracking + { Loveland, Longman }

regula

- unit clause $\quad \phi = \phi' \wedge \{x\}$

$\Downarrow$

x = TRUE

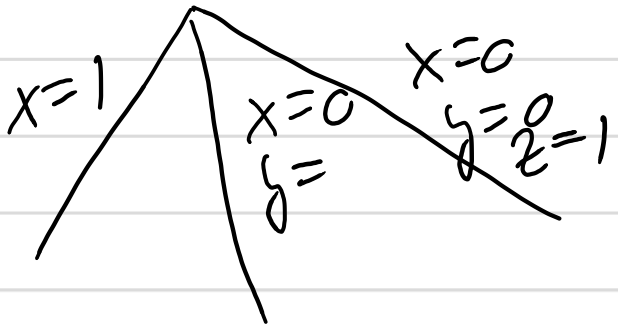
- pure literal apare cu aceeași polaritate.

x pozitiv în ϕ $\Rightarrow$ x = TRUE

EXEMPLU ALG de TIP DPLL

MONIEN-SPECKERMEYER

$C = x \vee y \vee z$



Assignment partial AUTARK

⇓

satisface toate clauzele în care apar var. setate.

Prima pas → verific AUTARK.

(~2012) DELACOLIKAR P ≠ NP cu tr. fază NU!

fizicieni → METODE NERIGUROASE pt analiza pb. combinatoriale

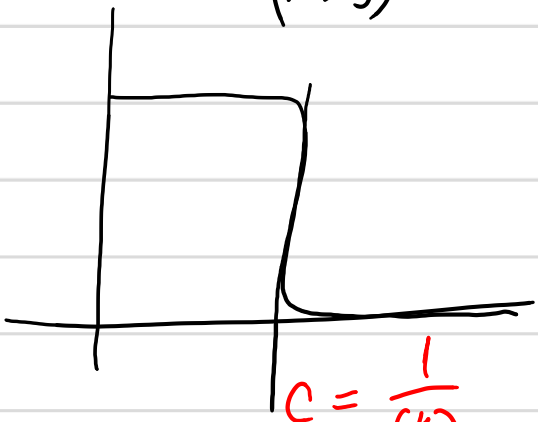
{2022} GIORGIO PARISI → premiul NOBEL

EXEMPLE 2-SAT

$C = 1$

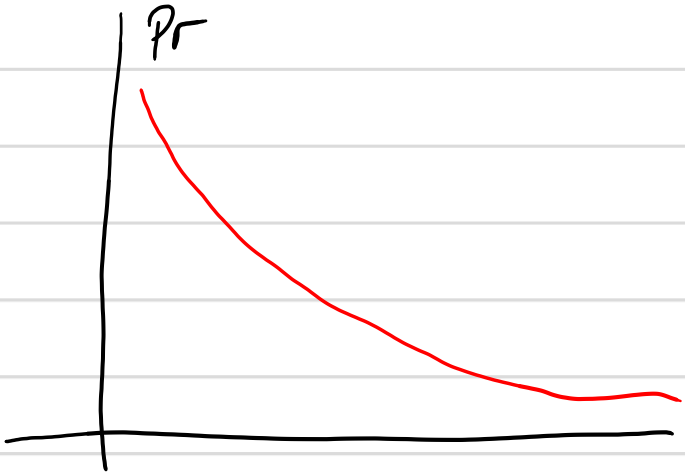
1-IN-K SAT

$(k \geq 3)$



$C = \frac{1}{\binom{k}{2}}$

Pb ferE TR. fază



HORN-SAT

K-SAT → 2022 ANNALS OF MATHEMATICS

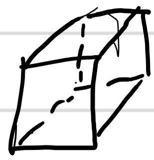
$(k \geq 3)$

C_k cunoscut (~70 pagini)

3-SAT $C_* \sim 4.24$ UB
LB

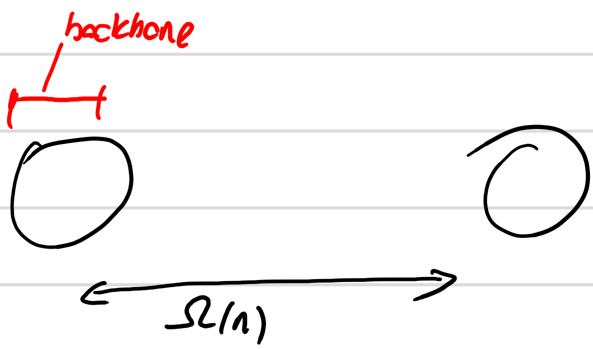
INTUITIE "FIZICA"

Sol. unei formule $A \in \{0,1\}^n$



A, B vecine $d_H(A,B) \le C \cdot \log(n)$

CLUSTERE de soluții



PB NP-complete
care este usoara
"aproape peste tot"

1-in-k SAT ~ 2-SAT
NP-complete (P)

Data viitoare SAT solvere.

PROOF COMPLEXITY $\phi \in \overline{SAT}$

REZOLUTIE

$$\frac{C_1 \vee x \qquad C_2 \vee \overline{x}}{C_1 \vee C_2} \qquad \frac{x \qquad \overline{x}}{\square}$$

$\phi_1, \ldots$ ϕ_m

↓

IB

↑

fie clauze ale lui ϕ

$\phi_i = REZ(\phi_j, \phi_k)$

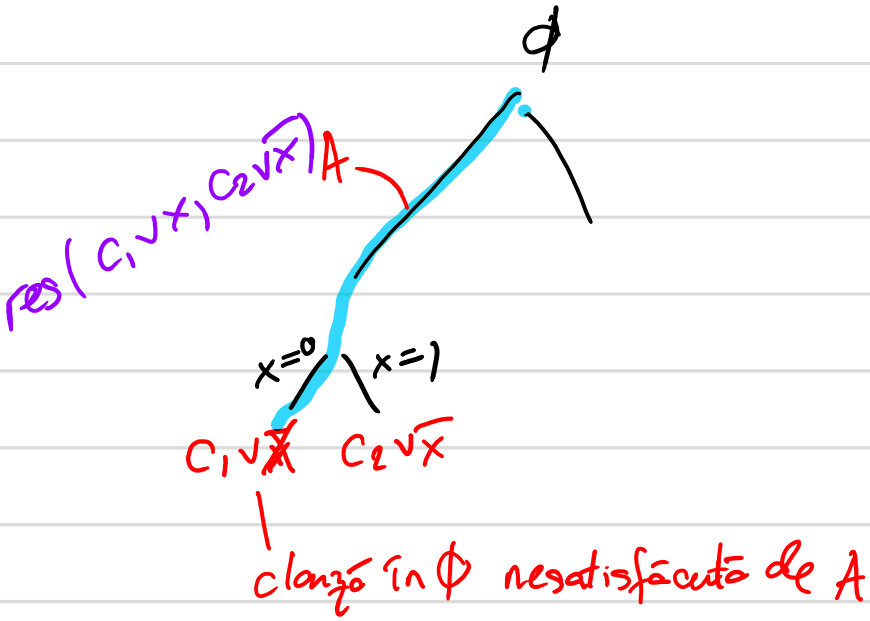
$(j, k < i)$

clauze într-o dem prin rezoluție pt $\phi \in \overline{SAT}$

||

$Ros(\phi)$

Alg DPLL $\phi \rightarrow$ dem res prin rezoluție



clauză în ϕ nesatisfăcută de A