

## SAT

Odločitelni problem:

$S$  množica (grafi, števila, matrice, ...)

$D \subseteq S$  (povezani grafi, pravi števila, obratljiva, ...)

Odločitelni problem: ali dani  $x \in S$  pripada  $D$ ?

1) Kako predstavimo elemente  $S$  s pod. strukturo?

2) Algoritem:

VHOD:  $x$

IZHOD:  $\begin{cases} \text{True} & x \in D \\ \text{False} & x \notin S \end{cases}$

## SAT

Ali je dana Boolova formula  $\varphi$  izpolnljiva?

Ali obstaja valuacija  $x_1 \mapsto \perp$  pri kateri je  $\varphi$  enaka T?  
 $x_2 \mapsto \top$   
 $\vdots$   
 $x_n \mapsto \perp$

Algoritem: preizkusimo vse valuacije.

Če imamo  $n$   $\varphi$  spremenljivke  $x_1, \dots, x_n$ ,  
 je različnih valuacij  $2^n$ .

Časovna zahtevnost:  $O(2^n)$  kjer je  $n$  število spremenljivk

$$O(2^{|\varphi|})$$

$|\varphi|$  velikost  $\varphi$   
 ||  
 $m$

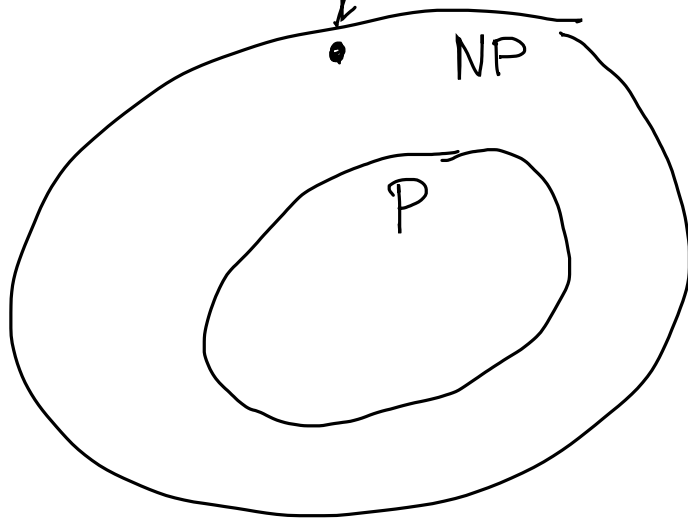
## NP poln

P

odgovor znammo poiskati v času  $O(p(n))$   
 "lahki"  $\uparrow$  polinom

NP

problemi, kjer lahko hitro pravinimo rešitev  
 $\uparrow$  v polinomskem času



$$P \subseteq NP$$

Problem D je poln, če  
 lahko vsak drug problem  
učinkovito prevedemo na D.

## SAT je NP-poln

1) SAT  $\in$  NP

Ali lahko odgovorimo na vprašanje

"Ali je  $\varphi$  izpolnljiva?"

$\varphi \in \text{SAT}$ ?

Če dobimo ustrezan nasvet?

NASVET: naloga, mi hitri je  $\varphi$  resnična. ✓

2) Vsaki  $D \in \text{NP}$  lahko prevedemo na SAT,

Ideja: obstaja Turingov stroj  $T$ , ki ~~reši~~ reši  $D$  s pomočjo nasveta v času  $p(n)$  polinom

Delovanje stroja  $T$  opišemo z Boolovo formulo  $\varphi_T(x)$  tako, da je  $\varphi_T(x) \in \text{SAT} \iff$  odgovor na " $x \in D$  je da".

### Primer prevedbe na SAT

3COL : Dan je graf  $G = (V, E)$ . Ali lahko vozlišča pobarvamo s tremi barvami tako, da sta vsaki dve sosednji vozlišči različnih barv?

$V = v_1, \dots, v_n$  vozlišča barve 1, 2, 3

$\{v_i, v_j\} \in E$  -----  $v_i$  in  $v_j$  sta povezani

Spremenljivke:

$C_{i,k}$  za  $i = 1, \dots, n$ ,  $k = 1, 2, 3$  vozlišče  $v_i$  je barve  $k$

**3COL**  
 $\left( \bigwedge_{i=1}^m (C_{i,1} \vee C_{i,2} \vee C_{i,3}) \right) \wedge$  vsak  $v_i$  je pobarvan z naj eno barvo

$\left( \bigwedge_{i=1}^m \bigwedge_{1 \leq k < l \leq 3} \neg (C_{i,k} \wedge C_{i,l}) \right) \wedge$   $v_i$  ni hkrati pobarvan z dvema barvama

$\bigwedge_{\{v_i, v_j\} \in E} \neg \left( \bigwedge_{k \in \{1,2,3\}} C_{i,k} \wedge C_{j,k} \right)$

povezani vozlišči  $v_i$  in  $v_j$   
 nista iste barve

$$n = |V|, \quad m = |E|$$

Število spremenljivk:  $3n$

Velikost formule:  $3n + m \cdot 3 \cdot 2 + m \cdot 3 \cdot 2$

$$O(m+n) = O(|V| + |E|)$$

Povezanost

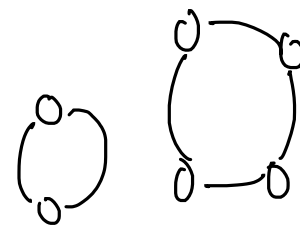
$$G = (V, E)$$

Ali je  $G$  povezan?

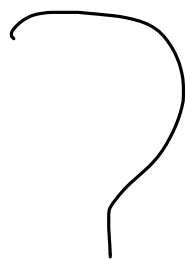
1) Ugotovimo v linearnem času, ali je  $G$  povezan.

Če je povezan: formula  $T$

Če ni povezan: formule  $1$



To je cikel!



a

Zakaj je to med najlažji?

## Sudoku

1) Prevedemo na barvanje grafe z 9 barvanji.

Vozlišča: kvadrati (81 vozlišči)

Povezave: kvadrati povežemo kadar sodelujeta  
v skupni vrstici, stolpcu ali 3x3 kvadratu.

Zapolnjeni kvadrati?

AP

"Se da pobavati z 9 barvanji"

2) Brute force:

Spremenljivke

$X_{i,j,k}$

$i, j, k \in \{1, 2, \dots, 9\}$

polje  $(i, j)$  vsebuje število  $k$



## Sudoku formula

$$\left( \bigwedge_{i,j=1,\dots,9} \bigvee_{k=1,\dots,9} X_{i,j,k} \right) \wedge$$

$(i,j)$  je ~~zapoljen~~ ni prazen

$$\left( \bigwedge_{i,j=1,\dots,9} \bigwedge_{1 \leq k < l \leq 9} \neg (X_{i,j,k} \wedge X_{i,j,l}) \right) \wedge$$

$(i,j)$  ni zapoljen dvakrat.

brava se ne pomori v  
stolpcu, vrstici ali  $3 \times 3$

$\wedge$

Začetno stanje:

Na kvadratu

$(a_i, b_i)$  je upisan  $k_i$   
pri čemer  $i = 1, \dots, m$

$$\bigwedge_{i=1,\dots,m} X_{a_i, b_i, k_i}$$

## Hadamardova matrika

Spremenljivke:

$$X_{i,j} \quad i, j \in \{1, \dots, n\}$$

$$X_{i,j} = \begin{cases} 1 & \text{če je polje } (i,j) = 1 \\ -1 & \text{če je polje } (i,j) = -1 \end{cases}$$

Formula:

$$\begin{array}{c} \triangle \\ 1 \leq i < j \leq n \end{array}$$

"Skalarni produkt  $i$ -te in  $j$ -te vrstice = 0"

NOVE SPREMENLJIVKE ZA

RACUNANJE SKALARNEGA PRODUKTA?

za  $i$ -to in  $j$ -to vrstico