RECAP

- COOK'S THEOREM: $BCSAT \in NPH$
  - "simulate" $V_L(x, y)$ with $C_{V_L,x}(y)$

A certificate y_x for $x \in L$ becomes a ~~satisfying~~ assignment for $f(x) = \langle C_{V_L,x}(y) \rangle$

- FORMULA SATISFIABILITY (SAT):

  $BC\text{-}SAT \leq_p SAT$:

  - Trivial reduction based on subexpressions not ptc (poly-time computable)

We need a more sophisticated approach!

$C = (I \cup G \cup \{o_y\}, W)$

x_i ← I; y_g $\forall g \in G$ ← G; y_o ← $\{o_y\}$

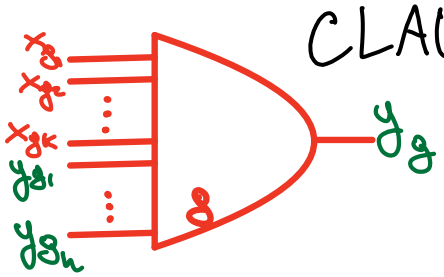
New variables $y_g : g \in G$

We add extra variables y_g associated to the gates, describing the output of each gate $g \in G$ and create a formula that reflects valid configurations of the circuit

RECALL: A configuration is the set of all bits on the wires under a valid switching of the circuit: $(\vec{b}_x, \vec{b}_y)$

$\vec{b}_x$ ← x; $\vec{b}_y$ ← y (gate outputs)

For each gate $g \in G$ we introduce a sub-formula Γ_g describing the input-output relation of the gate:

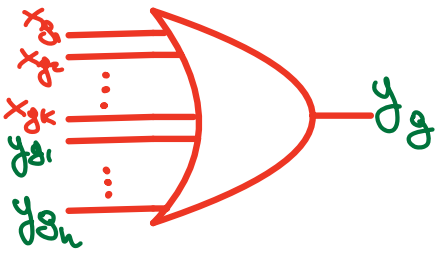


CLAUSE

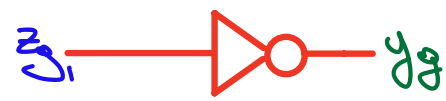
"equation"

$\Gamma_g : y_g \leftrightarrow x_{g,1} \wedge \dots \wedge x_{g,k} \mid y_{g,1} \wedge \dots \wedge y_{g,h}$

input di circuito | output di altri gate



$\Gamma_g : y_g \leftrightarrow x_{g,1} \vee \dots \vee x_{g,k} \vee y_{g,1} \vee \dots \vee y_{g,h}$



$\Gamma_g : y_g \leftrightarrow \neg(z_{g,1})$

Observe that subexpression Γ_g is true under a truth assignment $\Leftrightarrow$ y_g is assigned the correct output value w.r.t. the values assigned to the gate's inputs

We can then obtain the formula

$$\psi(\vec{x}, \vec{y}) = \bigwedge_{g \in G} \Gamma_g$$

Formula ψ describes a configuration of the circuit C:

$\psi(\vec{b}_1, \vec{b}_2) = 1 \Leftrightarrow$ the values of the outputs of the gates of $C(\vec{b}_1)$ are $(b_2)_g : g \in G$

$\Leftrightarrow (\vec{b}_1, \vec{b}_2)$ is a valid configuration

non basta ψ per riduzione $\Rightarrow$ formula sempre satisfiable

OBSERVATION: $\psi(\vec{x}, \vec{y})$ is always satisfiable (HOMEWORK: how many satisfying assignments?)

We have that $\boxed{|\langle \psi(\vec{x}, \vec{y}) \rangle| = \Theta(|\langle C(\vec{x}) \rangle|)}$

since each subexpression uses a number of symbols linear in the size of the corresponding gate!

The reduction function f uses ψ as follows:

$$\boxed{f(\langle C(\vec{x}) \rangle) = \phi_C(\vec{x}, \vec{y}) \cdot \psi(\vec{x}, \vec{y}) \wedge y_0}$$

y_0: variable associated to gate of output wire

$$\boxed{|\langle \phi_C(\vec{x}, \vec{y}) \rangle| = \Theta(|\langle \psi(\vec{x}, \vec{y}) \rangle|) = \Theta(|\langle C(\vec{x}) \rangle|)}$$

thus f is ptc

We are left to prove that

$x \in L_1 \Leftrightarrow f(x) \in L_2$

$\begin{cases} x \in L_1 \Rightarrow f(x) \in L_2 \\ f(x) \in L_2 \Rightarrow x \in L_1 \end{cases}$ OR $\begin{cases} x \in L_1 \Rightarrow f(x) \in L_2 \\ x \notin L_1 \Rightarrow f(x) \notin L_2 \end{cases}$ difficoltà dipende dal caso

$\langle C(\vec{x}) \rangle \in$ BC-SAT $\Leftrightarrow f(\langle C(\vec{x}) \rangle) = \langle \phi_C(\vec{y}) \rangle \in$ SAT

$\Rightarrow$ If $\langle C(\vec{x}) \rangle \in$ BC-SAT then $\exists \vec{b}_1 \in \{0,1\}^n : C(\vec{b}_1) = 1$

Consider the configuration of the circuit under $\vec{b}_1$, and let $\vec{b}_2$ be the values carried by the wires of the outputs of the gates

We have $\psi(\vec{b}_1, \vec{b}_2) = 1$

Moreover, since $C(\vec{b}_1) = 1$ we have $b_0 = 1$ (b_0)

$\Rightarrow \phi_C(\vec{b}_1, \vec{b}_2) = \psi(\vec{b}_1, \vec{b}_2) \wedge b_0 = 1 \Rightarrow f(\langle C(\vec{x}) \rangle) \in$ SAT

$\Leftarrow$ $f(\langle C(\vec{x}) \rangle) \in$ SAT $\Rightarrow \exists \vec{b}_1, \vec{b}_2 : \phi_C(\vec{b}_1, \vec{b}_2) = 1$

$\Rightarrow$ 1. $\psi(\vec{b}_1, \vec{b}_2) = 1$: the truth assignments represent a legal configuration $(\vec{b}_1, \vec{b}_2)$ of the circuit C

operandi di ϕ_C

$\Rightarrow$ 2. Under $(\vec{b}_1, \vec{b}_2) : b_0 = 1 \Rightarrow$ $C(\vec{b}_1) = 1$

Thus $\langle C(\vec{x}) \rangle \in$ BC-SAT

LESSON LEARNED: We have to make sure that the reduction is poly-time computable!

SIMILAR PITFALL: $f_{L' \to L}$ cannot possibly know whether $x \in L'$ or $x \notin L'$ unless $L \in P$! This is never the case if you are trying to prove that $L \in NPC$

"non si può forzare riduzioni diverse in base a $x \in L'$"

IMPORTANT

Next reduction is a special case of a large family: **reductions by restriction**
These reductions are used to prove that an NPC problem stays NPC even if we restrict the set of admissible instances

DEF Given a set of boolean variables $\{x_1, x_2, \dots, x_n\}$:

- A **literal** is either a variable x_i or its negation $\neg x_i$ ($\bar{x}_i$)
  We will use y to denote a literal

- A **clause** is a disjunction of 3 distinct literals, e.g. $C_i = x_1 \vee \bar{x}_3 \vee x_5$

- A **3-CNF formula** $\phi(x_1, \dots, x_m)$ is a conjunction of clauses built on the m variables

e.g. $\phi(x_1, x_2, x_3, x_4) = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3)$

3-CNF-SAT:

I: $\langle \phi(x_1, x_2, \dots, x_m) = \bigwedge_{i=1}^{m} C_i \rangle$, ϕ 3-CNF formula

Q: Is $\phi(\vec{x})$ satisfiable?

We will prove that **3-CNF-SAT $\in$ NPC**.

Meaning:

Even restricting the shape of the formula to a very simple one, the problem stays difficult!

3-CNF-SAT $\in$ NP (trivial, exercise)

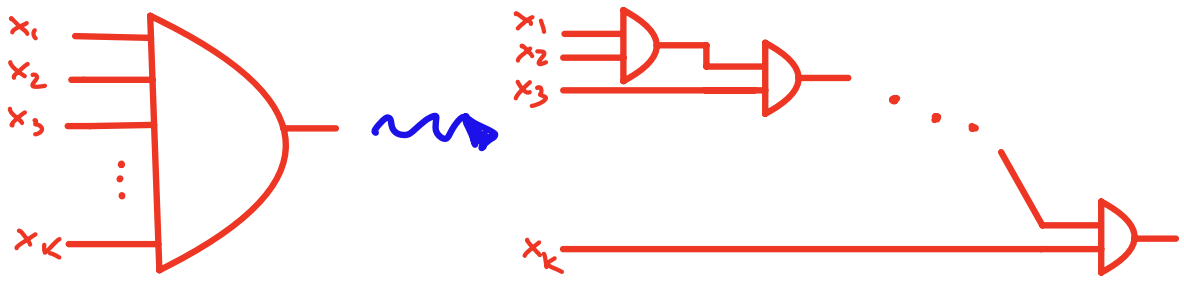
3-CNF-SAT $\in$ NPH.

può essere difficile scrivere formula in CNF

We reduce again from BC-SAT, using a similar idea to BC-SAT $\leq_P$ SAT

- PREPROCESSING STEP: We modify C to get an equivalent one:

Replace each AND or OR gate with fan-in ≥ 3 with a cascade of gates with fan-in 2, e.g.,



The resulting circuit C' is equivalent to C. Moreover $|\langle C' \rangle| = \mathcal{O}(|\langle C \rangle|)$
(# new gates $\leq$ # wires of C)

- Next, we write the formula $\psi(x,y) \wedge y_0$ as done for formula satisfiability. We have four types of subexpressions Γ:

$y_i \longleftrightarrow w_i^1 \vee w_i^2$ $\quad$ $y_i \longleftrightarrow w_i^1 \wedge w_i^2$

$y_i \longleftrightarrow \overline{w}_i$ $\quad$ w_i either x_k or y_j $\quad$ y_0

- We can re-write each subexpression as a conjunction of disjunctions:

$$y_i \longleftrightarrow w_i^1 \vee w_i^2 \equiv (y_i \vee \overline{w}_i^1) \wedge (y_i \vee \overline{w}_i^2) \wedge (\overline{y}_i \vee w_i^1 \vee w_i^2)$$

$$y_i \longleftrightarrow w_i^1 \wedge w_i^2 \equiv (\overline{y}_i \vee w_i^1) \wedge (\overline{y}_i \vee w_i^2) \wedge (y_i \vee \overline{w}_i^1 \vee \overline{w}_i^2)$$

$$y_i \longleftrightarrow \overline{w}_i \equiv (y_i \vee w_i) \wedge (\overline{y}_i \vee \overline{w}_i)$$

Equivalence verified via truth tables (HOMEWORK)

e.g.:

y_i	w_i	$y_i \to \overline{w_i}$	A: $y_i \vee w_i$	B: $\overline{y_i} \vee \overline{w_i}$	$A \wedge B$
0	0	1	0	1	0
0	1	1	1	1	1
1	0	1	1	1	1
1	1	0	1	0	0

$=$

- After this transformation, $\psi(x,y) \wedge y_0$ has been rewritten as a conjunction of disjunctive clauses - However, some of the clauses have < 3 literals!
- We add "dummy" variables to bring all clauses to 3 literals:

$$(y \vee w) = (y \vee w) \vee 0 = (y \vee w) \vee (z \wedge \overline{z}) = (y \vee w \vee z) \wedge (y \vee w \vee \overline{z})$$

(For clause y_0 repeat twice)

- We have obtained a 3-CNF-FORMULA $\phi_{C'}(\vec{x}, \vec{y}, \vec{z})$ equivalent to $\psi_{C'}(\vec{x}, \vec{y}) \wedge y_0$

$$C \in \text{BC-SAT} \Leftrightarrow C' \in \text{BC-SAT} \Leftrightarrow \psi_{C'}(\vec{x}, \vec{y}) \wedge y_0 \in \text{SAT} \Leftrightarrow \phi_{C'}(\vec{x}, \vec{y}, \vec{z}) \in \text{3-CNF SAT}$$

LESSON LEARNED: Reductions by restriction must "modify" f so that it maps into the set of restricted instances.

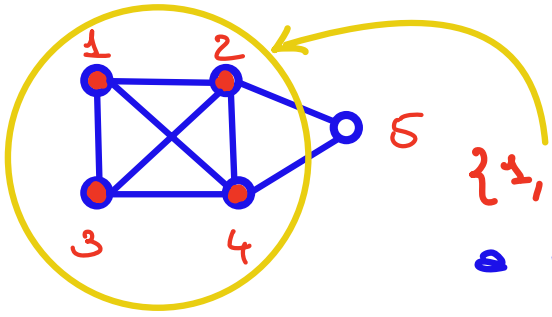
PROBLEMS ON GRAPHS

We will prove the NP-Completeness of three decision problems on graphs, related to very important optimization problems.

DEF Given $G=(V,E)$ undirected, a **clique** of size K is a subset $V' \subseteq V$ of K nodes such that each pair of distinct nodes in V' is connected by an edge (clique = complete subgraph)

$$\exists V' \subseteq V : (|V'|=K) \wedge \left(\forall u \neq v \in V : (u \in V') \wedge (v \in V') \Rightarrow \{u,v\} \in E\right)$$

EXAMPLE:



$\{1,2,3,4\}$ is a clique of size 4

We have:

CLIQUE

- I: $\langle G=(V,E), K\rangle$, G undirected graph, $1 \leq K \leq |V|$
- Q: Does G contain a clique of size K?

The optimization version of this problem requires determining the clique of max size.

QUESTION: Why doesn't the decision problem ask "size $\geq k$"? [Argue that the two questions are equivalent]

Important applications in bioinformatics, computational chemistry, social network analysis

Let's prove that CLIQUE $\in$ NPC

- 1. CLIQUE $\in$ NP trivial. Candidate certificate: set of k nodes.
  [Write $V_{CLIQUE}(x, y)$ as an exercise]
- 2. CLIQUE $\in$ NPH
  Reduction from 3-CNF-SAT.
  3-CNF-SAT $\leq_p$ CLIQUE
  known NPH candidate

We start from $\phi(x_1, x_2, \ldots, x_m) = C_1 \wedge C_2 \wedge \ldots \wedge C_m$
with $C_i = y_1^i \vee y_2^i \vee y_3^i$, $y_j^i \in \{x_k, \bar{x}_k : 1 \leq k \leq m\}$

We have to define a reduction function that takes ϕ and returns an instance of CLIQUE in poly-time:

$$f(\langle \phi(x_1, \ldots, x_m) \rangle) = \langle G_\phi, k_\phi \rangle$$

1. We set $k_\phi = m$ (# of clauses of ϕ)
2. $G_\phi = (V_\phi, E_\phi)$

V_ϕ:

(one node for each literal y_j^i $\quad 1 \le i \le m$, $1 \le j \le 3$):

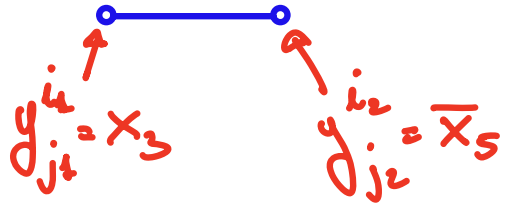
$$V_\phi = \{ v_j^i : 1 \le i \le m,\ 1 \le j \le 3 \} \Rightarrow |V_\phi| = 3m$$

E_ϕ:

$$\{ v_{j_1}^{i_1}, v_{j_2}^{i_2} \} \in E_\phi \Leftrightarrow (i_1 \neq i_2) \wedge \left(y_{j_1}^{i_1} \neq \neg y_{j_2}^{i_2} \right)$$

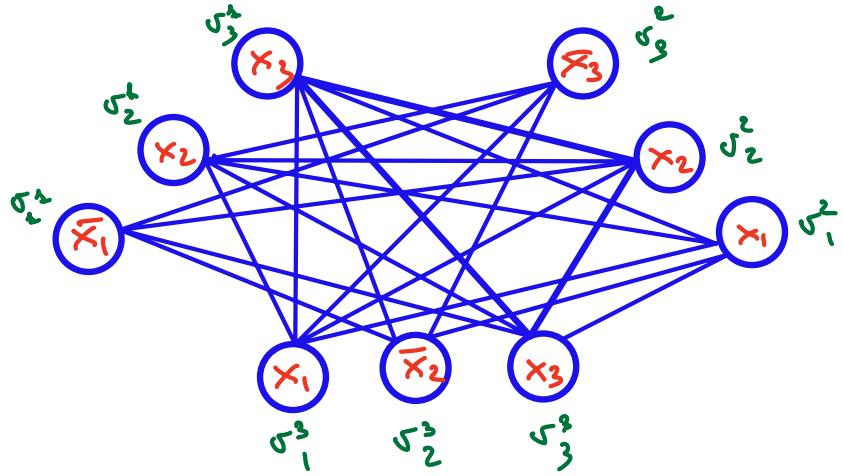
There is an edge between two nodes if their corresponding literals belong to distinct clauses and are not the negation of each other (e.g. $y_{j_1}^{i_1} = x_1$, $y_{j_2}^{i_2} = \bar{x}_1$)

INTUITION: Two literals corresponding to an edge can be made both true under the same truth assignment

e.g. 

both true if $b_3 = 1$, $b_5 = 0$

EXAMPLE: $\phi(x_1, x_2, x_3) = (\bar{x}_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee x_3)$



Running time: $\Theta(n^2) = \Theta(|\langle \phi \rangle|^2)$

Each node is compared to all other nodes to determine the edges

$\Rightarrow$ f is ptc