Théorème de Cook-Levin :

SAT est NP-complet.

① SAT $\in$ NP ✓

② SAT est NP-difficile : on montre que tout problème $A \in NP$ se réduit à SAT : $A \leq_p SAT$.

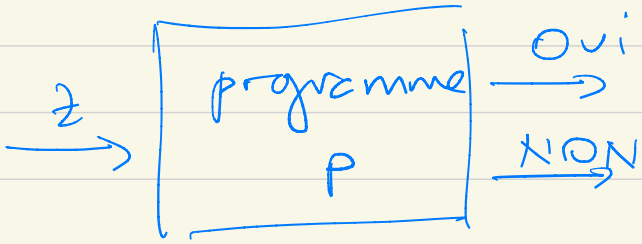
On part de la <u>déf. de NP</u> :

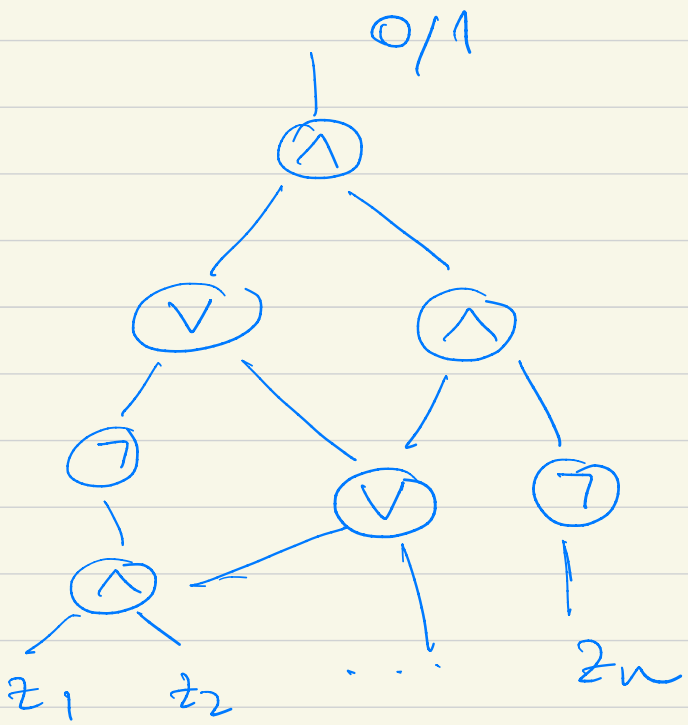
$A \in NP$ s'il existe un polynome $p(\cdot)$ et un vérificateur V poly tq.

x est instance positive de A $\Leftrightarrow$ il existe y de taille $\leq p(|x|)$ tq. V accepte $\langle x, y \rangle$

2 ingrédients dans la preuve :

1) On peut "coder" tout algorithme polynomial en circuit booléen de taille polynomiale, équivalent.





circuit booléen $C_{p,n}$

P accepte $z \iff C_{p,n}(z_1 \dots z_n) = 1$

si $T_p(n) \leq p(n)$ alors taille$(C_{p,n}) \leq q(p(n))$, q poly

z++

Ex. P : $z' := z+1$

$z = z_1 \dots z_n$

$z' = z'_1 \dots z'_n$

$z_j, z'_j \in \{0,1\}$

$z_1 = 0$

$$z'_j = \begin{cases} z_j & \text{si } \exists k \neq j \text{ tq. } z_k = 0 \\ 1 - z_j & \text{sinon} \end{cases}$$

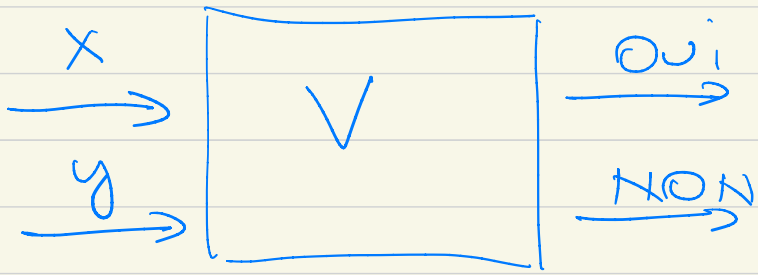
$$z'_j = (z_j \wedge \bigvee_{k>j} \neg z_k) \vee (\neg z_j \wedge \bigwedge_{k>j} z_k)$$

+1

0 1 0 | 0 1 1

0 1 0 | 1 0 0

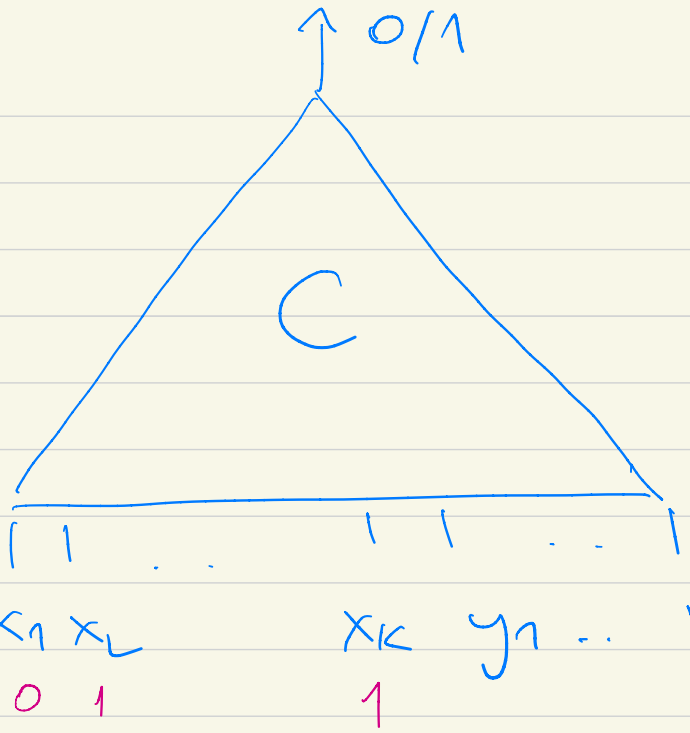
(2)



V : vérificateur, algo polynomial

(1)

circuit C de taille polynomiale en $|x|$



$x = x_1 .. x_K$, $y = y_1 .. y_m$

x instance positive de A $\Leftrightarrow$ il existe $y = y_1 .. y_m$ (m poly dans K) tq. C retourne 1 sur $\langle x, y \rangle$.

La question ci-dessus se réduit donc à la question suivante pour le circuit C :

Supposons que le circuit C est donné, ainsi que $x = x_1 .. x_k$.

On veut savoir s'il existe une valuation de $y = y_1 .. y_m$ tq.

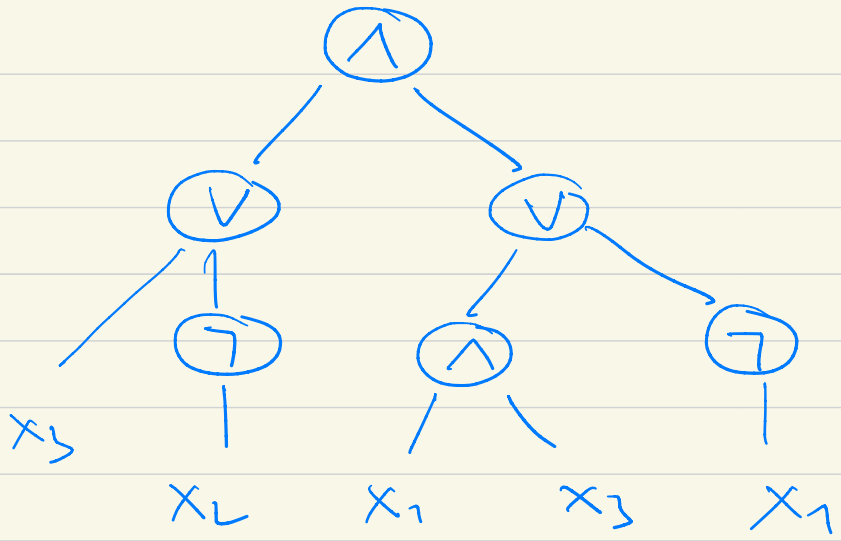
$$C(x, y) = 1.$$

Si la valuation de x est donnée, on peut remplacer les x_i par leurs valeurs, et on obtient un circuit $C'(y_1, .., y_m)$ en simplifiant.

La question devient : est-ce qu'il existe $val : \{y_1, .., y_m\} \to \{0, 1\}$ tq. C' est satisfait par val ?

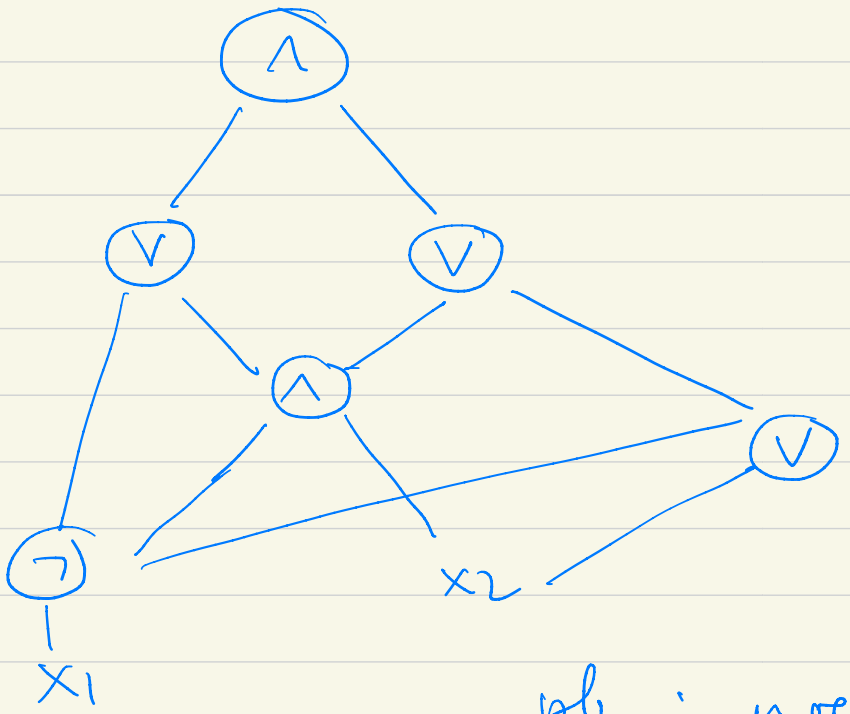
" C' s'évalue à 1 "

Ex.



Simple, ceci est une instance de SAT !

$$(x_3 \vee \neg x_2) \wedge ((x_1 \wedge x_3) \vee \neg x_1)$$



?

pb. : noeuds partagés

Le pb. auquel on s'intéresse est **Circuit-SAT** :

Entrée Circuit booléen C avec variables $y_1, \dots, y_m$

Q : Est-ce qu'il ex. une valuation $val : \{y_1, \dots, y_m\} \to \{0,1\}$ tq. C sous val est 1 ?

! On a réduit la question "x instance positive de A?" à une question de Circuit-SAT.

On montre :

$$\text{Circuit-SAT} \leq_p \text{SAT}$$

Soit C circuit booléen; on note par N les noeuds de C.

$C(y_1, .., y_m)$: y_i variables de C

On va rajouter des variables booléennes, une pour chaque noeud de C :

$n \in N \longrightarrow x_n$ var. booléenne

On construit une formule booléenne avec variables $\{ y_i : 1 \le i \le m \} \cup \{ x_n : n \in N \}$

On distingue le type de $n \in N$:

1) n feuille (étiquetée par un y_j)

$\longrightarrow$ on rajoute une contrainte :

$x_n \longleftrightarrow y_j$

$$\left[\begin{array}{l} z \longleftrightarrow z' \stackrel{1}{=} \\ (z \wedge z') \vee (\neg z \wedge \neg z') \end{array} \right.$$

2) Si n est une conjonction :

$$n = n_1 \wedge n_2$$

alors on rajoute la contrainte

$$X_n \Leftrightarrow X_{n_1} \wedge X_{n_2}$$

2') Pareil pour les disjonctions

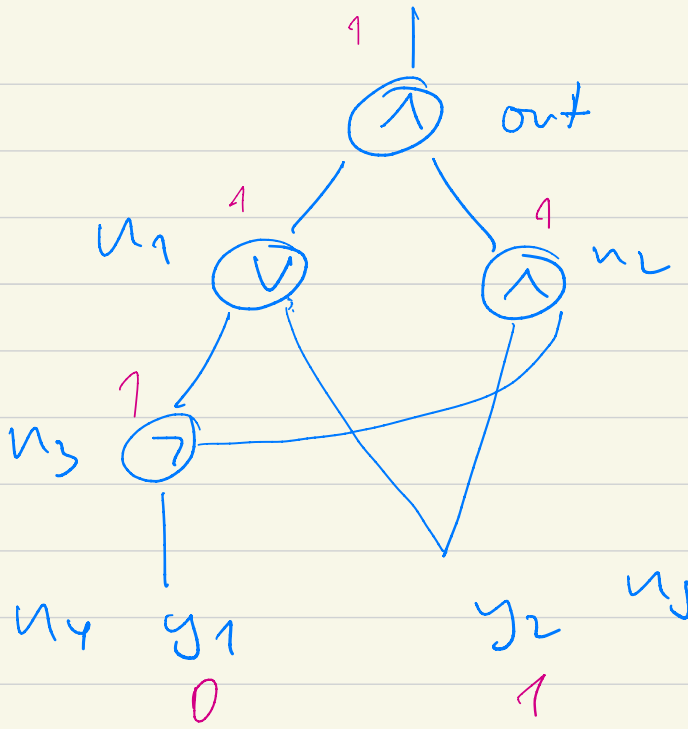
3) Si n est une négation :

$$n = \neg n_1$$

on rajoute la contrainte

$$X_n \Leftrightarrow \neg X_{n_1}$$

La formule φ_C est la conjonction de toutes les contraintes, plus la contrainte X_{out}, où $out \in N$ est la sortie de C.



C

$$\varphi_C = \underset{1}{\left(x_{out} \leftrightarrow \underset{1}{x_{u_1}} \wedge \underset{1}{x_{u_2}}\right)} \wedge$$

$$\left(x_{u_1} \leftrightarrow \underset{1}{x_{u_3}} \vee \underset{1}{x_{u_5}}\right) \wedge$$

$$\left(x_{u_2} \leftrightarrow \underset{1}{x_{u_3}} \wedge \underset{1}{x_{u_5}}\right) \wedge$$

$$\left(x_{u_3} \leftrightarrow \neg \underset{0}{x_{u_4}}\right) \wedge$$

$$\left(x_{u_4} \leftrightarrow \underset{0}{y_1}\right) \wedge$$

$$\left(x_{u_5} \leftrightarrow \underset{1}{y_2}\right) \wedge$$

$$\underset{1}{x_{out}}$$

On montre :

C est satisfaisable $\Leftrightarrow$

φ_C est satisfaisable

($\Rightarrow$) On prend une valuation $val : \{y_1, \ldots, y_m\} \to \{0,1\}$ qui satisfait C. Pour chaque noeud n de C on calcule sa valeur sous val. Ceci produit une valuation des variables x_n, $n \in \mathbb{N}$ de φ_C. Par déf. des contraintes de φ_C, toutes les contraintes sont satisfaites (et aussi la dernière, x_{out}!)

($\Leftarrow$) Si on a une valuation $val' : \{y_1, \ldots, y_m\} \cup \{x_n : n \in \mathbb{N}\}$

qui satisfait φ_C, alors cette valuation, restreinte aux variables y_i, satisfait le circuit C. Ceci parce que les valeurs des noeuds internes sont déterminées par les valeurs de y_i, et parce qu'on a la contrainte X_{out}.