Réductions
10 février 2022 11:11

DBL-SAT = { φ : il existe au moins 2 assignations distinctes qui satisfont φ }

Thm : DBL-SAT est NP-complet

① DBL-SAT $\in$ NP. Deux assignations A_1 et A_2 qui sat. φ peuvent servir de certif.
On peut vérifier chacune en temps $\mathcal{O}(|\varphi|)$.

② DBL-SAT est NP-difficile.
On montre SAT $\leq_p$ DBL-SAT.

$$\varphi \xrightarrow{f} \varphi'$$

Soit φ une instance de SAT.
On pose $\varphi' = \varphi \wedge (z \vee \bar{z})$, où z est une nouvelle var. pas dans φ.

$\Rightarrow$ Soit A une assign. qui sat. φ.
Alors $A + (z = T)$ et $A + (z = F)$ satisfont φ'.
$\Leftarrow$ Soit A_1 et A_2 des assign. qui sat. φ'.
En particulier, A_1 satisfait φ, peu importe z.
Donc $\varphi \in$ SAT.

SUBSET-SUM = { $\langle S, k \rangle$: S est un ensemble d'entiers encodés en binaire, k aussi t.q. il existe $S' \subseteq S$ avec $\sum_{s \in S'} s = \underbrace{k}_{\text{somme cible}}$ }

ex : $S = \{1, 8, 14, 15\}$ $k = 30$ $S' = \{1, 14, 15\}$

SUBSET-SUM est NP-complet.

$s \in S'$
$s = 2^{|S|}$

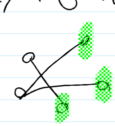
① $\in$ NP. On prend $S' \subseteq S$ avec $\sum_{s \in S'} s = k$ comme certificat.

On peut additionner les $s \in S'$ en temps linéaire par rapport au # de bits requis pour leur encodage.

② est NP-difficile.

Réduction via IND-SET. ($\langle G, k \rangle$: G a un ens indep $|I| = k$)

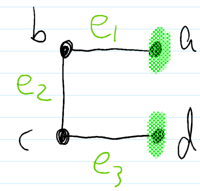
Soit $\langle G, k \rangle$ une instance de IND-SET.



- On transforme $\langle G, k \rangle$ en $\langle S, t \rangle$ une instance de SUBSET-SET.
- On numérote les arêtes $E(G) = \{e_1, e_2, \ldots, e_m\}$
- Pour chaque $u \in V(G)$, on ajoute à S l'entier

$s_u = (\sum 2^{n \cdot i}) + 1$ où $n = |V(G)|$

$\langle G, 2 \rangle$



$(e_1) \mapsto 2^{n \cdot 1}$ $n = 4$

à S l'entier

$$s_u = \left(\sum_{e_i : u \in e_i} 2^{n \cdot i}\right) + 1 \quad , \text{où } n = |V(G)|$$

- Pour chaque $e_i \in E(G)$, on ajoute aussi
  $s_{e_i} = 2^{n \cdot i}$
- On pose $t = \left(\sum_{i=1}^{m} 2^{n \cdot i}\right) + k$
- $\langle S, t \rangle$ peut être construit en temps poly car les valeurs exponentielles prennent un # de bit polynomial par rapport à $|V(G)|$ et $|E(G)|$.

e_3 v

s_a: 0000 0000 0001 0001
s_b: 0000 0001 0001 0001
s_c: 0001 0001 0000 0001
s_d: 0001 0000 0000 0001
s_{e_1}: 0000 0000 0001 0000
s_{e_2}: 0000 0001 0000 0000
s_{e_3}: 0001 0000 0000 0000
t: 0001 0001 0001 $\underbrace{0010}_{k=2}$

À montrer : $\langle G, k \rangle \in$ IND-SET $\iff \langle S, t \rangle$ admet $S' \subseteq S$ avec $\sum_{s \in S'} s = t$.

$\Rightarrow$ Soit I un ens. indép. de G avec $|I| = k$.
On choisit dans S' d'abord le sous-ensemble $\{s_u : u \in I\}$.
De cette façon, le dernier groupe de n bits sera égal à k et une partie de $(n \cdot i)$-ème bits seront à 1. Puisque I est indépendant, aucun autre bit ne sera à 1.
Pour atteindre t, on ajoute les s_{e_i} nécessaires.

$\Leftarrow$ Supposons qu'il $\exists\, S' \subseteq S$ avec $\sum_{s \in S'} s = t$.
Soit $I = \{u : s_u \in S' \text{ et } u \in V(G)\}$
Puisque S' atteint t avec le dernier groupe de n bits à k, il faut que $|I| = k$.
De plus, $\forall u, v \in I$, s_u et s_v n'ont pas de bit commun à 1 (sa[uf]
le dernier).
Par construction, ceci veut dire que u et v ne partagent pas d[...]
et donc I est indépendent.

SET-COVER $= \{\langle S, U, k \rangle : S$ est une collection d'ensembles t.q.

nf

árête

SET-COVER $= \{ \langle S, U, k \rangle :$ S est une collection d'ensembles t.q. $\exists S' \subseteq S$ avec $\bigcup_{S_i \in S'} S_i = U$ et $|S'| = k \}$

ex: $S = \{ \{1,2\}, \{2,3,4\}, \{1,3,5\} \}$ $U = \{1,2,3,4,5\}$ $k = 2$

$S' = \{ \{2,3,4\}, \{1,3,5\} \}$

SET-COVER est NP-complet.

① $\in NP$. On utilise $S' \subseteq S$ comme certificat. Il est de vérifier que $|S'| = k$ et $\bigcup_{S_i \in S'} S_i = U$.

② est NP-difficile.
Réduction via 3-SAT.

$$\varphi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_2 \vee \bar{x}_3 \vee x_1) \wedge (x_2 \vee x_3 \vee \bar{x}_1)$$

C_1 $\quad C_2 \quad C_3$

$x_1 = T$ $\quad x_1 = F$ $\quad x_2 = T$ $\quad x_2 = F$ $\quad \ldots$

$$\varphi \xrightarrow{f} \langle S, U, k \rangle$$

Soit $C_1, C_2, \ldots, C_m$ les clauses de φ et $x_1, x_2, \ldots, x_n$ ses variables.

On définit $U = \{ C_1', C_2', \ldots, C_m', x_1', x_2', \ldots, x_n' \}$

$$S = \{ \underbrace{S_1}_{x_1 = T}, \underbrace{\bar{S}_1}_{x_1 = F}, \underbrace{S_2}_{x_2 = T}, \underbrace{\bar{S}_2}_{x_2 = F}, \ldots, S_n, \bar{S}_n \}$$

où $\forall i = 1..n$

$$S_i = \{ x_i' \} \cup \{ C_j' : x_i = T \text{ satisfait } C_j \}$$

$$\bar{S}_i = \{ x_i' \} \cup \{ C_j' : x_i = F \text{ satisfait } C_j \}$$

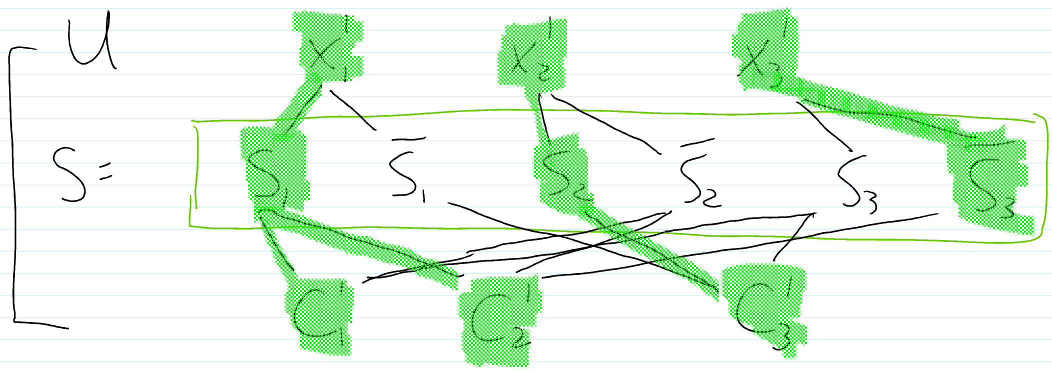
$\bar{S}_i = \{ x_i' \} \cup \{ C_j' : x_i = f \text{ satisfait } C_j \}$

$$\overset{C_1}{(x_1 \vee \bar{x}_2 \vee x_3)} \wedge \overset{C_2}{(\bar{x}_2 \vee \bar{x}_3 \vee x_1)} \wedge \overset{C_3}{(x_2 \vee x_3 \vee \bar{x}_1)}$$

$\varphi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_2 \vee \bar{x}_3 \vee x_1) \wedge (x_2 \vee x_3 \vee \bar{x}_1)$

$x_1 = T$ $x_2 = T$ $x_3 = f$

arête = c



$k = 3$

On pose $k = n$.

On peut construire $\langle S, U, k \rangle$ en temps poly$(|\varphi|)$.

$\varphi \in$ 3-SAT $\Leftrightarrow \langle S, U, k \rangle \in$ SET-COVER

$\Rightarrow$ Soit A une assign. qui satisfait φ.

Soit $S' = \{ S_i : x_i = T \text{ dans } A \} \cup \{ \bar{S}_i : x_i = f \text{ dans } A \}$

Alors : • $|S'| = n = k$ car A assigne un de $x_i = T$ ou f à chaque

• Tous les x_i' sont couverts pour la m̂ raison.

• Tous les C_j' sont couverts par S' car A satisfait c

clause.

Donc $\langle S, U, k \rangle \in$ SET-COVER

$\Leftarrow$ Soit $S' \subseteq S$ qui couvre tout avec $|S'| = k = n$.

Puisque $|S'| = n$, et qu'il faut couvrir chaque x_i', il faut choisir un de chaque S_i ou $\bar{S}_i$ (pas les deux).

On satisfait φ avec l'assignation

$x_i = T \Leftrightarrow S_i \in S'$

ntient

$i = 1..n$

hage

$x_i = T \iff S_i \in S'$

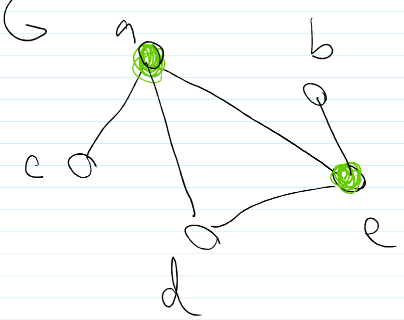
Cette assignation satisfait chaque clause car chaque C_i' est

---

VERTEX-COVER

Soit G un graphe. On dit que $X \subseteq V(G)$ est une couverte sommets (vertex cover) si $\forall uv \in E(G)$, on a $u \in X$ ou (ou les deux)

ex: G



$\{a, e\}$ est un vertex-cover. $k=2$

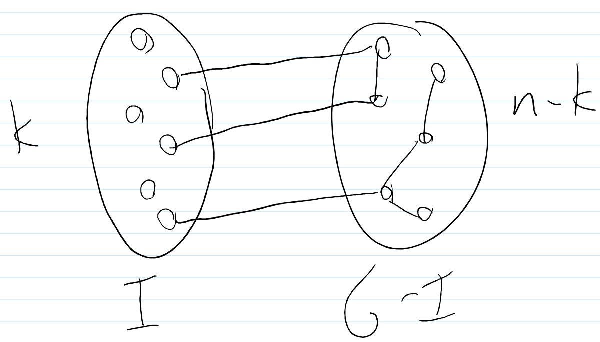
$\{b, d, c, e\}$ aussi

VERTEX-COVER $= \{\langle G, k\rangle :$ G contient un vertex cover de taille

<u>Théorème</u>: Un graphe G a un ensemble indep. de taille k

$\iff$

G a un vertex-cover de taille $n-k$.



VERTEX-COVER est NP-complet

1. $\in$ NP. Exercice.
2. est NP-difficile.

convert. ∎

par

$v \in X$.

$k\}$

② est NP-difficile.

Réduction via IND-SET.

$$\langle G, k\rangle \text{ IND-SET} \xrightarrow{f} \langle G, n-k\rangle \text{ VERTEX-COVER}$$

Par le Thm, G a un ens. indep de taille k $\Leftrightarrow$ G un a vertex

$$\langle G, k\rangle \in \text{IND-SET} \Leftrightarrow \langle G, n-k\rangle \in \text{VERTEX-}$$

- cover de taille $n-k$

COVER