Réductions
10 février 2022 11:11

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

<u>Thm</u>: 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.

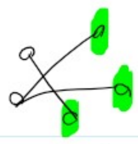
$s \in S'$
$s = 2^{|S|}$

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. 

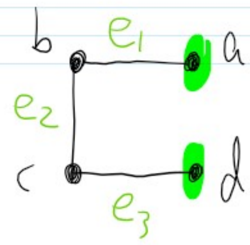
- On transforme $\langle G, k \rangle$ en $\langle S, t \rangle$ une instance de SUBSET-SET.
- On numérote les arêtes $E(G) = \{e_1, e_2, \ldots, e_m\}$
- Pour chaque $u \in V(G)$, on ajoute à S l'entier

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

- Pour chaque $e_i \in E(G)$, on ajoute aussi

$$s_{e_i} = 2^{n \cdot i}$$

- On pose $t = \left(\sum_{i=1}^{m} 2^{n \cdot i} \right) + k$

$\langle G, 2 \rangle$ 

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

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 0010.

$i=1$

- $\langle S,t \rangle$ peut être construit en temps poly car les valeurs exponentielles prennent un # de bit polynomial par rapport à $|V(G)|$ et $|E(G)|$.

s_{e_3}: 000 | 0000 0000 0000

t 000 | 000 | 000 | $\underbrace{0010}_{k=2}$

À montrer: $\langle G,k \rangle \in$ IND-SET $\Leftrightarrow$ $\langle S,t \rangle$ 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 $I = \{u : s_u \in S'$ 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 (sauf le dernier).
Par construction, ceci veut dire que u et v ne partagent pas d'arête et donc I est indépendant.