TD 08 – Complexité: NP-complétude

Exercice 1. *Compréhension du cours*

Pour chacun des énoncés de chacune des questions, indiquer s'il est vrai ou faux.

1. Si SAT $\in$ P alors :
   - **(a)** Clique $\in$ NP ;
   - **(b)** Tous les problèmes NP-difficiles sont dans P ;
   - **(c)** P = NP.

   ☞
   - **(a)** Vrai, c'est en faite vrai même si SAT $\neq$ NP.
   - **(b)** Faux, les problèmes EXP-difficiles sont NP-difficiles mais pas dans P par exemple.
   - **(c)** Vrai, comme SAT est NP-difficile (et donc plus difficile que tous les problèmes dans NP) alors s'il est dans P, alors tous les problèmes de NP sont dans P.

2. Si P $\neq$ NP alors :
   - **(a)** SAT $\notin$ P
   - **(b)** co-P $\neq$ P
   - **(c)** Aucun problème NP-difficile n'est dans P.

   ☞
   - **(a)** Vrai. Si P $\neq$ NP, alors il existe des problèmes dans NP mais pas dans P. Et SAT qui est NP-difficile (et donc plus difficile que tous les problèmes de NP) n'est à plus forte raison pas dans P.
   - **(b)** Faux, indépendamment de savoir si P = NP, on sait que P = coP.
   - **(c)** Vrai, car si un problème NP-difficile est dans P alors tous les problèmes dans NP sont aussi dans P et donc P = NP.

Exercice 2. *Ensemble dominant*

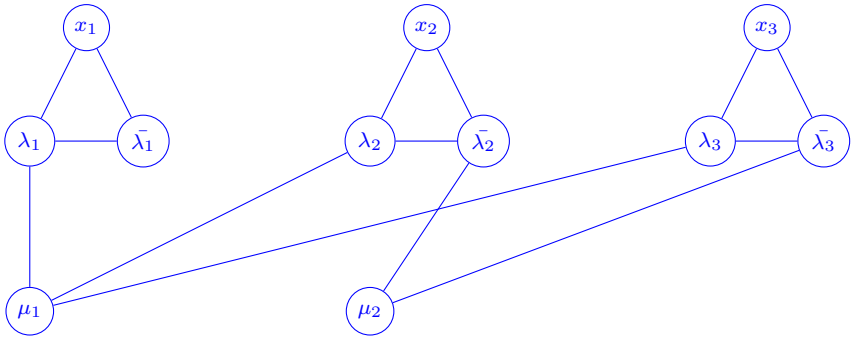
ENSEMBLE_DOMINANT
entrée : un graphe non-orienté $G = (V, E)$ et un entier $k \in \mathbb{N}$.
question : Existe-t-il un sous ensemble $V' \subseteq V$ tel que $|V'| = k$ et tout sommet de $V \setminus V'$ est adjacent à au moins un sommet de V' ?

1. Montrer que ce problème est dans NP.

   ☞ Pour montrer que le problème ENSEMBLE_DOMINANT est dans NP, il suffit de montrer que pour chaque instance positive du problème, il existe un certificat pouvant être vérifiée en temps polynomial. Dans ce cas, le certificat serait un ensemble V' de sommets de taille k, et la vérification consisterait à s'assurer que tout sommet de V est soit dans V' soit adjacent à au moins un sommet de V'. Cette vérification peut être effectuée en temps polynomial, car il suffit de parcourir tous les sommets de $v \in V$ et de s'assurer que soit $v \in V'$ soit un voisin de v est dans V' ce qui prend un temps $O(|V|+|E|)$. (Selon comment V' est encodé, il faut également vérifier que $|V'| = k$ mais c'est également polynomial.) Par conséquent, ENSEMBLE_DOMINANT est dans NP.

2. Montrer que ce problème est SAT $\leq_m^P$ ENSEMBLE_DOMINANT

   ☞ On définit la réduction polynomiale de SAT vers ENSEMBLE_DOMINANT suivante $f : \phi \to (G, n)$ où ϕ est une formule CNF avec n variables $\lambda = \{\lambda_1, \ldots, \lambda_n\}$ et m clauses $\mu = \{\mu_1, \ldots, \mu_m\}$. On définit $G = (V, E)$ comme étant composés de $3n + m$ sommets. Chaque variable λ_i est représenté dans le graphe par 3 sommets $x_i, \lambda_i, \bar{\lambda_i}$ formant un triangle. Chaque clause μ_j est représenté par un sommet μ_j. De plus si λ_i (*resp.* $\bar{\lambda_i}$) apparaît dans μ_j alors on ajoute une arête $\{\lambda_i, \mu_j\}$.
   Exemple avec la formule $\phi = (\lambda_1 \vee \lambda_2 \vee \lambda_3) \wedge (\bar{\lambda_2} \vee \bar{\lambda_3})$:



f est clairement calculable en temps polynomial.

Maintenant, si ϕ est une instance positive de SAT alors il existe une valuation $v : \lambda \to \{\bot, \top\}$ qui satisfait ϕ. Soit $V' = \{\lambda_i \in \lambda \mid v(\lambda_i) = \top\} \cup \{\bar{\lambda_i} \mid v(\lambda_i) = \bot\}$. Pour tout $i \in [n]$, V' domine $\{\lambda_i, \bar{\lambda_i}, x_i\}$ car λ_i ou $\bar{\lambda_i} \in V'$ et que $\{\lambda_i, \bar{\lambda_i}, x_i\}$ est une clique dans G. De plus, pour toute clause μ_j, V' domine μ_j car comme v satisfait ϕ, il y a deux cas :

(a) il existe $\lambda_i \in \mu_j$ tel que $v(\lambda_i) = \top$ et donc $\{\lambda_i, \mu_j\} \in E$ et $\lambda_i \in V'$;

(b) il existe $\bar{\lambda_i} \in \mu_j$ tel que $v(\lambda_i) = \bot$ et donc $\{\bar{\lambda_i}, \mu_j\} \in E$ et $\bar{\lambda_i} \in V'$.

Donc V' (de taille n) domine G et $f(\phi) = (G, n)$ est une instance positive de ENSEMBLE_DOMINANT.

Dans l'autre direction, supposons que $f(\phi) = (G, n)$ est une instance positive de ENSEMBLE_DOMINANT. Soit V' l'ensemble dominant de taille n dans G. Comme $x_1, \dots, x_n$ n'ont pas de voisins en communs, on peut se convaincre que pour tout i, V' contient exactement 1 sommets parmi $\{\lambda_i, \bar{\lambda_i}, x_i\}$ et donc que V' ne contient aucun sommet $\mu_j \in \mu$ (étant donné sa taille).

Maintenant, définissons la valuation de $v : \lambda_i \mapsto \begin{cases} \top & \text{si } \lambda_i \in V' \\ \bot & \text{sinon.} \end{cases}$ Soit $\mu_j \in \mu$. Comme V' domine G, et que $\mu_j \notin V'$, soit :

(a) Il existe $\lambda_i \in V'$ tel que $\{\lambda_i, \mu_j\} \in E$ et donc $\lambda_i \in \mu_j$ et par définition de v, $v(\lambda_i) = \top$;

(b) Il existe $\bar{\lambda_i} \in V'$ tel que $\{\bar{\lambda_i}, \mu_j\} \in E$ et donc $\bar{\lambda_i} \in \mu_j$ et $v(\lambda_i) = \bot$ car $\lambda_i \notin \mu_j$.

Dans les deux cas, la clause μ_j est satisfaite. Donc ϕ est satisfaite et est donc une instance positive de SAT.

3. Conclure.

☞ Comme SAT $\leq_m^P$ ENSEMBLE_DOMINANT et que SAT est NP-difficile alors ENSEMBLE_DOMINANT aussi. Comme ENSEMBLE_DOMINANT est en plus dans NP alors il est NP-complet.

Exercice 3. *one-way (Bonus)*

Une fonction one-way ("à sens unique") est une fonction $f : \mathbb{N} \to \mathbb{N}$ tel que

- f est bijective,
- x est codé sur k bits $\Leftrightarrow f(x)$ est codé sur k bits,
- f est calculable en temps polynomial,
- f^{-1} n'est pas calculable en temps polynomial.

Supposons qu'une telle fonction existe et considérons le problème suivant :

ONE_WAY
entrée : Deux entiers x et y encodés en binaire sur k bits
question : $f^{-1}(x) < y$?

1. Montrer que ONE_WAY $\in$ NP.

☞ Pour montrer que ONE_WAY $\in$ NP, il suffit de montrer qu'il existe un certificat vérifiable en temps polynomial pour toute instance positive du problème. Le certificat peut-être la valeur z qui est supposée être $f^{-1}(x)$. On peut vérifier en temps polynomial que $z < y$ et calculer $f(z)$ pour vérifier si $f(z) = x$.

2. Montrer que ONE_WAY $\in$ coNP

☞ C'est le même principe : il suffit de montrer qu'il existe un certificat vérifiable en temps polynomial pour toute instance négative du problème. Le certificat est également z qui est supposée être $f^{-1}(x)$. On peut vérifier en temps polynomial que $z \geq y$ (la négation de $z < y$) et calculer $f(z)$ pour vérifier si $f(z) = x$.

3. Montrer que ONE_WAY $\notin$ P.

☞ Il suffit de montrer que si ONE_WAY $\in$ P alors f^{-1} est calculable en temps polynomial ce qui contredit les hypothèses sur f. On peut calculer $f^{-1}(x)$ pour tout x de manière dichotomique en faisant appel à la fonction qui décide ONE_WAY $\lceil \log_2(n) \rceil$ fois où n est le nombre de bits de x.

4. Que peut-on en déduire sur la relation entre P et NP si les fonctions one-way existent ?

☞ Si les fonctions one-way existent, cela signifie que certains problèmes sont dans NP mais pas dans P et donc que P $\neq$ NP.