TD 10 – Révisions (2)

Rappel : Lorsqu'aucune précision n'est donnée quand au problème **SAT**, il s'agit de celui-ci :

SAT
entrée : une formule propositionnelle ϕ en forme normale conjonctive.
question : ϕ est-elle satisfaisable ?

Exercice 1. **Noyau $\leq_m^p$ SAT**

Un *noyau* d'un graphe orienté $G = (V, A)$ est un ensemble N de sommets indépendants (aucune arrête entre deux sommets de N) et tel que tout sommet extérieur à N a un successeur dans N. Autrement dit, $N \subseteq V$ est un noyau s'il satisfait les deux contraintes :

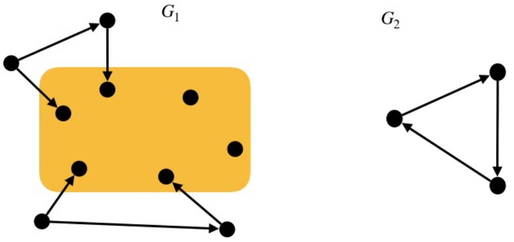
(i) $\forall x, y \in N \ : \ (x, y) \notin A$ **(ii)** $\forall x \notin N \ : \ \exists y \in N \ : \ (x, y) \in A$

On définit alors le problème **Noyau** ci-dessous :

Noyau
entrée : un graphe orienté $G = (V, A)$.
question : G admet-il un noyau ?

1. Donner un exemple de graphe $G_1 \in$ **Noyau**, et un exemple de graphe $G_2 \notin$ **Noyau**.

Solution :



2. Montrer que **Noyau** $\in$ NP.

Solution : Comme d'habitude il suffit de deviner un sous-ensemble $N \subseteq V$ et vérifier s'il satisfait les contraintes.

3. Montrer que **Noyau** $\leq_m^p$ **SAT**, sans utiliser la question 2.

Solution : Soit $G = (V, E)$ un graphe à n sommets. Pour chaque sommet $i \in V$ on crée une variable propositionnelle p_i (qui a vocation a être vraie lorsque i est dans le noyau de G), puis on considère les formules suivantes :

— $\phi_1 = \bigwedge_{(i,j)\in E}(p_i \to \neg p_j) = \bigwedge_{(i,j)\in E}(\neg p_i \vee \neg p_j)$;

— $\phi_2 = \bigwedge_{i\in V}\left(p_i \vee \bigvee_{(i,j)\in E} p_j\right)$;

— $\phi_G = \phi_1 \wedge \phi_2$.

Montrons que G admet un noyau $\Leftrightarrow$ ϕ_G est satisfaisable.

$\boxed{\Rightarrow}$ Soit v un modèle de ϕ_G. On pose $N = \{i \in V : v(p_i) = 1\}$. Alors, d'une part, pour toute $(i, j) \in E$, i ou j n'est pas dans N (puisque v satisfait ϕ_1), ce qui signifie que les sommets de N sont deux à deux non-adjacents ; d'autre part, pour tout sommet $i \notin N$ on a $v(p_i) = 0$ et donc, puisque v satisfait ϕ_2, $v(\bigvee_{(i,j)\in E} p_j) = 1$, ce qui impose que l'une des arêtes partant de i arrive sur un sommet $j \in N$. Ainsi, N est bien un noyau de G.

$\boxed{\Leftarrow}$ Soit N un noyau de G. Considérons la valuation v sur les variables de ϕ_G définie par : $v(p_i) = 1$ ssi $i \in N$. Puisque aucune arête de G n'a ses deux extrémités dans N, on a $i \in N \Rightarrow j \notin N$ pour tout $(i, j) \in E$.

Et donc, par construction de v : $v(p_i \to \neg p_j) = 1$ pour tout $(i,j) \in E$, d'où s'ensuit que v satisfait ϕ_1. De plus, un sommet $i \in V$ est soit dans N, soit relié à un sommet de N, ce qui signifie que l'une des arêtes partant de i arrive dans N. Ceci induit l'égalité $v(p_i \vee \bigwedge_{(i,j)\in E} p_j) = 1$ pour tout $i \in V$. La satisfaction de ϕ_2 par v s'en déduit. Finalement, on a montré que v satisfait $\phi_1 \wedge \phi_2 = \phi_G$, preuve que cette dernière formule est satisfaisable.

4. Montrer que **Noyau** est NP-complet. (Indice : réduire depuis **SAT**.)

Solution : Étant donnée une formule $\phi = \phi_1 \vee \cdots \vee \phi_m$ en forme normal conjonctive, on construit un graphe orienté G qui admet un noyau ssi ϕ est satisfaisable. Pour chaque clause ϕ_i on prend trois sommets $\phi_{i,1}, \phi_{i,2}$ et $\phi_{i,3}$ relié en triangle par les arcs $(\phi_{i,1}, \phi_{i,2})$, $(\phi_{i,2}, \phi_{i,3})$ et $(\phi_{i,3}, \phi_{i,1})$. Pour chaque variable x_j qui apparaît dans la formule, on prend deux sommets x_j et $\neg x_j$ et on les relie avec les arcs $(x_j, \neg x_j)$ et $(\neg x_j, x_j)$. Enfin, pour chaque littéral ℓ (donc soit $\ell = x_j$, soit $\ell = \neg x_j$ pour quelque j), si le littéral ℓ apparaît dans la clause ϕ_i, on ajoute trois arcs $(\phi_{i,1}, \ell)$, $(\phi_{i,2}, \ell)$ et $(\phi_{i,3}, \ell)$.

Un ensemble $N \subseteq V$ de sommets de G est un noyau ssi N (a) ne contient que des sommets correspondants aux littéraux, (b) il contient exactement l'un entre x_i et $\neg x_i$ pour chaque variable et (c) il contient au moins un littéral pour chaque clause de ϕ. En effet

- **(a)** si N contenait un sommet du type $\phi_{i,k}$, alors les sommets correspondants aux littéraux qui apparaissent dans la clause ϕ_i ne pourraient pas être contenus dans N (sinon on aurait un arc entre deux sommets de N) et donc il faudrait trouver un noyau pour le sous-graphe qui comprend $\phi_{i,1}$, $\phi_{i,2}$ et $\phi_{i,3}$ et les arcs relatifs ; mais, comme déjà vu dans la solution de la question 1, un triangle n'admet pas de noyau ;
- **(b)** si N contenait, à la fois, une variable x_j et sa négation $\neg x_j$, il y aurait deux sommets reliés par un arc ;
- **(c)** si, pour une certaine clause ϕ_i, l'ensemble N ne contenait aucun littéral qui apparaît dans ϕ_i, alors les trois sommets correspondants $\phi_{i,1}$, $\phi_{i,2}$ et $\phi_{i,3}$ constitueraient un triangle isolé du reste du graphe, et cela n'admet pas de noyau (question 1).

Donc le noyau N correspond à un modèle v de la formule ϕ, défini par $v(x_j) = 1 \Leftrightarrow x_j \in N$.

Vice versa, si ϕ est satisfaisable, soit v un modèle et soit $N = \{x_j : v(x_j) = 1\} \cup \{\neg x_j : v(x_j) = 0\}$. Alors N est un noyau de G. En effet :

- **(a)** il n'y a pas d'arcs entre deux sommets dans N, puisque une variable et sa négation n'apparaissent jamais simultanément dans N, et le graphe n'a pas d'arcs entre deux littéraux avec des variables distinctes ;
- **(b)** pour chaque sommets correspondant à une variable x_j, soit $x_j \in N$ (et alors $\neg x_j$ a un sommet adjacent dans N), soit $\neg x_j \in N$ (et alors x_j a un sommet adjacent dans N) ;
- **(c)** puisque v satisfait ϕ, en particulier il satisfait chaque clause ϕ_i, ce qui implique que au moins un littéral ℓ de ϕ_i est vrai et donc $\ell \in N$. Par conséquent, les trois sommets $\varphi_{i,1}$, $\varphi_{i,2}$ et $\varphi_{i,3}$ ont un sommets adjacent dans N, notamment ℓ lui-même.

Donc ϕ est satisfaisable ssi G a un noyau, comme demandé par la définition de réduction. La fonction $\phi \mapsto G$ peut être calculé en temps polynomial, puisque on ajoute un nombre polynomial de sommets et arcs à G pour chaque variable et clause de ϕ.

Exercice 2. *vrai ou faux ?*

On considère quatre problèmes de décision A, B, C, D vérifiant :

(**i**)$A \in \mathsf{P}$ (**ii**)B est NP-difficile (**iii**)$C \in \mathsf{NP}$

1. Si on suppose que $\mathsf{P} = \mathsf{NP}$, alors que dire de la validité des affirmations suivantes ?

- **(a)** Si $A \leq_m^p D$, alors $D \in \mathsf{P}$.
- **(b)** Si $D \leq_m^p A$, alors $D \in \mathsf{P}$.
- **(c)** Si $D \leq_m^p B$, alors D est NP-difficile.
- **(d)** Si $B \leq_m^p D$, alors D est NP-difficile.
- **(e)** Si $D \leq_m^p C$, alors $D \in \mathsf{NP}$.
- **(f)** Si $C \leq_m^p D$, alors $D \in \mathsf{NP}$.

2. Si on suppose que $\mathsf{P} \neq \mathsf{NP}$, alors que dire de la validité de ces mêmes affirmations ?

Exercice 3. *quelques machines de Turing*

1. Construire des machines de Turing qui décident les langages suivants.

(a) L'ensemble des mots sur $\{0, 1\}$ comportant un nombre pair de 1.

(b) L'ensemble des mots sur $\{a, b\}$ qui sont des palindromes.

2. Évaluer le temps de calcul de vos machines.

Exercice 4. *colorabilité*

Voici les définitions des problèmes k**-SAT** et k**-Couleur**, pour $k \geq 2$:

k**-SAT**
entrée : une formule ϕ sous forme normale conjonctive avec des clauses de taille k.
question : ϕ est-elle satisfaisable ?

k**-Couleur**
entrée : un graphe non-orienté $G = (V, E)$.
question : G est-il k-coloriable ?

Un graphe est *k-coloriable* s'il est possible de colorier ses sommets avec au plus k couleurs, de sorte que deux sommets adjacents soient toujours de couleurs distinctes.

1. Donnez un exemple de graphe G_1 à 5 sommets qui soit 3-coloriable, en justifiant.

2. Donnez un exemple de graphe G_2 à 5 sommets qui ne soit pas 3-coloriable, en justifiant.

3. Montrez que **3-Couleur** $\in \mathsf{NP}$.

☞ Un 3-coloriage d'un graphe $G = (V, E)$ peut être décrit par une fonction $c : V \to \{1, 2, 3\}$ telle que $(x, y) \in E \Rightarrow c(x) \neq c(y)$. On considère la relation R qui relie les graphes 3-coloriables à leurs 3-coloriages. Autrement dit, pour tout graphe $G = (V, E)$ et toute application $c : V \to \{1, 2, 3\}$, on pose :

$$R(G, c) \Leftrightarrow \text{ } c \text{ est un 3-coloriage de } G.$$

Alors R est une certification polynomiale de 3**-Couleur**. On a en effet :

(a) G est 3-coloriable ssi il existe c tel que $R(G, c)$;

(b) Si $R(G, c)$, alors c est de taille polynomialement bornée par $|G|$. En effet, c est décrite par la donnée d'une couleur $i \in \{1, 2, 3\}$ pour chaque sommet $x \in V$ donc, en définitive, par une suite de $|V|$ couleurs. Cette information est clairement de taille $O(|V|)$, et donc $O(|G|)$.

(c) On peut décider $R(G, c)$ en temps polynomial : il suffit de vérifier, pour chaque $xy \in E$, que $c(x) \neq c(y)$. Ceci se fait clairement en temps linéaire — et a fortiori, polynomial — en la taille de G.

Le problème 3**-Couleur** admet ainsi une certification polynomiale ; il appartient donc à NP.

4. Montrez que pour $k \geq 2$ fixé, k**-Couleur** $\leq_m^p$ k**-SAT**.

☞ Il s'agit de constuire une application calculable en temps polynomial et qui associe à chaque graphe G une formule ϕ_G (sous forme k-CNF) telle que :

$$G \text{ est } k\textbf{-Couleur} \Leftrightarrow \phi_G \text{ est satisfaisable.}$$

L'idée intuitive est de concevoir cette formule de telle sorte qu'elle décrive, dans le langage du calcul propositionnel, un 3-coloriage de G. C'est le passage le plus délicat de la preuve de réduction, qui nous oblige à faire preuve d'imagination. Il faut d'abord choisir un ensemble de variables propositionnelles susceptibles de porter une information « atomique » sur les coloriages. À charge ensuite pour ϕ_G de connecter ces informations atomiques pour décrire un bon coloriage de G. On se rend compte assez facilement que l'information de base, pour parler de coloriage de G, est du type : *tel sommet est colorié par telle couleur*. On crée alors une variable propositionnelle x_i pour chaque sommet $x \in V$ et chaque couleur $i \in [k]$ (où, pour abréger, on a noté $[k]$ l'ensemble $\{1, \ldots, k\}$ des couleurs possibles). On se retrouve ainsi avec $|V| * k$ variables propositionnelles $(x_i)_{x \in V,\, i \in [k]}$, à partir desquelles on peut commencer à bâtir ϕ_G, en s'appuyant sur la vocation de x_i à transcrire l'information « x est colorié par i ».

Un coloriage de G par les couleurs $1, 2, \ldots, k$ doit respecter trois contraintes :

— chaque sommet est colorié par *au moins une* couleur ;
— chaque sommet est colorié par *au plus une* couleur ;
— deux sommets adjacents sont de couleurs distinctes.

Ces trois contraintes sont exprimées par les formules suivantes :

$\phi_G^1 : \bigwedge_{x\in V} \ \bigvee_{i\in[k]} x_i$

$\phi_G^2 : \bigwedge_{x\in V} \ \bigwedge_{i\neq j\in[k]} (x_i \Rightarrow \neg x_j)$

$\phi_G^3 : \bigwedge_{xy\in E} \ \bigwedge_{i\in[k]} (x_i \Rightarrow \neg y_i)$

On note ϕ_G la conjonction de ces trois formules :

$$\phi_G = \phi_G^1 \wedge \phi_G^2 \wedge \phi_G^3.$$

Notre objectif est désormais de démontrer que l'application $r : G \mapsto \phi_G$ est une réduction polynomiale de k-**Couleur** à k-**Sat**.

Notons d'abord que chaque ϕ_G^i est une conjonction de k-clauses : pour ϕ_G^1 c'est clair, puisque chaque conjonct $\bigvee_{i\in[k]} x_i$ est une k-clause. Quant à ϕ_G^2 et ϕ_G^3, ce sont même des conjonctions de 2-clauses : il suffit de réécrire chaque implication du type $p \Rightarrow \neg q$ sous la forme $\neg p \vee \neg q$ pour s'en convaincre. L'application $r : G \mapsto \phi_G$ a donc bien pour prototype :

$$r : I(k\textbf{-Couleur}) \to I(k\textbf{-Sat})$$

qui est le prototype demandé pour une réduction de k-**Couleur** à k-**Sat**.

Par ailleurs, r est calculable en temps polynomial. On voit bien en effet que la construction de $r(G) = \phi_G$ à partir de G n'exige aucun calcul sophistiqué. On peut ici se contenter de constater que la formule ϕ_G est de taille polynomialement bornée par $|G|$, puisqu'elle contient moins de $k|V| + 2k^2|V| + 2k|E|$ littéraux, et que ce nombre est majoré par $(2k^2 + 3k)|V|^2$, qui est un $O(|V|^2)$ et donc un $O(|G|)$.

Reste à établir que r préserve les instances positives, c.a.d.que

$$G \in I^+(k\textbf{-Couleur}) \Leftrightarrow \phi_G \in I^+(k\textbf{-Sat}).$$

$\boxed{\Rightarrow}$: Supposons que $G \in I^+(k\textbf{-Couleur})$. Alors G admet un k-coloriage $c : V \to [k]$, à partir duquel on définit l'interprétation I_c suivante : pour toute variable $x_i \in \text{var}(\phi_G)$ (c.a.d., pour tout $x \in V$ et tout $i \in [k]$),

$$I_c(x_i) = 1 \Leftrightarrow c(x) = i.$$

À chaque $x \in V$, le coloriage c attribue une couleur $i \in [k]$ (à savoir, $i = c(x)$), ce qui s'écrit aussi $I_c(x_i) = 1$, par définition de I_c. Il s'ensuit :

$$\forall x \in V : \ I_c\left(\bigvee_{i\in[k]} x_i\right) = 1,$$

ou encore :

$$I_c\left(\bigwedge_{x\in V} \ \bigvee_{i\in[k]} x_i\right) = 1,$$

d'où finalement :

$$I_c\left(\phi_G^1\right) = 1.$$

De plus, c n'affecte qu'une seule couleur à chaque sommet. De sorte que si x est un sommet et si i et j sont deux couleurs distinctes, $c(x) = i$ entraîne $c(x) \neq j$. Ce qui se traduit, avec le choix que nous avons fait pour I_c, par :

$$\forall x \in V, \ \forall i \neq j \in [k] : \ I_c\left(x_i \Rightarrow \neg x_j\right) = 1,$$

et donc :

$$I_c\left(\bigwedge_{x\in V} \ \bigwedge_{i\neq j\in[k]} x_i \Rightarrow \neg x_j\right) = 1,$$

c.a.d.,

$$I_c\left(\phi_G^2\right) = 1.$$

Enfin, pour chaque arête xy de G, c affecte des couleurs différentes à x et y : si $c(x) = i$ alors $c(y) \neq j$. Ceci entraîne :

$$\forall xy \in E, \ \forall i \in [k] : \ I_c\left(x_i \Rightarrow \neg y_i\right) = 1,$$

et donc :

$$I_c\left(\bigwedge_{xy\in E} \ \bigwedge_{i\in[k]} x_i \Rightarrow \neg y_i\right) = 1,$$

c.a.d.,

$$I_c\left(\phi_G^3\right) = 1.$$

Par conséquent, l'interprétation I_c que nous avons définie à partir du coloriage c satisfait $\phi_G^1 \wedge \phi_G^2 \wedge \phi_G^3$ et donc, est un modèle de ϕ_G.

$\boxed{\Leftarrow}$: Supposons que $\phi_G \in I^+(k\text{-}\mathbf{Sat})$. Alors ϕ_G admet un modèle I, à partir duquel on définit l'application $c_I : V \to [k]$ suivante : pour tout $x \in V$, $c_I(x)$ est l'unique $i \in [k]$ tel que $I(x_i) = 1$. Notons pour commencer que c_I est bien définie, puisque que pour chaque x il existe bien un et un seul $i \in [k]$ tel que $I(x_i) = 1$, en vertu du fait que I satisfait les formules ϕ_G^1 et ϕ_G^2 qui, précisément, garantissent cette existence et cette unicité. La définition de c_I est donc cohérente et on a :

$$c_I(x) = i \Leftrightarrow I(x_i) = 1.$$

Par ailleurs, pour tout $xy \in E$ et tout $i \in [k]$, on a $I(x_i \Rightarrow \neg y_i) = 1$, c.a.d.

$$I(x_i) = 1 \Rightarrow I(y_i) = 0.$$

On en déduit, par définition de c_I, que pour tout $xy \in E$ et tout $i \in [k]$:

$$c_I(x) = i \Rightarrow c_I(y) \neq i.$$

D'où finalement :

$$\forall xy \in E : c_I(x) \neq c_I(y),$$

et cette dernière assertion signifie que c_I est un coloriage de G à valeur dans $[k]$, donc un k-coloriage de G.

5. Que peut-on en déduire sur la complexité de k-**Couleur** pour tout k ? Et pour $k = 2$?

☞ Pour tout $k \geq 2$, de k-**Couleur** $\leq_m^p$ k-**SAT** et de k-**SAT**$\in$ NP on déduit que k-**Couleur**$\in$ NP, car la classe NP est close pour les réduction many-one polynomiales.

Pour $k = 2$, de 2-**Couleur** $\leq_m^p$ 2-**SAT** et de 2-**SAT**$\in$ P on déduit que 2-**Couleur**$\in$ P, car la classe P est close pour les réductions many-one polynomiales.

Pour chaque graphe non-orienté G, on note $r(G)$ le graphe obtenu en adjoignant à G un nouveau sommet α relié à chacun des sommets de G. Autrement dit, pour $G = (V, E)$, le graphe $r(G) = (V', E')$ est défini par :

$$V' = V \cup \{\alpha\} \quad \text{et} \quad E' = E \cup \big\{\{\alpha, x\} \mid x \in V\big\}.$$

6. Dessiner les graphes $r(G_1)$ et $r(G_2)$ avec G_1 et G_2 vos réponses aux questions 1 et 2.
7. Que peut-on dire de la 4-colorabilité de chacun des deux graphes $r(G_1)$ et $r(G_2)$?

☞ $r(G_1)$ est 4-coloriable et $r(G_2)$ n'est pas 4-coloriable.

8. Montrez que l'application $r : G \mapsto r(G)$ est une réduction many-one polynomiale de k-**Couleur** à $(k+1)$-**Couleur**.

☞ L'application r a bien le prototype $I(k\text{-}\mathbf{Couleur}) \to I((k+1)\text{-}\mathbf{Couleur}$ exigé. De plus, elle est clairement calculable en temps polynomial : pour construire $r(G)$, il suffit de connecter un nouveau sommet à tous les sommets de G, et ceci se fait en temps $O(|G|)$. Reste à vérifier qu'elle préserve les instances positives, c.a.d. :

$$G \in I^+(k\text{-}\mathbf{Couleur}) \Leftrightarrow r(G) \in I^+((k+1)\text{-}\mathbf{Couleur}).$$

$\boxed{\Rightarrow}$: Soit $G \in I^+(k\text{-}\mathbf{Couleur})$. À partir d'un k-coloriage de G, on obtient facilement un $(k+1)$-coloriage de $r(G)$ en conservant la couleur des sommets de G et en coloriant d'une nouvelle couleur le sommet α. Ainsi, $r(G) \in I^+((k+1)\text{-}\mathbf{Couleur})$.

$\boxed{\Leftarrow}$: Inversement, si $r(G) \in I^+((k+1)\text{-}\mathbf{Couleur})$, ce graphe admet un $(k+1)$-coloriage. La couleur affectée à α est nécessairement distincte de celles affectées aux autres sommets, puisque ceux-ci sont tous adjacents à α dans $r(G)$. De sorte que les sommets de $V(G)$ sont coloriés avec k-couleurs et G est bien k-coloriable, c.a.d.$G \in I^+(k\text{-}\mathbf{Couleur})$.

9. Si l'on arrive à démontrer que 3-**Couleur** est NP-complet, que peut-on en déduire sur la complexité de k-**Couleur** pour chaque $k \geq 3$?

☞ De la question précédente on déduit la suite de réductions :

$$3\text{-}\mathbf{Couleur} \leq_m^p 4\text{-}\mathbf{Couleur} \leq_m^p \cdots \leq_m^p k\text{-}\mathbf{Couleur} \leq_m^p \cdots$$

Par transitivité de la réduction polynomiale, on en déduit que 3-**Couleur** $\leq_m^p$ k-**Couleur** pour tout $k \geq 3$. La NP-difficulté de 3-**Couleur** entraîne alors celle de k-**Couleur**. Comme ce dernier problème est dans NP, on peut finalement affirmer : pour chaque $k \geq 3$, k-**Couleur** est NP-complet.

10. Montrer que 3-**Couleur** est NP-complet. (Indice : réduire depuis **3-SAT**.)

☞ Voir `https://cgi.csc.liv.ac.uk/~igor/COMP309/3CP.pdf`.