Graphes, rayons et applications

Pour X un ensemble, on note $|X|$ son cadinal.
Dans la suite on considère des graphes non orientés $G = (V, E)$ où V est un ensemble de sommets et E un ensemble d'arêtes, c'est-à-dire, un ensemble $E \subseteq \{\{x, y\} \mid (x, y) \in V^2 \text{ et } x \neq y\}$. Dans la suite, la *taille* de G est le nombre de sommets ($|V|$). On dit qu'il est infini si V est infini et dénombrable si V est infini et dénombrable.
Pour $0 \leq n$, un chemin est une suite finie $s_0, \ldots, s_n$ de sommets telle que pour tout entier $0 \leq i < n$ on a $\{s_i, s_{i+1}\} \in E$. Ainsi, une suite de un sommet est un chemin mais pas la suite vide. Le chemin est dit *simple* si tout sommet y apparaît au plus une fois.
Un *rayon* de G est une suite infinie de sommets $s_0, \ldots, s_n, \ldots$ telle que pour tout entier $0 \leq i$, la suite $s_0, \ldots, s_i$ est un chemin simple.
Un graphe est dit *connecté* si pour tout sommet $s, t \in V$, il existe un chemin de s à t.

Question 1. Montrez que si un graphe G admet un rayon, alors il est infini.

Question 2. Un graphe $G = (V, E)$ est dit localement fini si pour tout $s \in V$, l'ensemble $N_s := \{x \mid \{s, x\} \in E\}$ est fini. Il est localement borné s'il existe une constante M, telle que pour tout s, $|N_s| < M$. Donnez :

— Un exemple d'un graphe infini, connecté et localement borné.

— Un exemple de graphe infini, connecté, localement fini mais pas localement borné.

Dans la suite, on dit qu'un graphe admet la propriété (K) s'il est connecté, infini, et localement fini. Nous allons montrer le résultat suivant :

Tout graphe dénombrable qui vérifie (K) admet un rayon.

Question 3. Est-ce que chacune des trois propriétés de (K) sont nécessaires pour que ce théorème soit vrai ?

Question 4. Montrez qu'il existe un graphe G infini et localement fini tel que pour tout k, G possède un chemin simple de taille k mais tel que G n'admette pas de rayon.

Question 5. Étant donné un graphe $G = (V, E)$ et un sommet v de G. Le graphe $G_v = (V', E')$ avec $V' = V \setminus \{v\}$ et $E' = E \cap \{\{x, y\} \mid x \in V'\}$. Montrez que si G satisfait (K) et v est un sommet de G, alors G_v est une union disjointe finie de graphes connexes dont au moins l'un d'entre eux satisfait (K).

Question 6. Montrez que si G satisfait (K) alors il admet un rayon.

Application à la coloration de graphes Soit $G = (\mathbb{N}, E)$ un graphe. Une k-coloration de G est une fonction $f : \mathbb{N} \to \{0, \ldots, k-1\}$ tel que pour tout $\{x, y\} \in E$ on a $f(x) \neq f(y)$. On dit que G est k-coloriable s'il existe une k-coloration de G.

Question 7. Montrez qu'un graphe dénombrable G est k-coloriable si et seulement si tout ses sous-graphes finis sont k-coloriables.

Application aux mots infinis Soit Σ un alphabet. On note Σ^* l'ensemble des mots finis sur Σ et Σ^∞ l'ensemble des mots infinis. Dans la suite, on pose $L \subseteq \Sigma^*$ un langage arbitraire et $u \in \Sigma^\infty$ un mot infini. Un découpage de u est une suite infinie de mots finis $v_0, \ldots, v_n, \ldots$ telle que $u = v_0 v_1 \cdots v_n \cdots$.

Question 8. Montrez qu'il existe un découpage de u tel qu'à partir d'un certain rang, soit tous les mots appartiennent à L, soit aucun mot n'appartient à L.

Énumération rapide pour les équations booléennes

On considère dans cet exercice un système de m équations booléennes sur n variables $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in (\mathbb{Z}/2\mathbb{Z})^n$, de la forme : $\forall 1 \leq k \leq m, f_k(\mathbf{x}) = 0$. Chaque $f_k : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$ est une fonction booléenne *quadratique*, c'est-à-dire un polynôme de degré 2 :

$$f_k(\mathbf{x}) = f_k(0) + \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_{ij}x_i x_j \ ,$$

où les a_{ij} sont des coefficients booléens, et l'addition et le produit se font dans $\mathbb{Z}/2\mathbb{Z}$. Pour deux vecteurs $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}/2\mathbb{Z})^n$, on note $\mathbf{x} + \mathbf{y}$ leur addition bit à bit dans $(\mathbb{Z}/2\mathbb{Z})^n$.
Notons que le monôme $x_i x_i$ est équivalent à x_i puisque pour tout Booléen $x^2 = x$. On suppose que les équations sont aléatoires et indépendantes : chaque a_{ij} vaut 1 avec probabilité $\frac{1}{2}$. De plus, on pose $m \leq n$ afin de garantir l'existence (en moyenne) de solutions. On veut énumérer toutes les solutions du système.
On mesure la complexité des algorithmes en opérations binaires (additions et multiplications dans $\mathbb{Z}/2\mathbb{Z}$), ainsi que d'autres opérations de base qui seront détaillées par la suite. Pour tout $0 \leq j \leq n-1$, on note $\mathbf{e}_j^n \in (\mathbb{Z}/2\mathbb{Z})^n$ le vecteur booléen $(0, \ldots, 0, 1, 0, \ldots, 0)$, ne comportant qu'un 1 en position j. On pourra simplifier cette notation en $\mathbf{e}_j$ lorsque n est fixé et connu.
Pour tout entier $0 < \ell \leq 2^n - 1$, on écrit ℓ en base 2 **en plaçant le bit de poids faible à gauche**. On note alors $\nu(\ell)$ la position du premier bit à 1 dans cette écriture binaire, en partant de 0 ; et $\nu'(\ell)$ la position du deuxième bit à 1. Par exemple :

$$3 \text{ s'écrit } 11 \implies \nu(3) = 0, \nu'(3) = 1$$

$$26 \text{ s'écrit } 01011 \implies \nu(26) = 1, \nu'(26) = 3$$

Notons que $\nu(0)$ n'est pas défini, de même que $\nu'(\ell)$ si ℓ est une puissance de 2 (et n'a donc qu'un seul bit à 1).

Question 1. Soit un système de $m = n$ équations à n variables. Montrer qu'on peut énumérer (exactement) toutes ses solutions en $O(n^3 2^n)$ opérations.

Le code de Gray à n bits est une liste de 2^n vecteurs générée récursivement de la manière suivante :

- Pour $n = 1$: renvoyer la liste à deux éléments $\big[(0), (1)\big]$
- Pour $n > 1$: soit $\big[y_0, \ldots, y_{2^{n-1}-1}\big]$ le code de Gray à $n-1$ bits. Renvoyer la liste de vecteurs :

$$\big[y_0 \| 0, \ \ y_1 \| 0, \ \ \ldots, \ \ y_{2^{n-1}-1} \| 0, \ \ y_{2^{n-1}-1} \| 1, \ \ \ldots, \ \ y_0 \| 1\big]$$

  où $\|$ est une concaténation (par exemple $(0,1,1)\|0 = (0,1,1,0)$)

Lorsque n est fixé, on note $\mathsf{Gray}(n, t)$ le t-ème élément de la liste, compté à partir de 0.

Question 2.
1. Donner le code de Gray pour $n = 3$
2. Montrer que pour tout n, le code de Gray à n bits contient chaque vecteur de $(\mathbb{Z}/2\mathbb{Z})^n$ exactement une fois
3. Montrer que pour tout $1 \leq t < 2^n$, $\mathsf{Gray}(n, t) = \mathsf{Gray}(n, t-1) + \mathbf{e}^n_{\nu(t)}$

Indice : on utilisera que $\nu(t) = v$ si et seulement si t s'écrit sous la forme $k2^v$ avec k impair.

Si $f(\mathbf{x})$ est une fonction quadratique booléenne en n variables, sa *dérivée en* x_i, notée $\frac{\partial f}{\partial i}$, est la fonction :

$$\frac{\partial f}{\partial i} : \mathbf{x} \mapsto f(\mathbf{x} + \mathbf{e}_i^n) + f(\mathbf{x})$$

On suppose dans la suite que calculer ν, ν' ou incrémenter un compteur coûte une seule opération.

Question 3. 1. Montrer que $\frac{\partial f}{\partial i}$ est une fonction affine sur $(\mathbb{Z}/2\mathbb{Z})^n$.

2. En déduire un algorithme qui énumère tous les zéros de f en $O(n2^n)$ opérations au lieu de $O(n^2 2^n)$.
   Indice : on utilisera un code de Gray pour énumérer les vecteurs de $(\mathbb{Z}/2\mathbb{Z})^n$.

Question 4. Soit $t \geq 1$ une entrée du code de Gray. Soit s le plus petit entier strictement supérieur à t tel que $\nu(s) = \nu(t)$. Montrer que :

$$\mathsf{Gray}(n, t) + \mathsf{Gray}(n, s-1) = e^n_{\nu'(s)}$$

Comment interpréter ce résultat ?

Indice : on utilisera que si t s'écrit sous la forme $k2^v$ avec k impair, alors $\nu'(t) = \nu(t - 2^v)$.

Question 5. En déduire une modification de l'algorithme précédent pour énumérer tous les zéros de f en $O(2^n)$ opérations.

Question 6. En utilisant la question précédente, donner un algorithme pour résoudre un système de $m = n$ équations en n variables, qui utilise $O((\log n)2^n)$ opérations en moyenne.

Treillis distributifs

Un ensemble E muni de deux lois de composition interne $\vee$ et $\wedge$ est un *treillis distributif* si les conditions suivantes sont satisfaites.

1. **Associativité.** $\forall a, b, c \in E$, $(a \vee b) \vee c = a \vee (b \vee c)$, et $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
2. **Commutativité.** $\forall a, b \in E$, $a \vee b = b \vee a$, et $a \wedge b = b \wedge a$.
3. **Distributivité.** $\forall a, b, c \in E$, $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$, et $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$.
4. **Absorption.** $\forall a, b \in E$, $a \vee (a \wedge b) = a$, et $a \wedge (a \vee b) = a$.

Un treillis distributif $(E, \vee, \wedge)$ est dit *fini* si E est fini.

Exemples de treillis distributifs :

— $(\mathcal{P}(S), \cup, \cap)$, où S est un ensemble quelconque, et $\mathcal{P}(S)$ l'ensemble de ses sous-ensembles.

— $(\mathbb{Z}^d, \max_d, \min_d)$, pour $d \in \mathbb{N}^*$ et $\max_d : \mathbb{Z}^d \times \mathbb{Z}^d \to \mathbb{Z}^d$ défini par $\max_d((x_i)_{i=1}^d, (y_i)_{i=1}^d) \mapsto (\max(x_i, y_i))_{i=1}^d$, similairement pour $\min_d$.

On admet que ces exemples sont valides, on ne demande pas de les vérifier.

Question 1. Donner un exemple de treillis distributif à trois éléments.

Question 2. Étant donné un treillis distributif $(E, \vee, \wedge)$, on définit la relation $\leq$ sur E par : $a \leq b$ si et seulement si $a \wedge b = a$. Montrer que $\leq$ est une relation d'ordre partiel. Montrer que, de plus, toute paire (a, b) d'éléments de $(E, \leq)$ admet une borne supérieure (c'est-à-dire : l'ensemble des majorants de $\{a, b\}$ est non-vide et admet un minimum) et une borne inférieure (c'est-à-dire : l'ensemble des minorants est non-vide et admet un maximum).

Question 3. On dit qu'un ordre partiel sur E obtenu comme dans la question précédente est *issu* du treillis distributif $(E, \vee, \wedge)$. Donner un exemple d'ordre partiel qui ne peut pas être issu d'un treillis distributif.

Morphisme. Soit A, B deux treillis distributifs. Une application $\varphi : A \to B$ est un *morphisme* de treillis si pour tout $a, a' \in A$, $\varphi(a \wedge_A a') = \varphi(a) \wedge_B \varphi(a')$, et $\varphi(a \vee_A a') = \varphi(a) \vee_B \varphi(a')$.
Plongement. On dit que A se *plonge* dans B s'il existe un morphisme injectif de A dans B.
Dimension. La *dimension* $\dim(E)$ d'un treillis distributif E est le plus petit entier $d \in \mathbb{N}$, s'il existe, tel que E se plonge dans $(\mathbb{Z}^d, \max_d, \min_d)$. Si un tel d n'existe pas, on dit que la dimension est infinie.

Question 4. Soit S un ensemble fini. Montrer que la dimension de $(\mathcal{P}(S), \cup, \cap)$ est finie.

Dans la suite, on pose $(E, \vee, \wedge)$ un treillis distributif fini. On dit qu'un élément a est *irréductible* si $a = a_1 \vee a_2$ implique $a = a_1$ ou $a = a_2$.

Question 5. Soit $b \in E$, et soit $\{a_1, \ldots, a_k\}$ l'ensemble des éléments irréductibles inférieurs ou égaux à b pour l'ordre de la question 2. Montrer $a_1 \vee \cdots \vee a_k = b$.
Indication : on peut regarder d'abord le cas $(E, \vee, \wedge) = (\mathcal{P}(S), \cup, \cap)$, et s'en inspirer pour le cas général.

Question 6. Construire un plongement de E dans $(\mathcal{P}(E), \cup, \cap)$. En déduire que la dimension d'un treillis distributif fini est finie.

Couvrir. Soit a et b deux éléments d'un treillis distributif $(E, \vee, \wedge)$, et $<$ la relation d'ordre strict correspondant à l'ordre partiel de la question 2 (c'est-à-dire : $a < b \Leftrightarrow (a \wedge b = a$ et $a \neq b)$. On dit que b *couvre* a, noté $a \prec b$, si $a < b$ et $\neg(\exists c, a < c < b)$.
Couverture. La *couverture* de b est : $\mathsf{couv}(b) = |\{a : a \prec b\}|$.

Question 7. Soit a_1, a_2, b distincts tels que $a_1 \prec b$ et $a_2 \prec b$. Montrer $a_1 \vee a_2 = b$.

Question 8. Soit $E \subset \mathbb{Z}^d$ un sous-ensemble fini de $\mathbb{Z}^d$. On se place dans le treillis distributif $(E, \max_d, \min_d)$. Soit $b \in E$. Montrer $\mathsf{couv}(b) \leq d$.

Question 9. Soit E un treillis distributif fini. Montrer $\dim E \geq \max_{a \in E} \mathsf{couv}(a)$.

> Soit $(S, \leq)$ un ordre partiel fini.
> **Chaîne.** Une *chaîne* est un ensemble d'éléments de S deux à deux comparables pour $\leq$.
> **Antichaîne.** Une *antichaîne* est un ensemble d'éléments de S deux à deux incomparables pour $\leq$.
> **Idéal.** Un *idéal* est un ensemble $I \subseteq S$ tel que $b \in I \Rightarrow \forall a \leq b, a \in I$.
> **Théorème** *(Dilworth).* Si k est la cardinalité de la plus grande antichaîne de S, alors il existe une partition de S en k chaînes.

Question 10. Soit $\mathsf{Id}(S)$ l'ensemble des idéaux de S. Montrer que $(\mathsf{Id}(S), \cup, \cap)$ est un treillis distributif.

Question 11. En admettant le théorème de Dilworth, montrer :

$$\dim \mathsf{Id}(S) = \max_{I \in \mathsf{Id}(S)} \mathsf{couv}(I).$$

Indication : montrer que $\max_{I \in \mathsf{Id}(S)} \mathsf{couv}(I)$ est égal à la taille de la plus grande antichaîne dans S.