CONTRÔLE "GRAPHES AVANCÉS"
PARTIE "MATROÏDES"
2022-2023

Tout objet électronique (smartphone, tablette, ordinateur, calculatrice, etc.) interdit.

Tout document papier autorisé.

1. Caractérisation des matroïdes par les circuits

Soit V un ensemble fini (non vide), et soit $\mathcal{C}$ une collection de parties non vides de V telle qu'aucune partie en contienne une autre : pour tous $C, C' \in \mathcal{C}$, si $C \neq C'$ alors $C \setminus C'$ et $C' \setminus C$ sont tous deux non vides. L'objet de cet exercice est de démontrer que les deux propriétés suivantes sont alors équivalentes :

(i) $\mathcal{C}$ est l'ensemble des circuits d'un matroïde.
(ii) pour tous $C, C' \in \mathcal{C}$ tels que $C \neq C'$ et pour tout $x \in C \cap C'$, il existe $C'' \subseteq (C \cup C') \setminus \{x\}$ tel que $C'' \in \mathcal{C}$.

1.1. **Preuve de (i) $\Longrightarrow$ (ii).** On rappelle qu'il a été vu en exercice que, pour un matroïde, si C et C' sont deux circuits, alors $r(C \cup C') \leqslant |C \cup C'| - 2$.

Question 1. *Expliquer pourquoi cela permet de montrer l'implication* (i) $\Longrightarrow$ (ii).

1.2. **Preuve de (ii) $\Longrightarrow$ (i).** On suppose que la collection $\mathcal{C}$ vérifie (ii). L'objectif est de montrer que $\mathcal{C}$ est la collection des circuits d'un matroïde. Posons $\mathcal{I}$ l'ensemble des parties S de V ne contenant aucun C dans $\mathcal{C}$.

Considérons $S, T \in \mathcal{I}$ tels que $|S| < |T|$.

Question 2. *Soit $T' \in \mathcal{I}$ tel que $T' \subseteq S \cup T$. Supposons $S \setminus T' \neq \varnothing$ et soit $x \in S \setminus T'$. Montrer que $T' + x \in \mathcal{I}$ ou qu'il existe $y \in T' \setminus S$ tel que $T' + x - y \in \mathcal{I}$.*

Question 3. *En déduire qu'il existe $U \in \mathcal{I}$ tel que $S \subseteq U \subseteq S \cup T$ et $U \neq S$.*

Question 4. *Montrer que $(V, \mathcal{I})$ est un matroïde.*

Question 5. *Montrer que $\mathcal{C}$ est exactement l'ensemble des circuits de $(V, \mathcal{I})$.*

2. Matroïdes "secret-sharing"

La notation suivante sera utilisée : pour A une matrice et S un sous-ensemble de ses colonnes, A_S est la matrice restreinte aux colonnes dans S.

Soient E et Σ deux ensembles finis (non vides). (Voir E comme un ensemble d'"éléments" et Σ comme un ensemble de "symboles".) On considère une matrice $A = (a_{ie}) \in \Sigma^{[m] \times E}$: la matrice A est à m lignes, ses entrées sont prises dans Σ et ses colonnes sont indicées par les éléments de E. Pour $i \in [m]$, $e \in E$ et $S \subseteq E \setminus \{e\}$, on pose

$$n(i, e, S) = \left\{ a_{je} \colon j \in [m] \text{ et } a_{jf} = a_{if} \text{ pour tout } f \in S \right\}.$$

C'est donc l'ensemble des symboles que l'on voit sur la colonne e de la restriction de la matrice $A_{S\cup\{e\}}$ aux lignes que l'on ne peut distinguer de la ligne i dans A_S.

Une telle matrice A est *secret-sharing* si pour chaque paire (e,S) telle que $e \in E$ et $S \subseteq E \setminus \{e\}$, on est dans l'un de ces deux cas :

- $|n(1,e,S)| = |n(2,e,S)| = \cdots = |n(m,e,S)| = 1$.
- $n(1,e,S) = n(2,e,S) = \cdots = n(m,e,S) = \Sigma$.

Ces matrices sont étudiées en théorie de l'information.

Soit $\mathcal{I}$ l'ensemble des parties S de E telles que le nombre de lignes distinctes de la matrice A_S est $|\Sigma|^{|S|}$.

Question 6. *Montrer que $(E,\mathcal{I})$ est un matroïde.*

Question 7. *Montrer que le rang d'une partie S de E est égal au logarithme en base $|\Sigma|$ du nombre de lignes distinctes de A_S.*

3. Couplage et couverture dans les matroïdes

3.1. **Petit résultat préliminaire.** Soit $M = (V,\mathcal{I})$ un matroïde. Soit S une partie de V telle que $x \notin \mathrm{span}(S - x)$ pour tout $x \in S$.

Question 8. *Montrer que S est un indépendant.*

Le résultat de cette question pourra être utile pour répondre à la question 10.

3.2. **Un théorème de Lovász.** Soit $M = (V,\mathcal{I})$ un matroïde et $G = (V,E)$ un graphe (dont les sommets sont les éléments du matroïde). On suppose que pour toute arête $uv \in E$, la paire $\{u,v\}$ est un indépendant de M.

Un couplage C de G est *matroïdal* si l'ensemble des sommets couverts par C est un indépendant de M. De manière équivalente, C est un couplage matroïdal si et seulement si $r_M(V(C)) = 2|C|$. Le cardinal maximal d'un couplage matroïdal est noté $\nu_M(G)$.

Un sous-ensemble F d'arêtes de G est une *couverture matroïdale* si $\mathrm{span}(V(F)) = V$. Le cardinal minimal d'une couverture matroïdale est noté $\rho_M(G)$.

L'objet de cet exercice est de démontrer le théorème suivant, dû à Lovász (1980).

Théorème. *Si G est sans sommet isolé, alors $\nu_M(G) + \rho_M(G) = r_M(V)$.*

(Le cas particulier de ce théorème lorsque M est le matroïde trivial — toute partie de V est indépendante — est un théorème classique de Gallai de 1932.)

Question 9. *Démontrer que l'on a toujours $\nu_M(G)+\rho_M(G) \leqslant r_M(V)$. (On pourra considérer un couplage matroïdal C tel que $|C| = \nu_M(G)$ et une base de M contenant $V(C)$.)*

Soit F une couverture matroïdale telle que $|F| = \rho_M(G)$. Exécuter l'algorithme suivant :

- $C \leftarrow F$.
- Tant qu'il existe $e \in C$ tel que $r_M(V(C-e)) \geqslant r_M(V(C)) - 1$, faire $C \leftarrow C - e$.

Question 10. *Montrer que lorsque cet algorithme se termine, C est un couplage matroïdal. (On pourra utiliser le résultat de la question 8.)*

Question 11. *En déduire que $\nu_M(G) + \rho_M(G) \geqslant r_M(V)$.*