MATROÏDES — COMPLÉMENT SUR LA DUALITÉ

JEAN-SÉBASTIEN SERENI

Table des matières

Dans tout ce document, E est un ensemble fini et $\mathscr{M}$ un matroïde sur E. Posons $\mathcal{I} \coloneqq \mathcal{I}(\mathscr{M})$, $\mathscr{C} \coloneqq \mathscr{C}(\mathscr{M})$, $\mathscr{B} \coloneqq \mathscr{B}(\mathscr{M})$ et $r \coloneqq r_{\mathscr{M}}$.

1. Deux propriétés utiles

1.1. La propriété de circuit unique.

Proposition 1. *Soient I un ensemble indépendant dans M et e un élément de $\mathscr{M}$ tels que $I + e \notin \mathcal{I}$. Alors il existe un et un seul circuit de $\mathscr{M}$ contenu dans $I + e$.*

Démonstration. Comme $I + e \notin \mathcal{I}$, il existe un circuit $C \in \mathscr{C}$ contenu dans $I + e$. Supposons par l'absurde qu'il existe un circuit $C' \in \mathscr{C} \setminus \{C\}$ contenu dans $I + e$. Nécessairement, $e \in C \cap C'$. La propriété d'élimination (C3) implique l'existence d'un circuit de M contenu dans $(C \cup C') - e$. Mais $(C \cup C') - e \subseteq I \in \mathcal{I}$, ce qui est une contradiction. □

1.2. L'axiome d'échange « inversé ».

Proposition 2. *Soient B_0 et B_1 deux bases de $\mathscr{M}$. Pour tout $f \in B_1 \setminus B_0$, il existe $e \in B_0 \setminus B_1$ tel que $(B_0 - e) + f \in \mathscr{B}$.*

Démonstration. L'ensemble B_0 étant une base de $\mathscr{M}$, il suit que $B_0 + f \notin \mathcal{I}$. Ainsi, la proposition 1 implique qu'il existe un et un seul circuit C de $\mathscr{M}$ contenu dans $B_0 + f$. Par ailleurs, $\{f\} \in \mathcal{I}$ car $\{f\} \subseteq B_1 \in \mathcal{I}$, donc il existe $e \in C - f$. En conséquence, l'ensemble $(B_0 - e) + f$ ne contient pas de circuit, et est donc indépendant. Il s'agit donc d'une base de $\mathscr{M}$ puisque sa cardinalité est égale à celle de B_0. □

2. Dual d'un matroïde

Soit

$$\mathscr{B}^* \coloneqq \{E \setminus B \,:\, B \in \mathscr{B}\}.$$

Théorème 3. *L'ensemble $\mathscr{B}^*$ est la famille de bases d'un matroïde sur E.*

Date: 10 février 2012. Ce fichier contient notamment la solution des exercices 4 et 5 de la feuille d'exercices.

Démonstration. D'après le théorème 11 du cours, il nous suffit de prouver que $\mathscr{B}^*$ vérifie les propriétés (B1) et (B2). Tout d'abord, $\mathscr{B}^* \neq \emptyset$ car $\mathscr{B} \neq \emptyset$ puisque $\mathscr{B}$ vérifie (B1). Il nous reste à montrer que $\mathscr{B}^*$ satisfait (B2).

Soient B_0 et B_1 deux éléments de $\mathscr{B}^*$ et soit $e \in B_0 \setminus B_1$. Nous devons prouver l'existence d'un élément $f \in B_1 \setminus B_0$ tel que $(B_0 - e) + f \in \mathscr{B}^*$.

Par définition, pour $i \in \{0,1\}$ il existe $B'_i \in \mathscr{B}$ tel que $B_i = E \setminus B'_i$. Donc $e \in B_0 \setminus B_1 = B'_1 \setminus B'_0$.[1] D'après la proposition 2, il existe $f \in B'_0 \setminus B'_1$ tel que $(B'_0 - f) + e \in \mathscr{B}$. Comme $B'_0 \setminus B'_1 = B_1 \setminus B_0$, il suffit de remarquer que $E \setminus ((B'_0 - f) + e) = (B_0 - e) + f$ pour conclure la démonstration. □

La dualité de matroïdes est une opération involutive.

Proposition 4. $(\mathscr{M}^*)^* = \mathscr{M}$.

Posons $r^* := r_{\mathscr{M}^*}$, i.e. r^* est la fonction de rang du matroïde dual de $\mathscr{M}$. Alors, $r(\mathscr{M}) + r^*(\mathscr{M}^*) = |E|$. En fait, il est possible d'expliciter r^* en fonction de r. Avant de voir cela, notons deux faits utiles.

Remarque 1. Les faits suivants découlent directement des définitions.

– *Un ensemble $X \subseteq E$ est indépendant dans $\mathscr{M}^*$ si, et seulement si, $E \setminus X$ contient une base de $\mathscr{M}$.*
– *Si $X \subseteq E$ et $I^* \subseteq X$ avec $I^* \in \mathcal{I}(\mathscr{M}^*)$ tel que $|I^*| = r^*(X)$, alors toute base B de $\mathscr{M}$ contenue dans $E \setminus I^*$ contient $X \setminus I^*$.* En effet, sinon, il existe une base B de $\mathscr{M}$ contenue dans $E \setminus I^*$ et un élément x dans $X \setminus I^*$ tels que $x \notin B$. Dans ce cas, $I^* + x \in \mathcal{I}(\mathscr{M}^*)$ et $I^* + x \subseteq X$, ce qui contredit le fait que $|I^*| = r^*(X)$.

Nous somme prêts pour démontrer la formule suivante.

Théorème 5. *Pour tout sous-ensemble X de E,*

$$r^*(X) = |X| + r(E \setminus X) - r(\mathscr{M}). \tag{5.1}$$

Démonstration. Soit $X \subseteq E$. Soit I^* un ensemble indépendant de $\mathscr{M}^*$ contenu dans X tel que $r^*(X) = |I^*|$. Comme $I^* \in \mathcal{I}(\mathscr{M}^*)$, il existe une base de $\mathscr{M}$ contenue dans $(E \setminus I^*)$. Ainsi, $r(E \setminus I^*) = r(\mathscr{M})$.

Soit I un ensemble indépendant de $\mathscr{M}$ contenu dans $E \setminus X$ tel que $r(E \setminus X) = |I|$. Soit B un ensemble indépendant de $\mathscr{M}$ qui

(1) contienne I ;
(2) soit contenu dans $E \setminus I^*$; et
(3) soit de taille maximale sujet à (i) et (ii).

Alors $r(E \setminus I^*) = r(B)$. Donc $r(B) = r(\mathscr{M})$, i.e. $|B| = r(\mathscr{M})$.

Prouver (5.1) revient à prouver que $r(E \setminus X) + |X| - r^*(X) = r(\mathscr{M})$, c'est-à-dire

$$|I| + |X| - |I^*| = |B|\,. \tag{5.2}$$

Par définition, $I = B \setminus X$ (car $r(E \setminus X) = |I|$ et $I \subseteq B \in \mathcal{I}$). Pour obtenir (5.2) il suffit donc que $I^* = X \setminus B$, ce qui est vrai d'après la remarque 1. □

1. Ici et plus loin, ne pas hésiter à faire un dessin.

3. Hyperplans et dualité

Définition 6. Soit $\mathscr{M} = (E,\mathcal{I})$ un matroïde. Un « hyperplan » de $\mathscr{M}$ est un sous-ensemble H de E tel que $r_{\mathscr{M}}(H) < r_{\mathscr{M}}(E)$ et H est maximal pour cette propriété, c'est-à-dire : $r_{\mathscr{M}}(H+e) = r_{\mathscr{M}}(E)$ pour tout $e \in E \setminus H$.

Soit $\mathscr{M} = (E,\mathcal{I})$ un matroïde. Les circuits de $\mathscr{M}^*$ sont appelés « co-circuits de $\mathscr{M}$ ». La collection des co-circuits de $\mathscr{M}$ est donc $\mathscr{C}(\mathscr{M}^*)$, que l'on notera également $\mathscr{C}^*(\mathscr{M})$. Les singletons de E qui sont des boucles de $\mathscr{M}^*$, c'est-à-dire les singletons de E qui sont contenus dans *toutes* les bases de $\mathscr{M}$, sont les « co-boucles de $\mathscr{M}$ ». Le résultat suivant donne une caractérisation des co-circuits d'un matroïde.

Lemme 7. *Soient $\mathscr{M} = (E,\mathcal{I})$ un matroïde et C^* un sous-ensemble de E. Alors C^* est un co-circuit de $\mathscr{M}$ si, et seulement si, $E \setminus C^*$ est un hyperplan de $\mathscr{M}$.*

Démonstration. Nous notons r la fonction de rang de $\mathscr{M}$ et r^* celle de $\mathscr{M}^*$.

Supposons que $C^* \in \mathscr{C}^*(\mathscr{M})$. Ainsi, C^* est un sous-ensemble de E tel que $r^*(C^*) = |C^*| - 1$. Appliquons le théorème 5 à $\mathscr{M}$ avec $X = C^*$. Alors

$$\begin{aligned} r(E \setminus C^*) &= r^*(C^*) - |C^*| + r(\mathscr{M}) \\ &= |C^*| - 1 - |C^*| + r(\mathscr{M}) = r(\mathscr{M}) - 1. \end{aligned}$$

Il reste à prouver que $r((E \setminus C^*) + e) = r(\mathscr{M})$ pour tout $e \in C^*$. Or $r^*(C^* - e) = |C^*| - 1$ pour tout $e \in C^*$ puisque C^* est un circuit de $\mathscr{M}^*$. Par conséquent, le théorème 5 appliqué à $\mathscr{M}$ avec cette fois $X = C^* - e$ où $e \in C^*$ entraîne que

$$\begin{aligned} r((E \setminus C^*) + e) = r(E \setminus (C^* - e)) &= r^*(C^* - e) - |C^* - e| + r(\mathscr{M}) \\ &= |C^*| - 1 - (|C^*| - 1) + r(\mathscr{M}) = r(\mathscr{M}). \end{aligned}$$

Réciproquement, supposons que $E \setminus C^*$ soit un hyperplan de $\mathscr{M}$. Les mêmes applications du théorème 5 que précédemment nous assurent que $r^*(C^*) = |C^*| - 1$ et $r^*(C^* - e) = |C^*| - 1$ pour tout $e \in C^*$, c'est-à-dire $C^* \in \mathscr{C}^*(\mathscr{M})$. □

Une propriété importante concernant l'intersection des circuits et des co-circuits d'un matroïdes est la suivante.

Proposition 8. *Soit $\mathscr{M} = (E,\mathcal{I})$ un matroïde. Si $C \in \mathscr{C}(\mathscr{M})$ et $C^* \in \mathscr{C}^*(\mathscr{M})$, alors $|C \cap C^*| \neq 1$.*

Démonstration. Posons $r \coloneqq r_{\mathscr{M}}$ et $r^* \coloneqq r_{\mathscr{M}^*}$.

Supposons par l'absurde que $C \cap C^* = \{e\}$. Notons que $r(C) = |C| - 1 = r(C - e)$ puisque $C - e \in \mathcal{I}$. De plus, comme $e \in C^*$, le lemme 7 implique que $r(\mathscr{M}) = r((E \setminus C^*) + e) = r(E \setminus (C^* - e))$. En conséquent,

$$r(C) + r(\mathscr{M}) = r(C - e) + r(E \setminus (C^* - e)) = r(C \cap (E \setminus C^*)) + r(C \cup (E \setminus C^*)).$$

Mais, par sous-modularité de la fonction de rang,

$$r(C \cap (E \setminus C^*)) + r(C \cup (E \setminus C^*)) \leq r(C) + r(E \setminus C^*).$$

On obtient ainsi

$$r(C) + r(\mathscr{M}) \leq r(C) + r(E \setminus C^*) = r(C) + r(\mathscr{M}) - 1,$$

ce qui est une contradiction. □

Nous terminons cette section avec un exercice sur le dual de la somme directe de deux matroïdes.

Exercice 9. Soient $\mathscr{M}_1$ et M_2 deux matroïdes tels que $E(\mathscr{M}_1) \cap E(\mathscr{M}_2) = \emptyset$. À l'aide de la proposition 24 du cours, démontrez que $(\mathscr{M}_1 \oplus \mathscr{M}_2)^* = \mathscr{M}_1^* \oplus \mathscr{M}_2^*$.

4. Dual d'un matroïde graphique

Définition 10. Soit G un graphe plan (c'est-à-dire un graphe planaire plongé dans le plan). Le « dual géométrique » (ou « graphe dual ») de G , noté G^*, s'obtient de la façon suivante. Pour chaque face f de G, le graphe G^* comporte un sommet, noté f^*. Deux sommets f^* et g^* de G^* sont adjacents si, et seulement si, les faces correspondantes f et g de G partagent une arête.

De manière générale, étant donné un graphe plan G il existe un plongement plan naturel de son graphe dual G^*. De plus, ce plongement naturel fournit une bijection naturelle entre les arêtes de G et celles de G^*. En particulier, notons que si e est un « pont » de G, c'est-à-dire une arête e telle que le nombre de composantes connexes de $G - e$ soit strictement supérieur à celui de G, alors e^* est une boucle de G^*. De façon similaire, l'arête de G^* correspondant à une boucle de G est un pont de G^*.

Pour un graphe G, le matroïde graphique associé à G est noté $\mathscr{M}(G)$. Afin d'alléger l'écriture, nous notons $\mathscr{M}^*(G)$ le dual du matroïde graphique associé à G, i.e. $\mathscr{M}^*(G) \coloneqq (\mathscr{M}(G))^*$. De plus, nous identifions les éléments de $\mathscr{M}(G)$ et ceux de $\mathscr{M}^*(G)$ via la bijection naturelle entre les arêtes de G et celles de G^*.

Les matroïdes associés à un graphe plan et son graphe dual sont reliés par la relation suivante.

Théorème 11. *Soit G un graphe plan connexe. Le matroïde graphique associé au graphe dual G^* de G est isomorphe au dual du matroïde graphique associé à G. En d'autres termes, $\mathscr{M}(G^*) = \mathscr{M}^*(G)$.*

Démonstration. Comme $(G^*)^* = G^*$, il est suffisant de démontrer que pour tout arbre couvrant T de G, les arêtes de G qui ne sont pas dans T forment un arbre couvrant de G^*.

Soit B un ensemble d'arêtes de G formant un arbre couvrant de G. Soit B' l'ensemble des arêtes de G qui ne sont pas dans B. Nous commençons par prouver que les arêtes qui appartiennent à B' constituent un sous-graphe acyclique de G^*. Supposons, par l'absurde, que les arêtes dans B' contiennent un circuit C. Alors, il existe deux sommets de u et v de G tels que, dans le plan, u soit à l'intérieur de C et v à l'extérieur de C.[2] Ainsi, tout chemin de u à v intersecte le circuit C. En particulier, comme B forme un arbre couvrant de G, il existe une arête de B contenu dans C, lui-même contenu dans B', ce qui est une contradiction.

Pour conclure, nous appliquons la formule d'Euler. Soient n, e et f le nombre de sommets de G, le nombre d'arêtes de G et le nombre de faces de G, respectivement. La formule d'Euler (pour les graphes planaires) assure que $n - e + f = 2$. Soit n^* le nombre de sommets de G^*.

Tout d'abord, $n^* = f = e - n + 2$. En outre, $|B| = n - 1$ car B est un arbre couvrant de G. Donc $|B'| = e - n + 1$. Ainsi, le sous-graphe de G^* formé par les arêtes dans B' contient $n^* - 1$ arêtes. Comme il est acyclique, il couvre nécessairement au moins n^* sommets, c'est-à-dire tous les sommets de G^*. Ceci conclut la démonstration.[3] □

Nous obtenons ainsi le théorème suivant.

Théorème 12. *Si G est un graphe planaire, alors le dual du matroïde graphique associé à G est graphique.*

Les circuits du dual d'un matroïde graphique s'expriment en termes purement graphiques à l'aide des coupes. Soit G un graphe dont l'ensemble de sommets est V et l'ensemble d'arêtes est E. Si V_1 et V_2 sont deux sous-ensembles

2. Ceci utilise le théorème de Jordan.
3. Assurez-vous de pouvoir démontrer qu'un graphe acyclique avec $n - 1$ arêtes est connexe si, et seulement si, il possède n sommets.

disjoints de V, l'ensemble constitué des arêtes possédant un sommet extrémal dans V_1 et l'autre dans V_2 est noté $e(V_1, V_2)$. En d'autres termes,

$$e(V_1, V_2) \coloneqq \{(x_1, x_2) \in E \,:\, \forall i \in \{1,2\}, \quad x_i \in V_i\}\,.$$

Une *coupe* de G est un ensemble non vide d'arêtes $F \subseteq E$ tel que V puisse être partitionné en deux parts non vides V_1 et V_2 de sorte que $e(V_1, V_2) = F$. Une coupe F est *minimale* si, et seulement si, il n'existe pas de coupe strictement contenue dans F.

Lemme 13. *Soit G un graphe. Un ensemble F d'éléments de $\mathscr{M}^*(G)$ est un circuit dans $\mathscr{M}^*(G)$ si, et seulement si, les arêtes de G correspondant aux éléments dans F forment une coupe minimale de G.*

Démonstration. Identifier des sommets de G qui appartiennent à des composantes distinctes de G ne change pas la structure des cycles de G, et donc cela laisse $\mathscr{M}(G)$ inchangé. Nous pouvons ainsi supposer sans perte de généralité que G est connexe. Par ailleurs, nous ne ferons pas de distinction entre les arêtes de G et les éléments de $\mathscr{M}(G)$ (et donc ceux de $\mathscr{M}^*(G)$).

Tout d'abord, nous prouvons que si F est un circuit de $\mathscr{M}^*(G)$, alors F est une coupe minimale de G. Si le sous-graphe $G - F$ de G obtenu en supprimant les arêtes dans F était connexe, alors il existerait un arbre couvrant de G dont l'ensemble d'arêtes est contenu dans $E(\mathscr{M}) \setminus F$, et donc F serait indépendant dans $\mathscr{M}^*$, ce qui n'est pas le cas. Donc $G - F$ n'est pas connexe, i.e. F est une coupe de G. Il reste à montrer que cette coupe est minimale. Soit F' un sous-ensemble strict de F. Alors $F' \in \mathcal{I}(\mathscr{M}^*)$ car F est un circuit de $\mathscr{M}^*$. Donc il existe une base de $\mathscr{M}$ contenue dans $E(\mathscr{M}) \setminus F'$, c'est-à-dire un arbre couvrant de $G - F'$, le sous-graphe de G obtenu en enlevant les arêtes dans F'. Ainsi $G - F'$ est connexe et par conséquent F' n'est pas une coupe de G. La coupe F est donc bien minimale.

Réciproquement, prouvons que si F est une coupe minimale de G, alors F est un circuit de $\mathscr{M}^*(G)$. Soit (V_1, V_2) une partition de l'ensemble des sommets de G en deux parts non vides telle que $e(V_1, V_2) = F$. Toute base de $\mathscr{M}(G)$ est un arbre couvrant de G, et donc contient nécessairement un élément dans F. Ainsi, il n'existe pas de base de $\mathscr{M}$ contenu dans $E(\mathscr{M}) \setminus F$, et donc F n'est pas indépendant dans $\mathscr{M}^*$. Il ne reste plus qu'à prouver que $F - f \in \mathcal{I}(\mathscr{M}^*)$ pour tout $f \in F$. Or, pour tout $f \in F$, il existe une base B de $\mathscr{M}$ telle que $B \cap F = \{f\}$, c'est-à-dire $B \subseteq E(\mathscr{M}) \setminus (F - f)$. En effet, comme la coupe F est minimale, le sous-graphe $G[V_i]$ de G induit par les sommets dans V_i est connexe pour tout $i \in \{1,2\}$. Soit E_i l'ensemble d'arêtes d'un arbre couvrant de $G[V_i]$ pour $i \in \{1,2\}$. Alors $(V, (E_1 \cup E_2) + f)$ est un arbre couvrant de G dont l'ensemble d'arêtes est contenu dans $E(\mathscr{M}) \setminus (F - f)$, comme désiré. $\square$

Une question naturelle est de savoir si la classe des matroïdes graphiques est close sous l'opération de dualité. En d'autres termes, le dual d'un matroïde graphique est-il graphique ? Ceci n'est pas vrai en général.

Proposition 14. *Soient K_5 le graphe complet à 5 sommets et $K_{3,3}$ le graphe biparti complet avec 3 sommets dans chaque part. Les matroïdes $\mathscr{M}^*(K_5)$ et $\mathscr{M}^*(K_{3,3})$ ne sont pas graphiques.*

Démonstration. Supposons, par l'absurde, qu'il existe un graphe G tel que $\mathscr{M}^*(K_5)$ soit isomorphe à $\mathscr{M}(G)$. Comme précédemment, nous pouvons supposer que G est connexe. En particulier, le rang de $\mathscr{M}(G)$ est donc égal au nombre de sommets de G moins un. Ainsi, comme $\mathscr{M}(K_5)$ possède 10 éléments et a rang égal à 4, le matroïde G possède 10 arêtes et exactement 7 sommets. Le degré moyen de G est donc $20/7$, qui est strictement inférieur à 3. Par conséquent, G possède (au moins) un sommet v de degré au plus 2. Les arêtes incidentes à v forment une coupe minimale de G, qui a donc taille 1 ou 2. Ainsi, le lemme 13 assure que $\mathscr{M}^*(G)$ possède un circuit de taille au plus deux. Or $\mathscr{M}^*(G) = \mathscr{M}(K_5)$, et $\mathscr{M}(K_5)$ ne possède pas de circuit de taille au plus deux.

La démonstration dans le cas de $K_{3,3}$ est similaire.[4] $\square$

En fait, le théorème 12 admet une réciproque (que nous ne démontrerons pas).

Théorème 15. *Un graphe G est planaire si, et seulement si, $\mathscr{M}^*(G)$ est graphique.*

4. Exercice.