

MATROÏDES

JEAN-SÉBASTIEN SERENI

TABLE DES MATIÈRES

1. Quatre visions des matroïdes	1
2. Union de matroïdes	8
3. Algorithmes dans les matroïdes	9
4. Applications du théorème d'intersection	13
5. Représentabilité des matroïdes	18

1. QUATRE VISIONS DES MATROÏDES

1.1. Ensembles indépendants.

Définition 1. Un *matroïde* $\mathcal{M}$ est un couple $(E, \mathcal{I})$ où E est un ensemble fini et $\mathcal{I}$ une collection de parties de E telle que

- (I1) $\emptyset \in \mathcal{I}$;
- (I2) si $I_1 \in \mathcal{I}$ alors $I_0 \subseteq I_1 \Rightarrow I_0 \in \mathcal{I}$; et
- (I3) si $(I_0, I_1) \in \mathcal{I}^2$ alors $|I_0| < |I_1| \Rightarrow \exists e \in I_1 \setminus I_0$ tel que $I_0 \cup \{e\} \in \mathcal{I}$.

Exemple 2. Soit A une matrice de taille $m \times n$ à coefficients dans un corps $\mathbf{F}$. On note E l'ensemble des colonnes de A , et $\mathcal{I}$ la collection de sous-ensembles de E formant un système linéairement indépendant sur $\mathbf{F}$. Alors $\mathcal{M}_A := (E, \mathcal{I})$ est un matroïde. (Vérifiez-le!) Il s'agit du « matroïde vectoriel ».

1.2. Notations. Un ensemble satisfaisant la propriété (I2) est appelé « héréditaire ». La propriété (I3) est appelée « axiome d'augmentation ». Si $\mathcal{M} = (E, \mathcal{I})$ est un matroïde, on appelle « éléments de $\mathcal{M}$ » les membres de l'ensemble E . Les sous-ensembles de E qui appartiennent à $\mathcal{I}$ sont dits « indépendants ». Un sous-ensemble de E qui n'est pas indépendant est dit « dépendant ». De manière générale, on note $E(\mathcal{M}) := E$ et $\mathcal{I}(\mathcal{M}) := \mathcal{I}$. On dira également que « $\mathcal{M}$ est un matroïde sur E ».

Pour tout ensemble X et tout élément x , on note $X + x := X \cup \{x\}$ et $X - x := X \setminus \{x\}$. Si Y est un ensemble contenu dans X , l'on notera $Y \subseteq X$ alors que la notation $Y \subset X$ signifiera $Y \subseteq X$ et $Y \neq X$.

1.3. Circuits.

Définition 3. Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde. Un sous-ensemble C de E est un « circuit de $\mathcal{M}$ » si, et seulement si,

- $C \notin \mathcal{I}$; et
- $\forall e \in C, \quad C - e \in \mathcal{I}$.

L'ensemble de tous les circuits de $\mathcal{M}$ est noté $\mathcal{C}(\mathcal{M})$. Un élément $e \in E$ tel que $\{e\} \in \mathcal{C}$ est appelé « boucle ».

Date: 14 février 2012. Le fichier sera mis à jour au fur et à mesure de l'avancement des cours.

Remarque 1. Les circuits d'un matroïde sont donc les ensembles dépendants minimaux (au sens de l'inclusion). En particulier, l'on observe qu'un ensemble X est indépendant si, et seulement si, il ne contient pas de circuit — ceci découle directement de l'axiome d'hérédité (I2).

Les circuits possèdent des propriétés intéressantes, analogues à celles des ensembles indépendants. (Notons au passage que la collection des circuits d'un matroïde est déterminée par celle des ensembles indépendants, et *vice versa*.)

Lemme 4. Soient $\mathcal{M} = (E, \mathcal{I})$ un matroïde et $\mathcal{C}$ la famille de circuits de $\mathcal{M}$.

- (C1) $\emptyset \notin \mathcal{C}$;
- (C2) si $(C_0, C_1) \in \mathcal{C}^2$ et $C_0 \subseteq C_1$, alors $C_0 = C_1$; et
- (C3) si C_0 et C_1 sont deux circuits distincts de $\mathcal{M}$ possédant (au moins) un élément commun, alors pour tout $e \in C_0 \cap C_1$ il existe $C_2 \in \mathcal{C}$ tel que $C_2 \subseteq (C_0 \cup C_1) - e$.

Démonstration. Les propriétés (C1) et (C2) découlent directement de la définition d'un circuit et des propriétés (I1) et (I2). En particulier, si C est un circuit de $\mathcal{M}$ alors tout ensemble strictement contenu dans C est indépendant. Prouvons à présent (C3) par l'absurde : supposons que $X := (C_0 \cup C_1) - e$ ne contienne pas de circuit, c'est-à-dire $(C_0 \cup C_1) - e \in \mathcal{I}$.

Nous allons utiliser l'axiome d'augmentation (I3) afin d'obtenir une contradiction. Dans ce genre de situations, le schéma général est le suivant : (I3) nous permet « d'augmenter » par un élément de X tout ensemble indépendant I tel que $|I| < |X|$. On choisira pour I un ensemble maximal (au sens de l'inclusion) parmi tous les ensembles indépendants contenus dans X (et vérifiant certaines autres conditions notées (\$)). Si l'on parvient à prouver que $|I| < |X|$, l'on sait alors qu'il existe $x \in X \setminus I$ tel que $I + x \in \mathcal{I}$. Comme $I + x \subseteq X$ et $I \subset I + x$, l'on obtient une contradiction (pourvu que l'on sache que $I + x$ vérifie (\$), ce qui est généralement trivial).

Comme $C_0 \neq C_1$, la propriété (C2) implique l'existence d'un élément $f \in C_1 \setminus C_0$. Par définition d'un circuit, l'ensemble $C_1 - f$ est indépendant. Considérons tous les sous-ensembles de E qui

- (i) sont indépendants ;
- (ii) contiennent $C_1 - f$; et
- (iii) sont contenus dans $C_0 \cup C_1$.

Parmi tous les sous-ensembles de E vérifiant ces trois conditions, nous en choisissons un qui soit maximal (au sens de l'inclusion) et nous l'appelons I (notons qu'il existe bien des ensembles vérifiant les conditions (i), (ii) et (iii), comme l'ensemble $C_1 - f$).

Généralement, l'on écrit ceci de la manière suivante, qui est plus concise.

Soit I un ensemble indépendant maximal (au sens de l'inclusion) qui contienne $C_1 - f$ et qui soit contenu dans $C_0 \cup C_1$.

Pour obtenir une contradiction, il suffit d'exhiber un sous-ensemble I' de E qui vérifie les trois conditions (i), (ii) et (iii) et qui en outre contienne strictement l'ensemble I . Nous utiliserons pour cela l'axiome d'augmentation appliqué à I et $(C_0 \cup C_1) - e$.

Nous devons donc montrer que $|I| < |(C_0 \cup C_1) - e|$. Pour cela, nous allons trouver deux éléments appartenant à $C_0 \cup C_1$ mais pas à I . Tout d'abord, $f \notin I$ car $C_1 \in \mathcal{C}$ et $C_1 - f \subseteq I$. De plus, $C_0 \not\subseteq I$ (car $C_0 \in \mathcal{C}$) donc il existe un élément $g \in C_0 \setminus I$. En particulier, $g \neq f$ et ainsi $g \notin C_1 \subseteq I + f$. D'où

$$|I| \leq |(C_0 \cup C_1) \setminus \{f, g\}| = |C_0 \cup C_1| - 2 < |(C_0 \cup C_1) - e|.$$

D'après l'axiome d'augmentation (I3), il existe donc un élément $h \in ((C_0 \cup C_1) - e) \setminus I$ tel que $I + h \in \mathcal{I}$. L'ensemble $I + h$ vérifie bien les trois conditions (i), (ii) et (iii), et pourtant I est strictement contenu dans $I + h$: ceci contredit la maximalité de I .¹ $\square$

La propriété (C3) est appelée « axiome d'élimination ». Le terme « axiome » est utilisé car, comme nous allons le voir, les propriétés (C1)–(C3) caractérisent entièrement les ensembles pouvant être la famille de circuits d'un matroïde.

Théorème 5. *Soient E un ensemble fini et $\mathcal{C}$ une collection de sous-ensembles de E qui satisfait les propriétés (C1), (C2) et (C3). Soit $\mathcal{I}$ la collection formée par tous les sous-ensembles de E qui ne contiennent aucun élément de $\mathcal{C}$. Alors, $\mathcal{M} := (E, \mathcal{I})$ est un matroïde et $\mathcal{C}$ est la famille de circuits de $\mathcal{M}$.*

Démonstration. Nous devons prouver que $\mathcal{I}$ satisfait les propriétés (I1)–(I3). La propriété (I1) découle directement de (C1) et de la définition de $\mathcal{I}$. Cette dernière implique également directement (I2). Il reste à prouver que $\mathcal{I}$ satisfait (I3), ce que nous faisons par l'absurde.

Soient donc I_0 et I_1 deux éléments de $\mathcal{I}$ tels que $|I_0| < |I_1|$ et $I_0 + e \notin \mathcal{I}$ pour tout élément $e \in I_1 \setminus I_0$. Nous allons obtenir une contradiction grâce à l'axiome d'élimination (C3). Celui-ci nous garantit, sous certaines conditions, l'existence d'un élément de $\mathcal{C}$ contenu dans un certain ensemble ; nous allons faire en sorte que cet ensemble soit lui-même contenu dans un ensemble I_2 qui appartient à $\mathcal{I}$; ceci sera une contradiction.

Considérons tous les sous-ensembles de E qui

- (i) appartiennent à $\mathcal{I}$;
- (ii) sont de cardinalité strictement supérieure à $|I_0|$; et
- (iii) sont contenus dans $I_0 \cup I_1$.

Notons qu'il existe un sous-ensemble de E vérifiant ces trois conditions, à savoir I_1 . Parmi tous les sous-ensembles de E vérifiant (i), (ii) et (iii), nous en choisissons un dont l'intersection avec I_0 est la plus grande possible, et nous l'appelons I_2 . (Un tel choix est possible car I_0 est fini.)

Encore une fois, l'on écrit habituellement ceci de la manière suivante.

Soit I_2 un sous-ensemble de $I_0 \cup I_1$ contenu dans $\mathcal{I}$ tel que $|I_2| > |I_0|$ et $|I_0 \setminus I_2|$ soit minimal. (Un tel choix est possible car I_1 satisfait aux deux premières conditions.)

Nous savons par hypothèse que I_0 n'est pas contenu dans I_2 (sinon, il existerait un élément h de $I_1 \setminus I_0$ tel que $I_0 + h \in \mathcal{I}$). Fixons un élément $e \in I_0 \setminus I_2$.

Pour tout $f \in I_2 \setminus I_0$, soit $A_f := (I_2 - f) + e$. Comme $A_f \subseteq I_0 \cup I_1$ et $|I_0 \setminus A_f| < |I_0 \setminus I_2|$, il suit que $A_f \notin \mathcal{I}$. La définition de $\mathcal{I}$ implique alors l'existence d'un élément $C_f \in \mathcal{C}$ contenu dans A_f . En particulier, $e \in C_f$ et $f \notin C_f$. (Notons au passage que $I_2 \setminus I_0 \neq \emptyset$ car $|I_2| > |I_0|$ par définition de I_2 .)

Comme $I_0 \in \mathcal{I}$, il suit que $C_f \not\subseteq I_0$ pour tout élément $f \in I_2 \setminus I_0$. Ainsi², $C_f \cap (I_2 \setminus I_0) \neq \emptyset$ pour tout élément $f \in I_2 \setminus I_0$, car $((I_0 \cap I_2) + e) - f \subseteq I_1$. Par conséquent, il existe un élément $g \in C_f \cap (I_2 \setminus I_0)$.

Ainsi, C_f et C_g sont deux éléments distincts de $\mathcal{C}$ et $e \in C_f \cap C_g$. La propriété (C3) implique donc l'existence d'un élément $C \in \mathcal{C}$ contenu dans $(C_f \cup C_g) - e$, lui-même contenu dans I_2 . Ceci contredit le fait que $I_2 \in \mathcal{I}$. Ainsi, nous avons vérifié que $\mathcal{M} = (E, \mathcal{I})$ est bien un matroïde.

1. Ici, nous aurions pu choisir I de la façon suivante : soit I un ensemble de taille *maximum* parmi tous les sous-ensembles de E vérifiant (i), (ii) et (iii) — un tel choix est possible car il n'existe qu'un nombre *fini* de sous-ensembles vérifiant les trois conditions. Pour cette preuve en particulier, la contradiction s'obtient de la même manière, mais d'un point de vue plus général, il suffirait alors de trouver un sous-ensemble I' de E vérifiant les trois conditions et tel que $|I| < |I'|$ (sans nécessairement avoir $I \subset I'$).

2. Faire un dessin !

Enfin, le fait que $\mathcal{C}$ soit la famille de circuits de $\mathcal{M}$ découle directement de la définition de $\mathcal{I}$ et du fait que $\mathcal{C}$ satisfait la propriété (C2). (Prouvez formellement que $\mathcal{C}(\mathcal{M}) = \mathcal{C}$!) $\square$

Le lemme 4 et le théorème 5 impliquent directement le corollaire suivant.

Corollaire 6. *Soient E un ensemble fini et $\mathcal{C}$ une collection de sous-ensembles de E . Il existe un matroïde $\mathcal{M}$ sur E tel que $\mathcal{C}(\mathcal{M}) = \mathcal{C}$ si, et seulement si, $\mathcal{C}$ satisfait les propriétés (C1)–(C3).*

Exercice 7. Soit $G = (V, E)$ un graphe (fini). Soit $\mathcal{C}$ la collection de tous les sous-ensembles de E qui induisent dans G un cycle élémentaire.

- (i) Montrez que $\mathcal{C}$ est la famille de cycles d'un matroïde $\mathcal{M}$.
- (ii) Identifiez l'ensemble $\mathcal{I}(\mathcal{M})$.
- (iii) Prouvez (directement) que $\mathcal{I}(\mathcal{M})$ satisfait (I1)–(I3).

Un tel matroïde est appelé « matroïde graphique ».

1.4. Bases. La notion de base est duale à celle de circuit : si $\mathcal{M} = (E, \mathcal{I})$ est un matroïde, tout élément de $\mathcal{I}$ qui est maximal (au sens de l'inclusion) est appelé « base de $\mathcal{M}$ ». Ceci est formalisé ci-dessous.

Définition 8. Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde. Un sous-ensemble B de E est appelé « base de $\mathcal{M}$ » si, et seulement si,

- $B \in \mathcal{I}$; et
- $\forall e \in E \setminus B, \quad B + e \notin \mathcal{I}$.

La collection de toutes les bases de $\mathcal{M}$ est notée $\mathcal{B}(\mathcal{M})$.

Comme pour les circuits, les bases possèdent des propriétés importantes et permettent également de définir la notion de matroïde. Une première propriété remarquable (et utile) des bases d'un matroïde est qu'elles ont toutes la même cardinalité.

Proposition 9. *Soient $\mathcal{M} = (E, \mathcal{I})$ un matroïde et B_0 et B_1 deux bases de $\mathcal{M}$. Alors $|B_0| = |B_1|$.*

Démonstration. Procédons par contradiction : si $|B_0| < |B_1|$, alors (I3) entraîne l'existence d'un élément $e \in B_1 \setminus B_0$ tel que $B_0 + e \in \mathcal{I}$. Ceci contredit le fait que B_0 soit une base de $\mathcal{M}$. $\square$

Une manière courante d'utiliser la proposition 9 est la suivante :

si B est une base d'un matroïde $\mathcal{M} = (E, \mathcal{I})$, alors pour montrer qu'un ensemble B' est aussi une base de $\mathcal{M}$ il suffit de prouver que $B' \in \mathcal{I}$ et $|B'| = |B|$. C'est ce que nous allons faire dans la prochaine démonstration.

Lemme 10. *Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde et soit $\mathcal{B}$ la collection des bases de $\mathcal{M}$. Alors,*

- (B1) $\mathcal{B}$ n'est pas vide; et
- (B2) si B_0 et B_1 sont deux bases de $\mathcal{M}$ et si $e \in B_0 \setminus B_1$, alors il existe un élément $f \in B_1 \setminus B_0$ tel que $(B_0 - e) + f \in \mathcal{B}$.

Démonstration. La propriété (B1) découle directement du fait que $\mathcal{I}$ est non vide (par (I1)). Prouvons à présent que $\mathcal{B}$ satisfait (B2). Nous utiliserons pour cela la proposition 9.

Il suffit de noter que $B_0 - e \in \mathcal{I}$, d'après (I2). Comme $|B_0 - e| < |B_1|$ et $B_1 \in \mathcal{I}$, il existe $f \in B_1 - (B_0 - e)$ tel que $(B_0 - e) + f \in \mathcal{I}$ d'après l'axiome d'augmentation (I3). Notons que $e \neq f$ car $e \notin B_1$. Par conséquent, $|(B_0 - e) + f| = |B_0|$ et donc $(B_0 - e) + f \in \mathcal{B}$ d'après la proposition 9. $\square$

La propriété (B2) est appelée « axiome d'échange ». Les propriétés (B1) et (B2) caractérisent entièrement les familles qui peuvent être vues comme la famille de bases d'un matroïde.

Théorème 11. *Soient E un ensemble fini et $\mathcal{B}$ une collection de sous-ensembles de E satisfaisant les propriétés (B1) et (B2). Soit $\mathcal{I}$ la collection de tous les sous-ensembles de E contenu dans (au moins) un élément de $\mathcal{B}$. Alors $\mathcal{M} := (E, \mathcal{I})$ est un matroïde et $\mathcal{B}(\mathcal{M}) = \mathcal{B}$.*

Démonstration. Prouvons que $\mathcal{I}$ satisfait les propriétés (I1)–(I3). Tout d'abord, $\mathcal{I}$ est héréditaire par définition, et ainsi satisfait (I2). De plus, comme $\mathcal{B}$ n'est pas vide — d'après (B1) — il vient que $\emptyset \in \mathcal{I}$. Il reste à prouver que $\mathcal{I}$ satisfait (I3), ce que nous ferons en utilisant la contraposée de (I3). Avant cela, nous allons démontrer que tous les éléments de $\mathcal{B}$ ont la même cardinalité, ce qui nous sera utile par la suite³.

Supposons par l'absurde que $\mathcal{B}$ contienne des éléments de cardinalités différentes. Soient B_0 et B_1 deux éléments de $\mathcal{B}$ avec $|B_0| < |B_1|$ et tels que $B_0 \setminus B_1$ soit de taille minimum pour cette propriété. Tout d'abord, $B_0 \setminus B_1 \neq \emptyset$, car la propriété (B2) implique directement qu'aucun éléments de $\mathcal{B}$ n'est (strictement) inclus dans un autre élément de $\mathcal{B}$. Nous pouvons donc fixer un élément e appartenant à $B_0 \setminus B_1$. Par (B2), il existe un élément $f \in B_1 \setminus B_0$ tel que $(B_0 - e) + f \in \mathcal{B}$. Mais $|(B_0 - e) + f| = |B_0| < |B_1|$ et $|((B_0 - e) + f) \setminus B_1| < |B_0 \setminus B_1|$, ce qui contredit le choix du couple (B_0, B_1) .

Supposons qu'il existe deux éléments I_0 et I_1 de $\mathcal{I}$ tels que $I_0 + e \notin \mathcal{I}$ pour tout élément $e \in I_1 \setminus I_0$. Notre but est de prouver que $|I_0| \geq |I_1|$. Pour cela, nous allons trouver deux éléments B_0 et B_1 de $\mathcal{B}$ tels que

$$(1.1) \quad B_1 \setminus B_0 = I_1 \setminus I_0$$

et

$$(1.2) \quad B_0 \setminus B_1 \subseteq I_0 \setminus I_1.$$

Ceci fournira la conclusion souhaitée : en effet, il suffit alors de remarquer que comme $|B_0| = |B_1|$ d'après la proposition 9, il suit $|B_0 \setminus B_1| = |B_1 \setminus B_0|$ et ainsi (en utilisant (1.1) et (1.2)), $|I_1 \setminus I_0| \leq |I_0 \setminus I_1|$, ce qui donne le résultat voulu. Il nous reste donc à prouver l'existence de B_0 et B_1 .

Par définition de $\mathcal{I}$, il existe $B_0 \in \mathcal{B}$ tel que $I_0 \subseteq B_0$. De même, l'ensemble I_1 est contenu dans un élément B_1 de $\mathcal{B}$, que l'on peut choisir de sorte que $|B_1 \setminus (I_1 \cup B_0)|$ soit aussi petit que possible. Il suit que $B_1 \setminus (I_1 \cup B_0)$ est vide. En effet, s'il existait un élément $e \in B_1 \setminus (I_1 \cup B_0)$, alors la propriété (B2) entraînerait l'existence d'un élément $f \in B_0 \setminus B_1$ tel que $(B_1 - e) + f \in \mathcal{B}$. Or

$$|((B_1 - e) + f) \setminus (I_1 \cup B_0)| < |B_1 \setminus (I_1 \cup B_0)|$$

par définition de e et f , ce qui contredit le choix de B_1 . Ainsi, $B_1 \setminus (I_1 \cup B_0) = \emptyset$, c'est-à-dire $B_1 \setminus B_0 = I_1 \setminus B_0$. Pour établir l'équation (1.1), il nous suffit désormais de prouver que $I_1 \setminus B_0 = I_1 \setminus I_0$. Si cette égalité n'était pas vérifiée, alors il existerait un élément $e \in (I_1 \setminus I_0) \cap B_0$. Par conséquent, $I_0 + e \in \mathcal{I}$, ce qui est contraire à l'hypothèse. Ainsi, $B_1 \setminus B_0 = I_1 \setminus B_0 = I_1 \setminus I_0$, i.e. l'équation (1.1) est vérifiée.

Il reste à prouver que B_0 et B_1 satisfont (1.2). Pour cela, il est suffisant de montrer que $B_0 \setminus B_1 = I_0 \setminus B_1$. Procédons par contradiction : si l'égalité n'est pas vraie, alors il existe un élément $e \in B_0 \setminus (I_0 \cup B_1)$. La propriété (B2) implique alors l'existence d'un élément $f \in B_1 \setminus B_0$ tel que $(B_0 - e) + f \in \mathcal{B}$. Comme $e \notin I_0$, il suit alors que $I_0 + f \in \mathcal{I}$, ce qui contredit l'hypothèse (car $f \notin I_0$). Ceci prouve que B_0 et B_1 satisfont (1.2) et conclut la preuve. $\square$

3. Attention, impossible d'utiliser la proposition 9 ici. C'était l'exercice caché : repérer cette utilisation abusive et la corriger.

Le lemme 10 et le théorème 11 permettent d'énoncer le résultat suivant.

Corollaire 12. *Soient E un ensemble fini et $\mathcal{B}$ une collection de sous-ensembles de E . Il existe un matroïde $\mathcal{M}$ tel que $\mathcal{B}(M) = \mathcal{B}$ si, et seulement si, $\mathcal{B}$ satisfait les propriétés (B1) et (B2).*

1.5. **Rang.** Soient $\mathcal{M}$ un matroïde et X un sous-ensemble de $E(\mathcal{M})$. D'après la propriété (I3), tous les sous-ensembles maximaux (au sens de l'inclusion) de X qui sont indépendants (dans $\mathcal{M}$) ont la même taille. Ceci permet de donner la définition suivante.

Définition 13. Soit $\mathcal{M}$ un matroïde. La « fonction de rang » de $\mathcal{M}$, notée $r_{\mathcal{M}}$ est la fonction qui associe à tout sous-ensemble X de $E(\mathcal{M})$ la taille d'un sous-ensemble de X qui soit indépendant et maximal (au sens de l'inclusion). Le « rang de $\mathcal{M}$ », noté $r_{\mathcal{M}}(\mathcal{M})$, est $r_{\mathcal{M}}(E(\mathcal{M}))$.

La fonction de rang d'un matroïde possède les propriétés suivantes.

Lemme 14. *Soit $\mathcal{M}$ un matroïde sur un ensemble fini E . Soit $r := r_{\mathcal{M}}$ la fonction de rang de $\mathcal{M}$.*

- (R1) $\forall X \subseteq E, \quad 0 \leq r(X) \leq |X|$;
- (R2) *si Y est un sous-ensemble de E , alors $X \subseteq Y \Rightarrow r(X) \leq r(Y)$;*
- (R3) *si X et Y sont deux sous-ensembles de E , alors $r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y)$.*

Démonstration. Les propriétés (R1) et (R2) découlent directement de la définition de la fonction de rang. Prouvons à présent (R3). Soit $I_{\cap}$ un plus grand sous-ensemble de $X \cap Y$ qui soit indépendant. Soit $I_{\cup}$ un plus grand sous-ensemble de $X \cup Y$ qui contienne $I_{\cap}$ et soit indépendant. En particulier, notons que $I_{\cup} \cap X \in \mathcal{I}(\mathcal{M})$ et $I_{\cup} \cap Y \in \mathcal{I}(\mathcal{M})$. Par définition, $r(X) \geq |I_{\cup} \cap X|$ et $r(Y) \geq |I_{\cup} \cap Y|$. Ainsi,

$$\begin{aligned}
 r(X) + r(Y) &\geq |I_{\cup} \cap X| + |I_{\cup} \cap Y| \\
 &= |(I_{\cup} \cap X) \cup (I_{\cup} \cap Y)| + |(I_{\cup} \cap X) \cap (I_{\cup} \cap Y)| \\
 &= |I_{\cup} \cap (X \cup Y)| + |I_{\cup} \cap (X \cap Y)| \\
 &= |I_{\cup}| + |I_{\cap}| \\
 &= r(X \cup Y) + r(X \cap Y).
 \end{aligned}$$

□

La propriété (R3) est appelée « sous-modularité » de la fonction de rang.

Comme pour les circuits et les bases, les propriétés (R1)–(R3) caractérisent les fonctions qui peuvent être vues comme la fonction de rang d'un matroïde. Pour prouver cette assertion, le lemme suivant sera utile.

Lemme 15. *Soient E un ensemble fini et r une fonction de l'ensemble des parties de E vers $\mathbf{N}$ qui satisfait les propriétés (R1)–(R3). Si X et Y sont deux sous-ensembles de E tels que $r(X + y) = r(X)$ pour tout $y \in Y$, alors $r(X \cup Y) = r(X)$.*

Démonstration. Nous procédons par récurrence sur la taille de $Y \setminus X$, le résultat étant trivialement vrai si $|Y \setminus X| \leq 1$. Supposons à présent que $|Y \setminus X| \geq 2$. Soient $y_1, \dots, y_k$ les éléments de $Y \setminus X$. Par hypothèse, nous savons que $r(X) = r(X + y_k)$. De plus, l'hypothèse de récurrence appliquée à X et $Y - y_k$ assure que

$$r(X \cup (Y - y_k)) = r(X \cup \{y_1, \dots, y_{k-1}\}) = r(X).$$

Ainsi, l'on obtient

$$\begin{aligned} r(X) + r(X) &= r(X \cup \{y_1, \dots, y_{k-1}\}) + r(X + y_k) \\ &\geq r(X \cup \{y_1, \dots, y_k\}) + r(X) \\ &\geq r(X) + r(X), \end{aligned}$$

où les deux dernières lignes découlent de la propriété (R2). En conséquence, $2r(X) = r(X \cup Y) + r(X)$, c'est-à-dire $r(X \cup Y) = r(X)$. $\square$

Théorème 16. *Soient E un ensemble fini et r une fonction de l'ensemble des parties de E vers $\mathbf{N}$ satisfaisant les propriétés (R1)–(R3). Soit $\mathcal{I}$ la collection de tous les sous-ensembles X de E tels que $r(X) = |X|$. Alors $\mathcal{M} := (E, \mathcal{I})$ est un matroïde et $r_{\mathcal{M}} = r$.*

Démonstration. Montrons que $\mathcal{I}$ satisfait les propriétés (I1)–(I3). D'après (R1), $r(\emptyset) = 0 = |\emptyset|$, donc $\emptyset \in \mathcal{I}$. Prouvons à présent que $\mathcal{I}$ est héréditaire, c'est-à-dire satisfait (I2). Soit $I \in \mathcal{I}$, i.e. $r(I) = |I|$. Soit $I' \subset I$. Nous devons prouver que $r(I') = |I'|$. Posons $I'' := I \setminus I'$. Alors $I' \cup I'' = I$ et $I' \cap I'' = \emptyset$, donc la propriété (R3) implique que

$$r(I') + r(I'') \geq r(I) + r(\emptyset)$$

donc, en utilisant (R1) et le fait que $r(I) = |I|$,

$$|I| = |I'| + |I''| \geq r(I') + r(I'') \geq |I'|.$$

Comme le premier terme et le dernier terme sont égaux, (R1) entraîne que $r(I') = |I'|$ (et $r(I'') = |I''|$).

Il reste à prouver que $\mathcal{I}$ satisfait (I3). Nous procédons par l'absurde et utilisons le lemme 15 pour obtenir une contradiction. Soient I_0 et I_1 deux éléments de $\mathcal{I}$ tels que $|I_0| < |I_1|$ et $I_0 + e \notin \mathcal{I}$ pour tout élément $e \in I_1 \setminus I_0$.

Pour tout $e \in I_1 \setminus I_0$, nous avons $|I_0 + e| > r(I_0 + e) \geq r(I_0) = |I_0|$, la première inégalité découlant du fait que $I_0 + e \notin \mathcal{I}$. Donc $r(I_0 + e) = r(I_0)$ pour tout $e \in I_1$. Ainsi, $r(I_0 \cup I_1) = r(I_0)$ par le lemme 15. Par conséquent, en utilisant la propriété (R2), il vient

$$r(I_1) \leq r(I_0 \cup I_1) = r(I_0) = |I_0| < |I_1|,$$

ce qui contredit le fait que $I_1 \in \mathcal{I}$. Nous avons bien prouvé que $\mathcal{M}$ est un matroïde.

Enfin, nous prouvons que $r_{\mathcal{M}} = r$. Soit X un sous-ensemble de E . Si $X \in \mathcal{I}$, alors $r(X) = |X| = r_{\mathcal{M}}(X)$. Donc $r_{\mathcal{M}}$ et r coïncident sur les éléments de $\mathcal{I}$.

Supposons à présent que $X \notin \mathcal{I}$. Soit I un sous-ensemble de X qui soit indépendant et de taille maximale (en particulier, $|I| < |X|$). Il suit que $r_{\mathcal{M}}(X) = r_{\mathcal{M}}(I) = r(I)$ (la dernière égalité venant du paragraphe précédent, puisque $I \in \mathcal{I}$). Nous devons donc prouver que $r(X) = r(I)$, ce que nous déduisons du lemme 15. Par définition, $I + e \notin \mathcal{I}$ pour tout $e \in X \setminus I$. Ainsi, le lemme 15 assure que $r(I \cup X) = r(I)$, ce qui conclut la démonstration. $\square$

Le lemme 14 et le théorème 16 impliquent directement le résultat suivant.

Corollaire 17. *Soit E un ensemble fini. Soit r une fonction de la collection des parties de E vers $\mathbf{N}$. Il existe un matroïde dont r est la fonction de rang si, et seulement si, la fonction r satisfait les propriétés (R1)–(R3).*

Enfin, nous terminons cette section sur le rang d'un matroïde en donnant une caractérisation des ensembles indépendants, des bases et des circuits d'un matroïdes via la fonction de rang.

Proposition 18. Soient $\mathcal{M}$ un matroïde et r sa fonction de rang. Soit $X \subseteq E(\mathcal{M})$.

- (i) $X \in \mathcal{I}(\mathcal{M})$ si, et seulement si, $r(X) = |X|$;
- (ii) $X \in \mathcal{B}(\mathcal{M})$ si, et seulement si, $|X| = r(X) = r(\mathcal{M})$; et
- (iii) $X \in \mathcal{C}(\mathcal{M})$ si, et seulement si, $X \neq \emptyset$ et $r(X - x) = |X| - 1 = r(X)$ pour tout élément $x \in X$.

1.6. Exemples. Nous avons déjà vu le matroïde vectoriel, basé sur la relation d'indépendance linéaire de vecteurs dans un espace vectoriel de dimension finie sur un corps fixé. Il est possible de définir, de manière analogue, le matroïde affine. Soient $v_1, \dots, v_k$ sont des vecteurs de dimension d à coefficients dans un corps $\mathbf{F}$. Ces vecteurs sont dits « affinement dépendants » si, et seulement si, $k \geq 1$ et il existe un k -uplet $(a_1, \dots, a_k)$ d'éléments de $\mathbf{F}$ non tous nuls et tels que

$$\sum_{i=1}^k a_i = 0 \quad \text{et} \quad \sum_{i=1}^k a_i v_i = 0.$$

Les vecteurs $v_1, \dots, v_k$ sont « affinement indépendants » si, et seulement si, ils ne sont pas affinement dépendants.

Exemple 19. Soit E l'ensemble de colonnes d'une matrice A de taille $m \times n$ à coefficients dans un corps $\mathbf{F}$. Soit $\mathcal{I}$ la collection de tous les sous-ensembles de E qui sont affinement indépendants dans l'espace vectoriel de dimension m sur $\mathbf{F}$. Alors $\mathcal{M} := (E, \mathcal{I})$ est un matroïde, appelé « matroïde affine ».

Exemple 20. Soient E un ensemble fini et $(A_1, \dots, A_n)$ une partition de E . Soit $\mathcal{I}$ la collection de tous les sous-ensembles X de E tels que

$$\forall i \in \{1, \dots, n\}, \quad |X \cap A_i| \leq 1.$$

Alors $\mathcal{M} := (E, \mathcal{I})$ est un matroïde, appelé « matroïde transversal ».

Exemple 21. Soit E un ensemble de taille n et soit $m \in \{1, \dots, n\}$. Si $\mathcal{I}$ est la collection de tous les sous-ensembles de E de taille au plus m , alors $(E, \mathcal{I})$ est un matroïde, appelé « matroïde uniforme ».

Définition 22. Soit $F_1, \dots, F_k$ des ensembles et $\mathcal{F}$ la famille $(F_1, \dots, F_k)$. Un « transversal » de la famille $\mathcal{F}$ est un ensemble $\{x_1, \dots, x_k\}$ tel que $x_i \in F_i$ pour tout $i \in \{1, \dots, k\}$. Un « transversal partiel » de $\mathcal{F}$ est un transversal d'une sous-famille de $\mathcal{F}$, c'est-à-dire un ensemble $\{x_1, \dots, x_s\}$ tel que $x_i \in F_{j_i}$ pour tout $i \in \{1, \dots, s\}$ et $1 \leq j_1 < \dots < j_s \leq k$.

Exercice 23. Soit $\mathcal{F} := (F_i)_{i=1}^m$ une famille de sous-ensembles d'un ensemble fini E . Soit $\mathcal{I}$ la collection de tous les transversaux partiels de $\mathcal{F}$. Le couple $\mathcal{M} := (E, \mathcal{I})$ est-il un matroïde ?

2. UNION DE MATROÏDES

Il est possible d'obtenir un matroïde en faisant la réunion de deux matroïdes sur des ensembles *disjoints*.

Proposition 24. Pour $i \in \{1, 2\}$, soit $\mathcal{M}_i = (E_i, \mathcal{I}_i)$ un matroïde. Supposons que $E_1 \cap E_2 = \emptyset$. Soit $\mathcal{I}$ la collection de sous-ensembles X de $E_1 \cup E_2$ tels que $X \cap E_i \in \mathcal{I}_i$ pour $i \in \{1, 2\}$. Alors $(E_1 \cup E_2, \mathcal{I})$ est un matroïde, appelé « réunion » ou « somme directe » des matroïdes $\mathcal{M}_1$ et $\mathcal{M}_2$, et noté $\mathcal{M}_1 \oplus \mathcal{M}_2$.

Démonstration. Exercice. □

Les circuits, les bases et la fonction de rang de la somme directe de deux matroïdes sont caractérisés comme suit.

Proposition 25. Soient $\mathcal{M}_1$ et $\mathcal{M}_2$ deux matroïdes sur des ensembles disjoints.

- (i) $\mathcal{C}(\mathcal{M}_1 \oplus \mathcal{M}_2) = \mathcal{C}(\mathcal{M}_1) \cup \mathcal{C}(\mathcal{M}_2)$;
- (ii) $\mathcal{B}(\mathcal{M}_1 \oplus \mathcal{M}_2) = \{B_1 \cup B_2 : \forall i \in \{1, 2\}, B_i \in \mathcal{B}(\mathcal{M}_i)\}$; et
- (iii) $\forall X \subseteq E(\mathcal{M}_1) \cup E(\mathcal{M}_2), \quad r_{\mathcal{M}_1 \oplus \mathcal{M}_2}(X) = r_{\mathcal{M}_1}(X \cap E(\mathcal{M}_1)) + r_{\mathcal{M}_2}(X \cap E(\mathcal{M}_2))$.

Démonstration. Exercice. □

3. ALGORITHMES DANS LES MATROÏDES

Les matroïdes unifient plusieurs concepts au sein d'une même axiomatique et il est naturel de se demander quels algorithmes restent fonctionnels dans ce cadre général. La première chose à clarifier est la manière dont un matroïde est donné en entrée.

Nous supposons que le matroïde est donné par un oracle et que l'oracle répond à chaque question en temps τ . Les temps d'exécution des algorithmes que nous verrons seront donc fonction de τ , qu'il suffira ainsi de remplacer par sa valeur réelle pour le cas considéré. Par exemple, dans le cas d'un matroïde graphique, tester si un ensemble est indépendant nécessite un temps linéaire dans la taille du graphe correspondant. Le temps de réponse τ de l'oracle sera donc linéaire en la taille du graphe dans ce cas.

3.1. Bases de poids maximum et minimum. Le problème suivant est fondamental dans la théorie des matroïdes. Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde et soit $w : E \rightarrow \mathbf{R}$ une pondération des éléments de $\mathcal{M}$. (Nous éluderons la question de la représentation des nombres réels. Au besoin, l'on peut se restreindre aux pondérations à valeurs dans $\mathbf{Z}$ ou $\mathbf{Q}$.) Le but est de trouver une base B de $\mathcal{M}$ telle que

$$\forall B' \in \mathcal{B}(\mathcal{M}), \quad \sum_{e \in B'} w(e) \leq \sum_{e \in B} w(e).$$

Une telle base B est appelée « base de poids maximum » du « matroïde pondéré $(\mathcal{M}, w)$ ». Pour tout sous-ensemble X de E , nous posons $w(X) := \sum_{e \in X} w(e)$.

Nous allons voir que l'algorithme glouton permet de résoudre ce problème. Pour cela, commençons par définir précisément ce que nous entendons par « algorithme glouton ».

Entrées : Un matroïde pondéré $(\mathcal{M}, w)$

début

Trier les éléments de $\mathcal{M}$ de façon décroissante suivant leur poids : $e_1, \dots, e_n$ avec $w(e_i) \geq w(e_j)$ si $i < j$

$A_0 \leftarrow \emptyset$

pour i de 1 à n **faire**

si $A_{i-1} + e_i \in \mathcal{I}(\mathcal{M})$ **alors**

$A_i \leftarrow A_{i-1} + e_i$

sinon

$A_i \leftarrow A_{i-1}$

fin

fin

retourner A_n

fin

Algorithme 1: L'algorithme glouton.

Théorème 26. Soit $(\mathcal{M}, w)$ un matroïde pondéré. L'algorithme glouton (algorithme 1) renvoie une base de poids maximum de $(\mathcal{M}, w)$ en temps $O(|E(\mathcal{M})| \log |E(\mathcal{M})| + |E(\mathcal{M})| \tau)$, où τ est le temps de réponse de l'oracle donnant le matroïde.

Démonstration. Soit n le nombre d'éléments de $\mathcal{M}$. Commençons par prouver que le temps d'exécution de l'algorithme glouton est $O(n \log n + n\tau)$. Le tri des n éléments de $\mathcal{M}$ se fait en $O(n \log n)$. Ensuite, la construction de la suite $(A_i)_{0 \leq i \leq n}$ nécessite n réponses de l'oracle et se fait ainsi en temps $O(n\tau)$.

Pour conclure la démonstration, il nous suffit désormais de prouver que A_n est une base de poids maximum de $(\mathcal{M}, w)$.

Tout d'abord, par construction et comme $\mathcal{I}(\mathcal{M})$ est héréditaire, A_n est un ensemble indépendant maximal (au sens de l'inclusion) de $\mathcal{M}$, i.e. $A_n \in \mathcal{B}(\mathcal{M})$.

À présent, supposons par l'absurde qu'il existe une base $B' \in \mathcal{B}(\mathcal{M})$ de poids strictement supérieur à celui de A_n . Nous allons obtenir une contradiction sur le fonctionnement de l'algorithme en utilisant l'axiome d'augmentation.

Soient $e_1, \dots, e_n$ les éléments de $\mathcal{M}$ triés de sorte que $w(e_i) \geq w(e_j)$ dès que $i < j$. En notant r le rang de $\mathcal{M}$, l'on peut écrire $A_n = \{e_{i_1}, \dots, e_{i_r}\}$ et $B' = \{e_{j_1}, \dots, e_{j_r}\}$ avec $i_k < i_\ell$ et $j_k < j_\ell$ dès que $k < \ell$.

Soit ℓ le plus petit entier positif k tel que $i_k > j_k$. En particulier, ℓ existe et est au plus r par hypothèse.

Considérons l'ensemble indépendant $A_{i_{\ell-1}}$, c'est-à-dire $\{e_{i_1}, \dots, e_{i_{\ell-1}}\}$ (en particulier, il s'agit de l'ensemble vide si $\ell = 1$). Soit I_1 l'ensemble indépendant $\{e_{j_1}, \dots, e_{j_\ell}\}$. D'après l'axiome d'augmentation (I3), il existe $k \in \{1, \dots, \ell\}$ tel que $A_{i_{\ell-1}} + e_{j_k} \in \mathcal{I}(\mathcal{M})$ et $e_{j_k} \notin A_{i_{\ell-1}}$. Or $j_k \leq j_\ell < i_\ell$, donc $w(e_{j_k}) \geq w(e_{j_\ell}) > w(e_{i_\ell})$. Ceci contredit la définition de l'algorithme glouton. $\square$

Un corollaire direct de ce résultat est qu'il est possible de trouver une base de poids minimum d'un matroïde.

Corollaire 27. *Soit $(\mathcal{M}, w)$ un matroïde pondéré. Il est possible de trouver une base de poids minimum de $(\mathcal{M}, w)$ en temps $O(|E(\mathcal{M})| \log |E(\mathcal{M})| + |E(\mathcal{M})| \tau)$.*

Démonstration. Il suffit d'appliquer le théorème 26 au matroïde pondéré $(\mathcal{M}, -w)$. $\square$

Exercice 28. Soit $(\mathcal{M}, w)$ un matroïde pondéré. Si $\mathcal{M}$ est en outre un matroïde graphique, à quoi correspond (en termes de graphes) le problème de trouver une base de poids minimum ?

Edmonds a prouvé que les matroïdes correspondent précisément aux structures pour lesquelles l'algorithme glouton renvoie un ensemble de poids maximum.

Théorème 29. *Soit $\mathcal{I}$ une collection de sous-ensembles d'un ensemble fini E , telle que $\emptyset \in \mathcal{I}$. Si, pour toute pondération positive w des éléments de E (i.e. $w : E \rightarrow \mathbf{R}^+$), l'algorithme 1 renvoie un ensemble appartenant à $\mathcal{I}$ de poids maximum (relativement à w), alors $(E, \mathcal{I})$ est un matroïde.*

Démonstration. Nous allons montrer que $\mathcal{I}$ satisfait les propriétés (I1)–(I3). L'ensemble vide appartient à $\mathcal{I}$ par hypothèse, donc (I1) est vérifiée.

À présent, nous prouvons par l'absurde que $\mathcal{I}$ est héréditaire : supposons qu'il existe un élément de $\mathcal{I}$ contenant un sous-ensemble qui n'appartient pas à $\mathcal{I}$. Parmi tous ces éléments de $\mathcal{I}$, on en choisit un, noté I , de taille minimum (notons que $|I| > 1$). Ainsi, il existe $f \in I$ tel que $I - f \notin \mathcal{I}$. Posons $I' := I - f$. Nous allons obtenir une contradiction en définissant une pondération bien choisie de E .

Soit

$$w: E \longrightarrow \mathbf{N}$$

$$e \longmapsto \begin{cases} 2 & \text{si } e \in I' \\ 1 & \text{si } e = f \\ 0 & \text{sinon.} \end{cases}$$

On observe que $w(J) \leq 2|I| - 1$ pour tout ensemble $J \subseteq E$. De plus, l'ensemble I est indépendant et atteint précisément ce poids. Ainsi, par hypothèse, l'algorithme glouton renvoie un ensemble de poids $2|I| - 1$, car la pondération w est positive. Cet algorithme commence par trier les éléments de E de façon décroissante suivant leur poids. Par conséquent, il place d'abord tous les éléments de I' , puis f et enfin les éléments de $E \setminus I$. Pour parvenir à créer un ensemble de poids $2|I| - 1$, les $|I'|$ premiers éléments ajoutés par l'algorithme doivent être précisément ceux de I' . Ainsi, $A_{|I'|} = I'$, mais $I' \notin \mathcal{I}$ ce qui est une contradiction.

Il reste à prouver que (I3) est vraie, ce que nous faisons également par l'absurde. Soient I_0 et I_1 deux éléments de $\mathcal{I}$ tels que $|I_0| < |I_1|$ et $I_0 + e \notin \mathcal{I}$ pour tout $e \in I_1 \setminus I_0$. Comme nous avons prouvé que $\mathcal{I}$ est héréditaire, nous pouvons supposer que $|I_1| = |I_0| + 1$. Posons

$$w: E \longrightarrow \mathbf{N}$$

$$e \longmapsto \begin{cases} |I_0| + 2 & \text{si } e \in I_0 \\ |I_0| + 1 & \text{si } e \in I_1 \setminus I_0 \\ 0 & \text{sinon.} \end{cases}$$

L'algorithme glouton renvoie un ensemble de $\mathcal{I}$ de poids au moins égal à celui de I_1 (puisque $I_1 \in \mathcal{I}$ et w est positive). Par définition, le poids de I_1 est au moins $|I_1|(|I_0| + 1) = |I_0|^2 + 2|I_0| + 1$. Analysons ce que fait l'algorithme : par définition de l'algorithme glouton et de w , il vient que $A_{|I_0|} = I_0$, car $\mathcal{I}$ est héréditaire. Ensuite, aucun élément de $I_1 \setminus I_0$ ne peut être ajouté à A_i , pour tout $i \geq |I_0|$ car $I_0 + e \notin \mathcal{I}$ pour tout $e \in I_1 \setminus I_0$ et car nous avons prouvé que $\mathcal{I}$ est héréditaire⁴. Ainsi, le poids de l'ensemble renvoyé par l'algorithme glouton est au plus

$$|I_0|(|I_0| + 2) = |I_0|^2 + 2|I_0| < |I_0|^2 + 2|I_0| + 1 = w(I_1).$$

Cette contradiction conclut la démonstration. $\square$

3.2. Intersection de matroïdes. Comme nous venons de le voir, tout problème qui peut se formuler comme une question d'optimisation sur les ensembles indépendants d'un matroïde se résout efficacement à l'aide de l'algorithme glouton. Néanmoins, cette classe de problèmes n'est pas très générale. En revanche, il existe un nombre important de questions qui peuvent se réduire à optimiser sur des ensembles qui sont indépendants dans deux matroïdes à la fois. Il existe des algorithmes permettant d'effectuer cette optimisation efficacement. Nous allons préciser un peu cette question à l'aide d'un exemple, puis nous verrons le théorème général sur l'intersection de deux matroïdes. Nous donnerons ensuite différentes applications. Avant d'aller plus loin, assurons-nous que nous ne possédons pas déjà la solution au problème.

Exercice 30. Soient $\mathcal{M}_1$ et $\mathcal{M}_2$ deux matroïdes sur le même ensemble E . Le couple $(E, \mathcal{I}(M_1) \cap \mathcal{I}(M_2))$ est-il nécessairement un matroïde ? Concluez.

Dans un graphe, un *couplage* est un ensemble d'arêtes deux-à-deux disjointes. Il est possible d'obtenir en temps polynomial un couplage maximum d'un graphe arbitraire. La restriction de cette question aux graphes bipartis possède un analogue dans le monde des matroïdes, dont la solution donne lieu à l'un des théorèmes fondamentaux de la théorie des matroïdes. Commençons par formuler précisément le problème.

Nous voulons construire, étant donné un graphe biparti arbitraire $G = (V, E)$ avec bipartition (V_1, V_2) , un couplage maximum de G en temps polynomial (en la taille de G). Ce problème peut se formuler à l'aide de matroïdes comme suit.

4. Bien comprendre pourquoi c'est important ici.

Pour $i \in \{1, 2\}$, soit $\mathcal{M}_i$ le matroïde sur E tel qu'un sous-ensemble E' de E est indépendant (dans $\mathcal{M}_i$) si, et seulement si, les sommets extrémaux des arêtes de E' dans V_i sont deux-à-deux distincts (i.e. $\forall e, e' \in E', e \neq e' \Rightarrow (e \cap V_i) \neq (e' \cap V_i)$).

Notons $E(v)$ l'ensemble des arêtes incidentes au sommet v . En voyant E comme l'union disjointe des ensembles $E(v)$ pour $v \in V_i$, le matroïde $\mathcal{M}_i$ est un matroïde transversal. Notons également que le rang de E est le nombre de sommets de V_i de degré non nul.

Remarquons à présent qu'un sous-ensemble E' de E est un couplage si, et seulement si, E' est indépendant à la fois dans $\mathcal{M}_1$ et dans $\mathcal{M}_2$, i.e. $E' \in \mathcal{I}(\mathcal{M}_1) \cap \mathcal{I}(\mathcal{M}_2)$. Le problème de trouver un couplage de taille maximum dans G se ramène donc à trouver un ensemble indépendant de taille maximum commun aux deux matroïdes $\mathcal{M}_1$ et $\mathcal{M}_2$ (tous deux matroïdes sur le même ensemble E).

Il se trouve que ce problème se résout en temps polynomial pour toute paire de matroïdes sur le même ensemble. Nous allons voir un algorithme résolvant ce problème, qui sera obtenu comme corollaire de la caractérisation suivante des ensembles maximaux communs. Nous donnerons ensuite plusieurs applications de ces deux résultats fondamentaux.

Théorème 31 (Théorème d'intersection de matroïdes). *Soit E un ensemble fini. Pour $i \in \{1, 2\}$, soit $\mathcal{M}_i(E, \mathcal{I}_i)$ un matroïde. Alors*

$$(3.1) \quad \max_{E' \in \mathcal{I}_1 \cap \mathcal{I}_2} |E'| = \min_{E_1 \cup E_2 = E} r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2).$$

Remarque 2. L'énoncé du théorème 31 reste vrai en se restreignant aux *partitions* (E_1, E_2) de E dans le membre de droite de (3.1), c'est-à-dire en imposant $E_1 \cap E_2 = \emptyset$ (pourquoi?). Ceci est souvent pratique pour alléger les démonstrations.

Démonstration du théorème 31. Nous prouvons uniquement que le membre de gauche de (3.1) est au plus le membre de droite de (3.1). L'autre inégalité fait l'objet d'une note à part, contenant des exercices.

Soient E_1 et E_2 deux sous-ensembles de E dont l'union est égale à E et tels que $r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2)$ soit minimum pour cette propriété. Il nous suffit de prouver que $|E'| \leq r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2)$ pour tout sous-ensemble E' de E qui est indépendant à la fois dans $\mathcal{M}_1$ et dans $\mathcal{M}_2$.

Comme $E' \in \mathcal{I}(\mathcal{M}_i)$,

$$|E' \cap E_i| = r_{\mathcal{M}_i}(E' \cap E_i) \leq r_{\mathcal{M}_i}(E_i).$$

Ainsi,

$$|E'| \leq |E' \cap E_1| + |E' \cap E_2| \leq r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2).$$

□

Corollaire 32. *Le problème d'intersection de matroïdes se résout en temps $O(r^2 n \tau)$ pour toute paire de matroïdes de rang au plus r sur un même ensemble fini de taille n et donnés par un oracle avec temps de réponse τ .*

Est-il possible d'étendre le corollaire 32 à plus de deux matroïdes ? La réponse est non, si $P \neq NP$.

Théorème 33. *Soient $\mathcal{M}_1, \mathcal{M}_2$ et $\mathcal{M}_3$ trois matroïdes. Il est NP-difficile de trouver un ensemble de taille maximum dans $\mathcal{I}_1 \cap \mathcal{I}_2 \cap \mathcal{I}_3$.*

La preuve consiste à réduire la question au problème Π du chemin hamiltonien dans les graphes orientés, qui est NP-difficile. Une instance de ce problème est un graphe orienté D et deux sommets s et t de D . La question est : *Existe-t-il dans D un chemin orienté de s à t qui passe une et une seule fois par chaque sommet de D ?*

Démonstration. Soit (D, s, t) une instance de Π .⁵ Nous allons construire trois matroïdes $\mathcal{M}_1, \mathcal{M}_2$ et $\mathcal{M}_3$ tels que la réponse à $\Pi(D, s, t)$ est oui si, et seulement si, il existe un ensemble X dans $\mathcal{I}(\mathcal{M}_1) \cap \mathcal{I}(\mathcal{M}_2) \cap \mathcal{I}(\mathcal{M}_3)$ de taille $|V(D)| - 1$. Ceci fournira la conclusion souhaitée.

Prenons pour $\mathcal{M}_1$ le matroïde graphique du graphe non orienté G sous-jacent à D . Si $X \subseteq E(G)$, notons $\vec{X}$ l'ensemble des arcs de D correspondant aux arêtes dans X . Pour $v \in V(D)$, soit $\bar{\chi}_v : V(D) \rightarrow \{0, 1\}$ donnée par $\bar{\chi}_v(u) = 1$ si $u \neq v$ et $\bar{\chi}_v(v) = 0$. Soient

$$\mathcal{I}_2 := \left\{ X \subseteq E(G) : \forall v \in V(D), \quad \left| \vec{X} \cap A^+(v) \right| \leq \bar{\chi}_t(v) \right\}$$

et

$$\mathcal{I}_3 := \left\{ X \subseteq E(G) : \forall v \in V(D), \quad \left| \vec{X} \cap A^-(v) \right| \leq \bar{\chi}_s(v) \right\}$$

Pour $i \in \{1, 2\}$, le couple $\mathcal{M}_i := (E(G), \mathcal{I}_i)$ est un matroïde (voir la feuille d'exercices).

Si P est un chemin hamiltonien dans D de s à t , l'ensemble des arêtes de G correspondantes a taille $|V(D)| - 1$ et est indépendant à la fois dans $\mathcal{M}_1, \mathcal{M}_2$ et $\mathcal{M}_3$. Réciproquement, soit X est un ensemble d'arêtes de G de taille $|V(D)| - 1$. Si $X \in \mathcal{I}(\mathcal{M}_1)$, alors $(V(G), X)$ est un arbre couvrant de G . Si de plus $X \in \mathcal{I}_2 \cap \mathcal{I}_3$, alors tout sommet de D a degré entrant et degré sortant au plus un dans $(V(D), \vec{X})$. De plus, s a degré entrant nul (donc nécessairement degré sortant un) et t a degré sortant nul (donc degré entrant nécessairement un). Ainsi, $(V(D), \vec{X})$ est un chemin hamiltonien dans D de s à t . $\square$

4. APPLICATIONS DU THÉORÈME D'INTERSECTION

Nous allons considérer plusieurs résultats classiques sur les graphes et les démontrer à l'aide du théorème d'intersection de matroïdes.

4.1. Couplages maximums dans les graphes bipartis. Soit $G = (V, E)$ un graphe. Un *couplage* de G est un ensemble M d'arêtes de G tel que chaque sommet de G soit incident à au plus une arête dans M . Un couplage M est *maximum* si $|M| \geq |M'|$ pour tout couplage M' de G .

Le graphe G est *biparti* si, et seulement si, il est possible de partitionner V en deux sous-ensembles A et B tels que $E \subseteq A \times B$. De manière équivalente, G est biparti si, et seulement si, G ne contient pas de cycle impair.

Une *sommet-couverture* de G est un ensemble X de sommets de G tel que toute arête de G soit incidente à un sommet appartenant à X . Une sommet-couverture X est *minimum* si $|X| \leq |X'|$ pour toute sommet-couverture X' de G .

Théorème 34. *Soit $G = (V, E)$ un graphe biparti connexe. La taille d'un couplage maximum de G est égal à la taille d'une sommet-couverture minimum de G .*

Démonstration. Tout d'abord, comme il est coutumier dans les théorèmes min-max, il n'est pas difficile de prouver que la quantité que l'on minimise est au moins égale à la quantité que l'on maximise. En effet, si X est une sommet-couverture (quelconque) de G et M un couplage (quelconque) de G , alors chaque arête de M est incidente à un sommet dans X . De plus, les arêtes dans M sont disjointes. Ainsi, il vient $|X| \geq |M|$.

⁵. s et t sont donc deux sommets fixés de D .

Il reste à prouver l'inégalité réciproque. Nous avons vu que la notion de couplage dans un graphe biparti peut s'exprimer à l'aide de deux matroïdes transversaux : pour chacune des deux parts de la bipartition, l'ensemble des arêtes du graphe est partitionné en fonction du sommet auquel l'arête est incidente. Ceci va nous permettre d'utiliser le théorème d'intersection, puisqu'un couplage est alors un ensemble indépendant dans chacun des deux matroïdes transversaux.

Plus précisément, soit (V_1, V_2) une partition de V telle que $E \subseteq V_1 \times V_2$. Pour $i \in \{1, 2\}$, soit $\mathcal{M}_i$ le matroïde sur E dont les ensembles indépendants sont les sous-ensembles X de E tels que tout sommet de V_i soit incident dans G à au plus une arête appartenant à X . En d'autres termes, $\mathcal{M}_i$ est le matroïde transversal sur E respectivement à la partition de E donnée par :

deux arêtes e et e' de G sont dans la même part de V_i si, et seulement si, elles sont incidentes au même sommet de V_i .

Notons que, pour $i \in \{1, 2\}$, le rang d'un sous-ensemble X d'arêtes est précisément le nombre de sommets de V_i incidents à une arête de X .

Un ensemble M d'arêtes de G est un couplage de G si, et seulement si, l'ensemble M est indépendant à la fois dans $\mathcal{M}_1$ et dans $\mathcal{M}_2$, i.e. $M \in \mathcal{I}(\mathcal{M}_1) \cap \mathcal{I}(\mathcal{M}_2)$. Soit M un couplage maximum de G . D'après le théorème 31, il existe une partition (E_1, E_2) de E telle que

$$|M| = r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2).$$

Pour $i \in \{1, 2\}$, soit S_i l'ensemble des sommets de V_i incidents à une arête dans E_i . Alors $|S_i| = r_{\mathcal{M}_i}(E_i)$ et $S_1 \cup S_2$ est une sommet-couverture de G . Ceci conclut la preuve. $\square$

4.2. Bases disjointes. Une autre question conséquence intéressante du théorème d'intersection concerne l'existence de bases disjointes dans un matroïde.

Théorème 35. *Soient k un entier et E un ensemble fini. Un matroïde $\mathcal{M} = (E, \mathcal{I})$ possède k bases disjointes si, et seulement si, pour tout sous-ensemble X de E ,*

$$(4.1) \quad |E \setminus X| \geq k(r_{\mathcal{M}}(E) - r_{\mathcal{M}}(X)).$$

Démonstration. Supposons que $\mathcal{M}$ contienne k bases $B_1, \dots, B_k$ deux-à-deux disjointes. Soit $X \subseteq E$. Alors

$$\begin{aligned} |E \setminus X| &\geq \sum_{i=1}^k |B_i \cap (E \setminus X)| = \sum_{i=1}^k (r_{\mathcal{M}}(E) - |B_i \cap X|) \\ &\geq \sum_{i=1}^k (r_{\mathcal{M}}(E) - r_{\mathcal{M}}(X)) = k \cdot (r_{\mathcal{M}}(E) - r_{\mathcal{M}}(X)). \end{aligned}$$

Prouvons à présent l'inégalité réciproque. Pour cela, nous allons appliquer le théorème d'intersection aux deux matroïdes $\mathcal{M}_1$ et $\mathcal{M}_2$ suivants.

Le matroïde $\mathcal{M}_1$ peut être vu comme la somme directe de k copies disjointes de $\mathcal{M}$. En d'autres termes, $\mathcal{M}_1 = (E_0, \mathcal{I}_1)$ avec $E_0 := E \times \{1, \dots, k\}$ et un sous-ensemble X de E_0 appartient à $\mathcal{I}_1$ si, et seulement si, pour tout $i \in \{1, \dots, k\}$, l'ensemble $\{e \in E : (e, i) \in X\}$ appartient à $\mathcal{I}$.

Le matroïde $\mathcal{M}_2$ est le matroïde transversal associé à la partition de E_0 suivant la première coordonnée. En d'autres termes, $\mathcal{M}_2 = (E_0, \mathcal{I}_2)$ où un sous-ensemble X de E_0 appartient à $\mathcal{I}_2$ si, et seulement si, pour tout $e \in E$, il existe au plus un indice $i \in \{1, \dots, k\}$ tel que $(e, i) \in X$.

Observons que $\mathcal{M}$ possède k bases disjointes si, et seulement si, il existe un ensemble X de taille $k \cdot r_{\mathcal{M}}(E)$ qui soit indépendant à la fois dans $\mathcal{M}_1$ et dans $\mathcal{M}_2$. En effet, si $B_1, \dots, B_k$ sont k bases disjointes de $\mathcal{M}$, alors $\{B_i \times \{i\} : i \in \{1, \dots, k\}\} \in \mathcal{I}_1 \times \mathcal{I}_2$.⁶ Réciproquement, s'il existe un ensemble $X \in \mathcal{I}_1 \times \mathcal{I}_2$ de taille $k \cdot r_{\mathcal{M}}(E)$, alors pour tout $i \in \{1, \dots, k\}$, l'ensemble $B_i := \{e \in E : (e, i) \in X\} \in \mathcal{I}$. En particulier, $|B_i| \leq r_{\mathcal{M}}(E)$ pour tout $i \in \{1, \dots, k\}$ et donc $|B_i| = r_{\mathcal{M}}(E)$ pour tout $i \in \{1, \dots, k\}$ en raison de la taille de X . Ainsi $B_1, \dots, B_k$ sont des bases de $\mathcal{M}$. Par ailleurs, $X \in \mathcal{I}_2$ entraîne que $B_i \cap B_j = \emptyset$ si $i \neq j$.

Supposons que (4.1) soit vérifiée pour tout $X \subseteq E$ et montrons que $\mathcal{M}$ contient k bases disjointes. D'après ce qui précède, il suffit de prouver que $\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| \geq k \cdot r_{\mathcal{M}}(E)$. Par le théorème d'intersection, il suffit donc de prouver que pour toute partition (E_1, E_2) de E_0 ,

$$(4.2) \quad r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2) \geq k \cdot r_{\mathcal{M}}(E).$$

Soit (E_1, E_2) une partition de E_0 . Remarquons que si $(e, i) \in E_2$, alors $r_{\mathcal{M}_2}(E_2 + (e, i')) = r_{\mathcal{M}_2}(E_2)$ pour tout $i' \in \{1, \dots, k\}$. Ainsi, nous pouvons supposer qu'il existe $E' \subseteq E$ tel que $E_2 = E' \times \{1, \dots, k\}$. En conséquence, $r_{\mathcal{M}_2}(E_2) = |E'|$. De plus, $E_1 = E_0 \setminus E_2 = (E \setminus E') \times \{1, \dots, k\}$. Par suite, $r_{\mathcal{M}_1}(E_1) = k \cdot r_{\mathcal{M}}(E \setminus E')$.

D'après la propriété (4.1) appliquée à $E \setminus E'$,

$$|E'| \geq k \cdot (r_{\mathcal{M}}(E) - r_{\mathcal{M}}(E \setminus E')),$$

c'est-à-dire

$$k \cdot r_{\mathcal{M}}(E \setminus E') + |E'| \geq k \cdot r_{\mathcal{M}}(E),$$

ce qui prouve (4.2) et conclut la démonstration. $\square$

Nous allons appliquer le théorème 35 aux matroïdes graphiques. Il est parfois désirable de savoir qu'un graphe possède des arbres couvrants disjoints.

Considérons un graphe G qui possède k arbres couvrants $T_1, \dots, T_k$ deux-à-deux arête-disjoints. Soit $(V_1, \dots, V_\ell)$ une partition de l'ensemble des sommets de G . Nécessairement, chaque arbre couvrant T_i possède au moins $\ell - 1$ arêtes dont les sommets extrémaux appartiennent à des parts différentes de la partition. Comme les arbres couvrants sont disjoints, il suit que G possède nécessairement au moins $k(\ell - 1)$ arêtes dont les sommets extrémaux appartiennent à des parts différentes de la partition $(V_1, \dots, V_\ell)$. Le théorème de Nash-Williams nous assure que cette condition nécessaire est également suffisante. Nous allons démontrer ceci à l'aide du théorème 35 : en effet, dans un graphe connexe G , les arbres couvrants correspondent aux bases du matroïde graphique associé à G . La condition « arête-disjoint » correspond précisément à la condition que les bases sont disjointes.

Théorème 36 (Nash-Williams). *Soit G un (multi)-graphe connexe. Le graphe G contient k arbres couvrants arête-disjoints si, et seulement si, pour toute partition $(V_1, \dots, V_\ell)$ de l'ensemble des sommets de G le nombre d'arêtes entre des sommets appartenant à des parts distinctes est au moins $k(\ell - 1)$.*

Démonstration. Nous avons déjà vu que la condition donnée dans l'énoncé du théorème est nécessaire, il nous reste à voir qu'elle est aussi suffisante.

Soit donc G un graphe tel que pour toute partition $(V_1, \dots, V_\ell)$ de l'ensemble des sommets, il existe au moins $k(\ell - 1)$ arêtes entre des parts distinctes. Soit $\mathcal{M}$ le matroïde graphique associé à G . Le graphe G possède k arbres couvrants arête-disjoints si, et seulement si, $\mathcal{M}$ possède k bases disjointes. Par le théorème 35, ceci équivaut au fait que pour tout ensemble X d'éléments de $\mathcal{M}$, on ait $|E(\mathcal{M}) \setminus X| \geq k(r_{\mathcal{M}}(\mathcal{M}) - r_{\mathcal{M}}(X))$.

6. Vérifiez-le.

Notons E l'ensemble d'arêtes de G (donc $E = E(\mathcal{M})$) et soit n le nombre de sommets de G . Fixons $X \subseteq E$. Notons $C_1, \dots, C_\ell$ les composantes du sous-graphe de G obtenu en ne gardant que les arêtes qui appartiennent à X . Soit V_i l'ensemble des sommets de C_i pour $i \in \{1, \dots, \ell\}$. Le rang de l'ensemble X dans le matroïde $\mathcal{M}$ est égal à $n - \ell$.⁷ En particulier, comme G est connexe, le rang de $\mathcal{M}$ est égal à $n - 1$. En conséquent, $r_{\mathcal{M}}(E) - r_{\mathcal{M}}(X) = (n - 1) - (n - \ell) = \ell - 1$.

Ainsi, nous devons démontrer que

$$(4.3) \quad |E \setminus X| \geq k \cdot (\ell - 1),$$

L'ensemble $E \setminus X$ contient toutes les arêtes entre les sommets dans V_i et les sommets dans V_j pour $i \neq j$ (et, potentiellement, $E \setminus X$ contient aussi d'autres arêtes à l'intérieur des ensembles V_i). Par suite, comme $(V_1, \dots, V_\ell)$ est une partition de l'ensemble des sommets de V , l'hypothèse sur G implique que $E \setminus X$ contient au moins $k(\ell - 1)$ arêtes. Ceci conclut la démonstration. $\square$

4.3. Couverture par des ensembles indépendants. Il existe un théorème dual au théorème 36, également démontré par Nash-Williams, qui concerne la couverture des arêtes d'un graphe par des sous-graphes acycliques.

Théorème 37. *Soit G un (multi)graphe. Il existe k sous-graphes acycliques de G tels que toute arête de G appartienne à au moins l'un de ces sous-graphes si, et seulement si, pour tout sous-ensemble non vide X de sommets de G , le sous-graphe de G induit par les sommets appartenant à X comporte au plus $k \cdot (|X| - 1)$ arêtes.*

Le théorème 37 se généralise aux matroïdes de la façon suivante ; les sous-graphes acycliques d'un graphe étant précisément les ensembles indépendants du matroïde graphique associé au graphe.

Théorème 38. *Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde. Il existe k ensembles indépendants $I_1, \dots, I_k$ de $\mathcal{M}$ dont la réunion est E si, et seulement si, pour tout $X \subseteq E$,*

$$(4.4) \quad |X| \leq k \cdot r_{\mathcal{M}}(X).$$

Démonstration. Une fois encore, il est rapide de prouver la nécessité de la condition donnée. Soient $I_1, \dots, I_k$ des ensembles indépendants de $\mathcal{M}$ dont la réunion est E . Pour tout $X \subseteq E$,

$$\begin{aligned} |X| &\leq \sum_{i=1}^k |X \cap I_i| \\ &\leq \sum_{i=1}^k r_{\mathcal{M}}(X) = k \cdot r_{\mathcal{M}}(X). \end{aligned}$$

Supposons à présent (4.4) vraie. Nous allons prouver l'existence des ensembles indépendants à l'aide du théorème d'intersection, que nous appliquerons aux matroïdes $\mathcal{M}_1$ et $\mathcal{M}_2$ définis lors de la démonstration du théorème 35. Pour mémoire : $\mathcal{M}_1 = (E_0, \mathcal{I}_1)$ avec $E_0 := E \times \{1, \dots, k\}$ et

$$\mathcal{I}_1 := \{X \subseteq E_0 : \forall i \in \{1, \dots, k\}, \{e \in E : (e, i) \in X\} \in \mathcal{I}\},$$

et $\mathcal{M}_2 = (E_0, \mathcal{I}_2)$ avec

$$\mathcal{I}_2 := \{X \subseteq E_0 : \forall e \in E, |\{i \in \{1, \dots, k\} : (e, i) \in X\}| \leq 1\}.$$

Il existe k ensembles $I_1, \dots, I_k$ indépendants de $\mathcal{M}$ dont la réunion est E si (et seulement si) il existe un sous-ensemble de E_0 de taille $|E|$ qui soit indépendant à la fois dans $\mathcal{M}_1$ et dans $\mathcal{M}_2$. En effet, soit X un sous-ensemble de

7. Exercice 7 de la feuille d'exercices.

E_0 appartenant à $\mathcal{I}_1 \cap \mathcal{I}_2$ tel que $|X| = |E|$. Pour tout $i \in \{1, \dots, k\}$, posons $I_i := \{e \in E : (e, i) \in X\}$. Alors $I_i \in \mathcal{I}$ car $X \in \mathcal{I}_1$. De plus,

$$|E| = |X| = \sum_{i=1}^k |I_i| = \left| \bigcup_{i=1}^k I_i \right|,$$

où la dernière égalité vient du fait que $I_i \cap I_j = \emptyset$ si $i \neq j$ car $X \in \mathcal{I}_2$. Ainsi, $\bigcup_{i=1}^k I_i = E$. (Réciproquement, en posant $I'_1 := I_1$ et $I'_i := I_i \setminus \bigcup_{j=1}^{i-1} I_j$ si $i \geq 2$, l'ensemble $\bigcup_{i=1}^k I'_i \times \{i\}$ est un sous-ensemble de E_0 de taille $|E|$ qui appartient à $\mathcal{I}_1 \cap \mathcal{I}_2$.)

Supposons que (4.4) soit satisfaite. D'après le théorème d'intersection, il suffit de prouver que $r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2) \geq |E|$ pour toute partition (E_1, E_2) de E_0 . Puisque, si $(e, i) \in E_2$ alors $r_{\mathcal{M}_2}(E_2 + (e, i')) = r_{\mathcal{M}_2}(E_2)$, nous pouvons supposer sans perte de généralité qu'il existe un ensemble $E' \subseteq E$ tel que $E_2 = E' \times \{1, \dots, k\}$. Ainsi, $r_{\mathcal{M}_2}(E_2) = |E'|$. De plus, $E_1 = (E \setminus E') \times \{1, \dots, k\}$. En particulier, $r_{\mathcal{M}_1}(E_1) = k \cdot r_{\mathcal{M}}(E \setminus E')$.

Par (4.4), il suit que $r_{\mathcal{M}_1}(E_1) \geq |E| - |E'|$. En conséquent, $r_{\mathcal{M}_1}(E_1) + r_{\mathcal{M}_2}(E_2) \geq |E| - |E'| + |E'| = |E|$, ce qui conclut la preuve. $\square$

Exercice 39. Prouvez le théorème 37 à l'aide du théorème 38.

Nous citerons deux autres conséquences du théorème d'intersection. La première est algorithmique et la seconde est souvent utile dans des problèmes combinatoires.

Le « degré moyen » d'un graphe G , noté $\text{AD}(G)$, est le rapport entre la somme des degrés des sommets et le nombre de sommets. Soit G un graphe. Le « degré moyen maximum » de G , noté $\text{MAD}(G)$, est le maximum des degrés moyens de ses sous-graphes, c'est-à-dire

$$\text{MAD}(G) = \max \{ \text{AD}(H) : H \text{ sous-graphe de } G \}.$$

D'une certaine manière, le degré moyen maximum d'un graphe capture la partie la plus dense du graphe. Il est particulièrement utile pour travailler avec les graphes dont la densité est bornée, comme par exemple les graphes plongés sur une surface (comme les graphes planaires) qui en outre ne possèdent pas de cycle de longueur inférieure à une constante fixée.

Théorème 40. *Il est possible de calculer le degré moyen maximum d'un graphe en temps polynomial en la taille du graphe.*

Soient E un ensemble fini et $X_1, \dots, X_m$ des sous-ensembles de E . Rappelons qu'un transversal de la famille $(X_1, \dots, X_m)$ est un sous-ensemble $\{x_1, \dots, x_m\}$ de E tel que $x_i \in X_i$ pour tout $i \in \{1, \dots, m\}$ (définition 22). Si $(Y_1, \dots, Y_m)$ est aussi une famille de sous-ensembles de E , un « transversal commun » à $(X_1, \dots, X_m)$ et $(Y_1, \dots, Y_m)$ est un sous-ensemble $\{z_1, \dots, z_m\}$ de E tel que $z_i \in X_i \cap Y_i$ pour tout $i \in \{1, \dots, m\}$. Le théorème suivant fournit une condition nécessaire et suffisante pour l'existence d'un tel transversal.

Théorème 41. *Soit E un ensemble fini. Soient $(X_1, \dots, X_m)$ et $(Y_1, \dots, Y_m)$ deux familles de sous-ensembles de E . Il existe un transversal commun à ces deux familles si, et seulement si, pour tout $I \subseteq \{1, \dots, m\}$ et tout $J \subseteq \{1, \dots, m\}$,*

$$\left| \left(\bigcup_{i \in I} X_i \right) \cap \left(\bigcup_{j \in J} Y_j \right) \right| \geq |I| + |J| - m.$$

5. REPRÉSENTABILITÉ DES MATROÏDES

5.1. Matroïde vectoriel et isomorphismes. Nous avons vu dans l'exemple 2 le matroïde vectoriel. Un corps $\mathbf{F}$ est fixé, ainsi qu'une matrice A à coefficients dans $\mathbf{F}$. Les éléments du matroïde vectoriel $\mathcal{M}(A)$ associé à A sont les colonnes de A . Un ensemble d'éléments de A est indépendant dans $\mathcal{M}(A)$ si, et seulement si, les colonnes correspondantes sont linéairement indépendantes sur $\mathbf{F}$.

Il est possible d'effectuer des opérations sur A sans changer le matroïde vectoriel associé. Plus précisément, deux matroïdes $\mathcal{M}_1$ et $\mathcal{M}_2$ sont « isomorphes » si, et seulement si, il existe une fonction $f : E(\mathcal{M}_1) \rightarrow E(\mathcal{M}_2)$ telle que $I \in \mathcal{I}(\mathcal{M}_1)$ si, et seulement si, $f(I) \in \mathcal{I}(\mathcal{M}_2)$. Les matroïdes vectoriels associés aux matrices A et A' sont isomorphes dès que A' s'obtient à partir de A en effectuant l'une des opérations suivantes.

- (i) Échanger deux lignes de A .
- (ii) Multiplier une ligne de A par un élément non nul de $\mathbf{F}$.
- (iii) Remplacer une ligne de A par la somme de cette ligne avec une autre ligne.
- (iv) Supprimer une ligne de A constituée uniquement de 0 (sauf si c'est la seule ligne de A).
- (v) Échanger deux colonnes de A .
- (vi) Multiplier une colonne de A par un élément non nul de $\mathbf{F}$.
- (vii) Remplacer chaque entrée de A par son image par un automorphisme fixé de $\mathbf{F}$.

Soit A est une matrice de rang r possédant r lignes et n colonnes. Il est possible, en effectuant une suite d'opérations parmi (i)–(vii), d'obtenir à partir de A une matrice de la forme $[I_r | D]$ où I_r est la matrice identité de taille $r \times r$ sur $\mathbf{F}$ et D est une matrice de taille $r \times (n - r)$ à coefficients dans $\mathbf{F}$.

5.2. Représentation d'un matroïde. Soit $\mathbf{F}$ un corps. Un matroïde $\mathcal{M}$ est « représentable sur $\mathbf{F}$ » si, et seulement si, il existe une matrice A à coefficients dans $\mathbf{F}$ telle que $\mathcal{M}(A)$ soit isomorphe à $\mathcal{M}$. Le matroïde $\mathcal{M}$ est « représentable » si, et seulement si, il existe un corps $\mathbf{F}$ sur lequel $\mathcal{M}$ soit représentable.

Ainsi, un matroïde de rang r sur un ensemble à n éléments est représentable sur un corps $\mathbf{F}$ si, et seulement si, il existe une matrice D de taille $r \times (n - r)$ à coefficients dans $\mathbf{F}$ telle que $\mathcal{M}$ soit isomorphe au matroïde vectoriel associé à la matrice $[I_r | D]$. Une telle matrice est une « représentation standard » de $\mathcal{M}$ sur $\mathbf{F}$.

Exemple 42. Posons

$$A := \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Vue comme matrice sur $\mathbf{F}_2$, le matroïde vectoriel associé à A est le matroïde uniforme $U_{2,3}$. Vue comme matrice à coefficients dans $\mathbf{F}_3$, le matroïde vectoriel associé à A est le matroïde $U_{3,3}$.

Tous les matroïdes ne sont pas représentables sur tous les corps. Considérons par exemple le matroïde uniforme $U_{2,4}$, i.e. l'ensemble des éléments est $\{1, 2, 3, 4\}$ et un sous-ensemble est indépendant si, et seulement si, son cardinal est au plus deux. Alors $U_{2,4}$ n'est pas représentable sur $\mathbf{F}_2$. En effet, si $\mathcal{M}$ est représentable sur $\mathbf{F}_2$, alors $\mathcal{M}$ est isomorphe au matroïde vectoriel associé à une matrice A de la forme

$$\left(\begin{array}{cc|cc} 1 & 0 & * & * \\ 0 & 1 & * & * \end{array} \right).$$

De plus, toute paire de colonnes de A doit former un couple de vecteurs linéairement indépendants sur $\mathbf{F}_2$. Ceci est impossible car $(\mathbf{F}_2)^2$ ne possède que trois vecteurs non nuls.

En revanche, $U_{2,4}$ est représentable sur $\mathbf{R}$, en prenant

$$A := \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}.$$

Il existe également des matroïdes représentables sur *tous les corps*, comme les matroïdes graphiques. En effet, soient $\mathbf{F}$ un corps et G un graphe avec ensemble de sommets $\{v_1, \dots, v_n\}$ et ensemble d'arêtes $\{e_1, \dots, e_m\}$ les arêtes de G . Soit A' la matrice de taille $n \times m$ à coefficients dans $\mathbf{F}$ telle que $A'_{i,j} = 1$ si l'arête e_j est incidente au sommet v_i dans G et $A'_{i,j} = 0$ sinon. La matrice A' est appelée « matrice d'incidence » du graphe G . La matrice A' possède donc exactement deux 1 dans chaque colonne. Soit A une matrice obtenue à partir de A' en remplaçant, dans chaque colonne, l'un des deux 1 par -1 . (En particulier, $A = A'$ si $\mathbf{F} = \mathbf{F}_2$.)

Montrons que le matroïde graphique associé à G est isomorphe au matroïde vectoriel associé à A . À cette fin, il est suffisant (en vertu de l'exercice 7) de prouver que la famille de circuits du matroïde vectoriel associé à A correspond exactement à la famille de cycles élémentaires de G .

Tout d'abord, si les vecteurs colonnes $(e_j)_{j \in X}$ forment un ensemble minimal de vecteurs non linéairement indépendants sur $\mathbf{F}$, il existe une combinaison linéaire $\sum_{j \in X} \alpha_j \cdot e_j$ égale au vecteur nul avec $\alpha_j \in \mathbf{F}^\times$ pour tout $j \in X$. Soit G' le sous-graphe de G induit par les arêtes $(e_j)_{j \in X}$. Tous les sommets de G' ont degré au moins 2 dans G' , donc G' contient un cycle.

Réciproquement, soit C un cycle élémentaire de G ; prouvons que les vecteurs colonnes de A correspondant aux arêtes dans C ne sont pas linéairement indépendants. Sans perte de généralité, nous pouvons supposer que $C = v_1, e_1, \dots, v_k, e_k, v_1$, avec $e_i = (v_i, v_{i+1})$ pour $i \in \{1, \dots, k-1\}$ et $e_k = (v_k, v_1)$. L'idée est de fixer une orientation du cycle et d'ajuster le signe de chaque vecteur colonne en fonction de cette orientation. Plus précisément (et en identifiant les arêtes de G et les vecteurs colonnes de A pour alléger les notations), nous considérons la combinaison linéaire

$$x := \sum_{j=1}^k A_{j,j} \cdot e_j,$$

dont les coefficients sont dans $\mathbf{F}^*$ par définition. Pour tout $i \in \{1, \dots, n\}$, il suit que $x_i = 0$ si $i > k$ et (en calculant l'indice modulo k dans $\{1, \dots, k\}$) $v_i = A_{i-1,i-1} A_{i,i-1} + A_{i,i}^2 = -1 + 1 = 0$ si $i \leq k$.

Nous obtenons ainsi l'observation suivante.

Proposition 43. *Tout matroïde graphique est représentable sur tout corps $\mathbf{F}$.*

Définition 44. Un matroïde qui est représentable sur

- $\mathbf{F}_2$ est « binaire » ;
- $\mathbf{F}_3$ est « ternaire » ;
- tous les corps est « régulier ».

Il est possible de démontrer le fait suivant.

Théorème 45. *Un matroïde est régulier si, et seulement si, il est binaire et représentable sur un corps de caractéristique différente de 2.*

Qu'en est-il de la représentabilité du dual d'un matroïde ?

Théorème 46. *Soit $\mathcal{M}$ un matroïde représentable sur un corps $\mathbf{F}$. Alors $\mathcal{M}^*$ est représentable sur $\mathbf{F}$.*

Démonstration. Soient n le nombre d'éléments de A et r son rang. Considérons une représentation standard $[I_r | D]$ de $\mathcal{M}$ sur $\mathbf{F}$, notée A . Nous allons démontrer que $A^* := [D^T | I_{n-r}]$ est une représentation de $\mathcal{M}^*$ sur $\mathbf{F}$. À cette fin, nous montrons que

- (i) si X est un ensemble d'indices de cardinal r tel que les colonnes $(A_j)_{j \in X}$ de A soient linéairement indépendantes sur $\mathbf{F}$, alors les colonnes $(A_j^*)_{j \notin X}$ de A^* sont linéairement indépendantes sur $\mathbf{F}$;
- (ii) réciproquement, pour tout ensemble X^* d'indices de cardinal $n - r$ tel que les colonnes $(A_j^*)_{j \in X^*}$ de A^* soient linéairement indépendantes sur $\mathbf{F}$, les colonnes $(A_j)_{j \notin X^*}$ de A sont linéairement indépendantes sur $\mathbf{F}$.

En réalité, (ii) se démontre de la même manière que (i) ; aussi ne prouverons-nous que (i).

Quitte à permuter des colonnes et des lignes de A (et de A^*), nous pouvons supposer que $X = \{1, \dots, s\} \cup \{r + 1, \dots, r + (r - s)\}$. Posons $X^* := \{s + 1, \dots, r\} \cup \{2r - s, \dots, n\}$. En outre, écrivons A de la manière suivante :

$$A = \begin{pmatrix} e_1 \cdots e_s & e_{s+1} \cdots e_r & e_{r+1} \cdots e_{2r-s} & e_{2r-s+1} \cdots e_n \\ I_s & 0 & D_{11} & D_{12} \\ 0 & I_{r-s} & D_{21} & D_{22} \end{pmatrix}$$

ainsi,

$$A^* = \begin{pmatrix} D_{11}^T & D_{21}^T & I_{r-s} & 0 \\ D_{12}^T & D_{22}^T & 0 & I_{n+s-2r} \end{pmatrix}.$$

Notre but est de prouver que $(A_j^*)_{j \in X^*}$ est un système linéairement indépendant sur $\mathbf{F}$, i.e. un système de rang $n - r$. Pour cela, il suffit de montrer que le rang de la matrice D_{21}^T est égal à $r - s$. Or ceci est vrai car $(A_j)_{j \in X}$ est un système linéairement indépendant sur $\mathbf{F}$, et donc le rang de D_{21} vaut $r - s$. $\square$

5.3. Matroïdes non représentables. S'il est des matroïdes réguliers, il en est également qui ne sont représentables sur aucun corps. Il est possible de démontrer que tout matroïde avec au plus 7 éléments est représentable (sur au moins un corps). En revanche, le matroïde de Vámos contient 8 éléments et n'est pas représentable. Nous donnons deux autres exemples de matroïdes non représentables : la somme directe du matroïde de Fano et du matroïde non Fano et le matroïde non Pappus.

5.3.1. Le matroïde de Vámos.

Définition 47. Le « matroïde de Vámos », noté V_8 , est le matroïde sur l'ensemble $E := \{a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4\}$ dont les bases sont tous les sous-ensembles de E de taille 4 exceptés

$$\{a_1, b_1, a_2, b_2\}, \{a_1, b_1, a_4, b_4\}, \{a_2, b_2, a_3, b_3\}, \{a_2, b_2, a_4, b_4\}, \{a_3, b_3, a_4, b_4\}.$$

Exercice 48. Démontrez que V_8 est bien un matroïde.

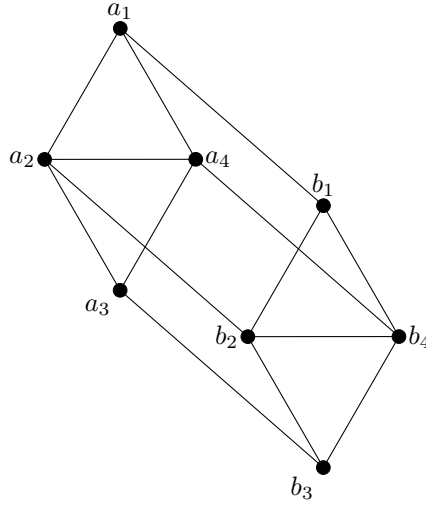
Des considérations élémentaires d'algèbre permettent de démontrer le résultat suivant.

Théorème 49. *Le matroïde de Vámos n'est pas représentable.*

Démonstration. Supposons, par l'absurde, que le matroïde de Vámos est représentable sur un corps $\mathbf{F}$. Pour un ensemble $L \subseteq \mathbf{F}^4$, nous notons $\langle L \rangle$ le sous-espace vectoriel de $\mathbf{F}^4$ engendré par L . Pour un sous-espace vectoriel V de $\mathbf{F}^4$, nous notons $\dim(V)$ la dimension de V .

Comme le rang de V_8 est égal à 4, il existe une fonction $\psi: E(V_8) \rightarrow \mathbf{F}^4$ telle que pour tout $X \subseteq E(V_8)$,

$$r_{V_8}(X) = \dim(\langle \psi(X) \rangle).$$

FIGURE 1. Le matroïde de Vámos V_8 .

Afin d'alléger l'écriture, si $\{x_1, \dots, x_k\}$ est un sous-ensemble de $E(V_8)$, nous posons

$$\mathcal{L}(x_1, \dots, x_k) := \langle \{\psi(x_1), \dots, \psi(x_k)\} \rangle.$$

Par exemple, par définition, $\dim(\mathcal{L}(a_1, b_1, a_3, b_3)) = r_{V_8}(\{a_1, b_1, a_3, b_3\}) = 4$. Nous allons obtenir une contradiction en montrant que $\dim(\mathcal{L}(a_1, b_1, a_3, b_3)) = 3$.

Tout d'abord,

$$\begin{aligned} \dim(\mathcal{L}(a_1, b_1) \cap \mathcal{L}(a_2, a_4, b_2, b_4)) &= \dim(\mathcal{L}(a_1, b_1)) + \dim(\mathcal{L}(a_2, a_4, b_2, b_4)) - \dim(\langle \mathcal{L}(a_1, b_1) \cup \mathcal{L}(a_2, a_4, b_2, b_4) \rangle) \\ &= 2 + 3 - 4 = 1. \end{aligned}$$

Ainsi, il existe un vecteur non nul $v \in \mathbf{F}^4$ tel que $\mathcal{L}(a_1, b_1) \cap \mathcal{L}(a_2, a_4, b_2, b_4) = \langle \{v\} \rangle$.

Nous allons montrer que $\langle \{v\} \rangle = \mathcal{L}(a_2, b_2) \cap \mathcal{L}(a_4, b_4)$. Pour cela, commençons par noter que

$$\begin{aligned} \dim(\mathcal{L}(a_1, b_1, a_2, b_2) \cap \mathcal{L}(a_2, a_4, b_2, b_4)) &= \dim(\mathcal{L}(a_1, b_1, a_2, b_2)) + \dim(\mathcal{L}(a_2, a_4, b_2, b_4)) \\ &\quad - \dim(\langle \mathcal{L}(a_1, b_1, a_2, b_2) \cup \mathcal{L}(a_2, a_4, b_2, b_4) \rangle) \\ &= 3 + 3 - 4 = 2. \end{aligned}$$

En particulier, comme $\dim(\mathcal{L}(a_2, b_2)) = 2$, nous déduisons que $\mathcal{L}(a_1, b_1, a_2, b_2) \cap \mathcal{L}(a_2, a_4, b_2, b_4) = \mathcal{L}(a_2, b_2)$. Par conséquent, comme $\langle \{v\} \rangle \subseteq \mathcal{L}(a_1, b_1) \cap \mathcal{L}(a_2, a_4, b_2, b_4) \subseteq \mathcal{L}(a_1, b_1, a_2, b_2) \cap \mathcal{L}(a_2, a_4, b_2, b_4) = \mathcal{L}(a_2, b_2)$, il suit

$$\langle \{v\} \rangle \subseteq \mathcal{L}(a_2, b_2).$$

Par symétrie, nous inférons que $\langle \{v\} \rangle \subseteq \mathcal{L}(a_4, b_4)$. Or,

$$\begin{aligned} \dim(\mathcal{L}(a_2, b_2) \cap \mathcal{L}(a_4, b_4)) &= \dim(\mathcal{L}(a_2, b_2)) + \dim(\mathcal{L}(a_4, b_4)) - \dim(\langle \mathcal{L}(a_2, b_2) \cup \mathcal{L}(a_4, b_4) \rangle) \\ &= 2 + 2 - 3 = 1, \end{aligned}$$

donc $\langle \{v\} \rangle = \mathcal{L}(a_2, b_2) \cap \mathcal{L}(a_4, b_4)$.

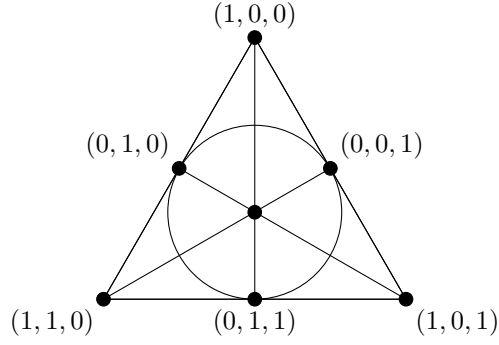


FIGURE 2. Le matroïde de Fano F_7 : l'ensemble des éléments est $\mathbf{F}_2^3 \setminus \{(0, 0, 0)\}$ et les bases sont les triplets (x, y, z) d'éléments tels que $x + y + z \neq (0, 0, 0)$.

Par symétrie, $\langle \{v\} \rangle = \mathcal{L}(a_1, b_1) \cap \mathcal{L}(a_3, b_3)$. En conséquent,

$$\begin{aligned} \dim(\mathcal{L}(a_1, b_1, a_3, b_3)) &= \dim(\langle \mathcal{L}(a_1, b_1) \cup \mathcal{L}(a_3, b_3) \rangle) \\ &= \dim(\mathcal{L}(a_1, b_1)) + \dim(\mathcal{L}(a_3, b_3)) - \dim(\mathcal{L}(a_1, b_1) \cap \mathcal{L}(a_3, b_3)) \\ &= 2 + 2 - 1 = 3. \end{aligned}$$

Néanmoins, l'ensemble $\{a_1, b_1, a_3, b_3\}$ est par définition indépendant dans V_8 , donc de rang 4. Cette contradiction conclut la démonstration. $\square$

5.3.2. Matroïde de Fano.

Définition 50. Le *matroïde de Fano*, noté F_7 , est le matroïde sur l'ensemble $E := \mathbf{F}_2^3 \setminus \{(0, 0, 0)\}$ dont les bases sont tous les triplets d'éléments distincts de E dont la somme dans $\mathbf{F}_2^3$ est non nulle.

Exercice 51. Vérifiez que F_7 est bien un matroïde.

Remarque 3. De manière équivalente, le matroïde de Fano est le matroïde sur $E := \{1, \dots, 7\}$ dont les bases sont tous les sous-ensembles de taille 3 de $\{1, \dots, 7\}$ exceptés

$$\{1, 2, 3\}, \{1, 4, 7\}, \{1, 5, 6\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 5\}, \{3, 6, 7\}.$$

Une notion utile est celle de « circuit fondamental ». Considérons un matroïde $\mathcal{M}$ et une base B de $\mathcal{M}$. D'après le lemme du circuit unique⁸, pour tout $e \in E(\mathcal{M}) \setminus B$, l'ensemble $B + e$ contient un et un seul circuit. Ce circuit est appelé « circuit fondamental de e respectivement à la base B ».

Considérons à présent une représentation standard A de $\mathcal{M}$ sur un corps $\mathbf{F}$. Ainsi, $A = [I_r | D]$ où r est le rang de $\mathcal{M}$. Les éléments de $\mathcal{M}$ correspondant aux r premières colonnes de A forment une base B de $\mathcal{M}$. De plus, il existe également une correspondance naturelle entre les *lignes* de A et les éléments de B . Notons $b_1, \dots, b_r$ les éléments de B de sorte que b_i corresponde à la colonne (et à la ligne) i de A , pour $i \in \{1, \dots, r\}$.

Soient $e \in E(\mathcal{M}) \setminus B$ et C le circuit fondamental de e respectivement à B . Les éléments de B contenus dans C se lisent directement dans la matrice A . En effet, notons j l'indice de la colonne correspondant à l'élément e (donc $j \in \{r+1, \dots, |E(\mathcal{M})|\}$). Pour $i \in \{1, \dots, k\}$, l'élément b_i appartient à C si, et seulement si, le coefficient $A(i, j)$ est non nul.

⁸. Exercice 4 de la feuille d'exercice.

Soit $D^\#$ la matrice obtenue à partir de D en remplaçant chaque entrée non nulle par 1. La matrice $D^\#$ est appelée « matrice des circuits fondamentaux respectivement à B ». À titre d'exemple, la matrice $D^\#$ pour F_7 est

$$(5.1) \quad H := \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Exercice 52. Soit H la matrice définie par (5.1).

- (i) Montrez que $[I_3|H]$ est une représentation de F_7 sur $\mathbf{F}_2$.
- (ii) Soit $\mathbf{F}$ un corps de caractéristique différente de 2. Montrez que $[I_3|H]$ n'est pas une représentation de F_7 sur $\mathbf{F}$.

Notons que la matrice $D^\#$ est définie également pour les matroïdes non représentables : ses colonnes correspondent aux vecteurs d'incidence des éléments de B appartenant aux circuits fondamentaux. La matrice $[I_r|D^\#]$ est une « représentation partielle de $\mathcal{M}$ » ; elle existe donc même si $\mathcal{M}$ n'est pas représentable. Par ailleurs, l'unicité des circuits fondamentaux (respectivement à une base et un élément donnés) nous assure l'unicité de la représentation partielle d'un matroïde.

Proposition 53. Soit $\mathcal{M}$ un matroïde de rang r . Si $[I_r|D_1]$ et $[I_r|D_2]$ sont deux représentations de $\mathcal{M}$ (pas nécessairement sur le même corps) avec le même isomorphisme (i.e. pour tout i , les colonnes i de chaque matrice correspondent au même élément de $\mathcal{M}$), alors $D_1^\# = D_2^\#$.

La proposition 53 et le théorème 46 impliquent le fait suivant.

Proposition 54. Soient $\mathcal{M}$ un matroïde représentable et B une base de $\mathcal{M}$. Si $D^\#$ est la matrice des circuits fondamentaux respectivement à B , alors $(D^\#)^T$ est la matrice des circuits fondamentaux respectivement à la base $E(\mathcal{M}) \setminus B$ du matroïde $\mathcal{M}^*$.

Remarque 4. L'hypothèse de représentabilité du matroïde $\mathcal{M}$ dans l'énoncé de la proposition 54 n'est pas nécessaire.

Avant de continuer plus avant notre présentation du matroïde de Fano, nous allons définir un nouveau matroïde.

Définition 55. Le « matroïde non Fano », noté F_7^- est le matroïde sur $E := \{1, \dots, 7\}$ dont les bases sont tous les sous-ensembles de taille 3 de $\{1, \dots, 7\}$ exceptés

$$\{1, 2, 3\}, \{1, 4, 7\}, \{1, 5, 6\}, \{2, 5, 7\}, \{3, 4, 5\}, \{3, 6, 7\}.$$

Exercice 56.

- (i) Vérifiez que F_7^- est bien un matroïde.
- (ii) Donnez la représentation partielle de F_7^- .
- (iii) Déduisez-en une représentation de F_7^- sur tout corps $\mathbf{F}$ de caractéristique différente de 2.
- (iv) Montrez que $[I_3|H]$ n'est pas une représentation de F_7^- sur $\mathbf{F}_2$.

Nous avons donc vu que F_7 est représentable sur $\mathbf{F}_2$ par $[I_3|H]$ et F_7^- est représentable sur tout corps différent de $\mathbf{F}_2$ par $[I_3|H]$, où H est la matrice définie par (5.1). Ces résultats sont optimaux, au sens suivant.

Théorème 57. Soit $\mathbf{F}$ un corps.

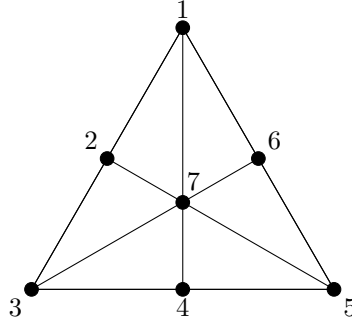


FIGURE 3. Le matroïde non Fano.

- (i) Le matroïde F_7 est représentable sur $\mathbf{F}$ si, et seulement si, $\mathbf{F}$ est de caractéristique 2.
- (ii) Le matroïde F_7^- est représentable sur $\mathbf{F}$ si, et seulement si, $\mathbf{F}$ est de caractéristique différente de 2.

Le théorème 57 nous permet de construire un nouveau matroïde non représentable.

Corollaire 58. *Le matroïde $F_7 \oplus F_7^-$ n'est pas représentable.*

Afin de démontrer le théorème 57, il nous suffit de démontrer le fait suivant.

Proposition 59. *Soit $\mathcal{M} \in \{F_7, F_7^-\}$. Si $[I_3|X]$ est une représentation de $\mathcal{M}$ sur un corps $\mathbf{F}$, alors X est égale à la matrice H donnée par (5.1).*

Démonstration. Soit B une base de $\mathcal{M}$ telle que X soit la matrice des circuits fondamentaux respectivement à B . Comme $[I_3|H]$ est une représentation de $\mathcal{M}$ (sur $\mathbf{F}_2$ si $\mathcal{M} = F_7$ et sur $\mathbf{F}_3$ si $\mathcal{M} = F_7^-$), la proposition 53 implique que $X^\# = H^\#$, qui vaut H .

Ainsi, quitte à multiplier des colonnes et des lignes de X par des éléments non nuls de $\mathbf{F}$, nous pouvons supposer qu'il existe trois éléments a, b et c de $\mathbf{F}^\times$ tels que

$$X = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & c & 1 \\ a & b & 0 & 1 \end{pmatrix}.$$

Notons à présent que les colonnes 3, 6 et 7 de $[I_3|X]$ sont liées. Il découle que, nécessairement, $c = 1$. Nous inférons similairement que $b = 1$ et $a = 1$. Ainsi, $X = H$. En particulier, $\mathbf{F} = \mathbf{F}_2$ si $\mathcal{M} = F_7$ et $\mathbf{F} \neq \mathbf{F}_2$ si $\mathcal{M} = F_7^-$. $\square$

5.3.3. Le matroïde de Pappus.

Définition 60. Le « matroïde de Pappus » est le matroïde sur l'ensemble $E := \{1, \dots, 9\}$ dont les bases sont tous les sous-ensembles de E de taille 3 exceptés

$$\{1, 2, 3\}, \{1, 4, 8\}, \{1, 5, 9\}, \{2, 4, 7\}, \{2, 6, 9\}, \{3, 5, 7\}, \{3, 6, 8\}, \{4, 5, 6\}, \{7, 8, 9\}.$$

Exercice 61.

- (i) Démontrez que le matroïde de Pappus est bien un matroïde.
- (ii) Montrez que si le matroïde de Pappus est représentable sur un corps $\mathbf{F}$, alors $|\mathbf{F}| \geq 4$ et $\mathbf{F} \neq \mathbf{F}_5$.

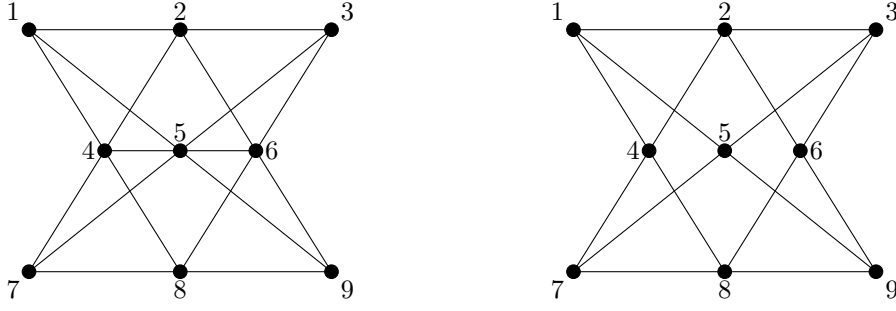


FIGURE 4. Le matroïde de Pappus et le matroïde non Pappus.

Définition 62. Le « matroïde non Pappus » est le matroïde sur l'ensemble $E := \{1, \dots, 9\}$ dont les bases sont tous les sous-ensembles de E de taille 3 exceptés

$$\{1, 2, 3\}, \{1, 4, 8\}, \{1, 5, 9\}, \{2, 4, 7\}, \{2, 6, 9\}, \{3, 5, 7\}, \{3, 6, 8\}, \{7, 8, 9\}.$$

Exercice 63. Démontrez que le matroïde non Pappus est bien un matroïde.

Le théorème de Pappus permet de démontrer que le matroïde non Pappus n'est pas représentable.

Théorème 64. *Le matroïde non Pappus n'est pas représentable.*

5.4. Représentation sur les corps finis. Il est intéressant d'obtenir des caractérisations des matroïdes représentables sur un corps fini donné. Cette question s'avère toutefois très difficile.⁹ Nous allons voir quelques résultats dans cette direction, en commençant par un exercice sur les matroïdes uniformes.

Exercice 65. Soient $\mathbf{F}$ un corps fini et n un entier au moins égal à 2. Le matroïde $U_{2,n}$ est représentable sur $\mathbf{F}$ si, et seulement si, $|\mathbf{F}| \geq k - 1$.

Passons à présent aux matroïdes binaires, pour lesquelles nous donnerons la caractérisation suivante (notons qu'une union disjointe peut être vide (union disjointe sur la collection vide d'objets)).

Théorème 66. *Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde. Les assertions suivantes sont équivalentes.*

- (i) *Le matroïde $\mathcal{M}$ est binaire.*
- (ii) *Si $C \in \mathcal{C}(\mathcal{M})$ et $C^* \in \mathcal{C}^*(\mathcal{M})$, alors $|C \cap C^*|$ est pair.*
- (iii) *La différence symétrique de deux circuits quelconques de $\mathcal{M}$ contient un circuit.*
- (iv) *La différence symétrique de deux circuits quelconques de $\mathcal{M}$ est une union disjointe de circuits.*
- (v) *La différence symétrique de tout ensemble de circuits est vide ou contient un circuit.*
- (vi) *Soit B une base de $\mathcal{M}$. Tout circuit de $\mathcal{M}$ s'exprime comme la différence symétrique de l'ensemble des circuits fondamentaux respectivement à B et e pour $e \in E$.*
- (vii) *Il existe une base B telle que tout circuit de $\mathcal{M}$ s'exprime comme la différence symétrique de l'ensemble des circuits fondamentaux respectivement à B et e pour $e \in E$.*

9. Il est par exemple possible de caractériser les matroïdes représentables sur $\mathbf{F}_i$ à l'aide de la notion de « mineurs exclus » pour $i \in \{2, 3, 4\}$. Toutefois, il n'est pas connu (conjecture de Rota) que pour tout corps fini $\mathbf{F}$, il existe une liste finie de mineurs exclus caractérisant les matroïdes représentables sur $\mathbf{F}$.

Nous ne donnons pas de démonstration du théorème 66, mais nous allons voir deux résultats intermédiaires. Si $\mathcal{M}$ est un matroïde et A est une représentation de $\mathcal{M}$, alors pour tout ensemble C d'éléments de $\mathcal{M}$ nous notons $\sigma_A(C)$ (ou juste $\sigma(C)$) la somme des colonnes de A qui correspondent aux éléments de C .

Lemme 67. *Soit $\mathcal{M}$ un matroïde binaire. La différence symétrique de toute paire de circuits de $\mathcal{M}$ est une union disjointe de circuits de $\mathcal{M}$.*

Démonstration. Soient C_1 et C_2 deux circuits de $\mathcal{M}$ et soit $C_0 := C_1 \triangle C_2$. Notons A une représentation de $\mathcal{M}$ sur $\mathbf{F}_2$. Si $i \in \{1, 2\}$, alors $\sigma(C_i) = \vec{0}$ car C_i est un circuit. En remarquant que $\sigma(C_0) = \sigma(C_1) + \sigma(C_2)$ (puisque les éléments de $C_1 \cap C_2$ apparaissent deux fois dans la somme et donc n'apportent au final aucune contribution), nous déduisons que $\sigma(C_0) = \vec{0}$. Ainsi, $C_0 \notin \mathcal{I}(\mathcal{M})$.

Soient $C^1, \dots, C^k$ des sous-ensembles de C minimaux tels que $\sigma(C^i) = \vec{0}$ pour tout $i \in \{1, \dots, k\}$. Nécessairement, $C^i \cap C^j = \emptyset$ si $i \neq j$ et chaque ensemble C^i est un circuit par minimalité. Comme $\cup_{i=1}^k C^i = C$, la conclusion suit. $\square$

Nous avons déjà vu que, dans tout matroïde, l'intersection d'un circuit et d'un co-circuit ne peut pas être un singleton. Il est possible d'obtenir une propriété plus forte pour les matroïdes binaires.

Lemme 68. *Soit $\mathcal{M}$ un matroïde binaire. Si $C \in \mathcal{C}(\mathcal{M})$ et $C^* \in \mathcal{C}^*(\mathcal{M})$, alors $|C \cap C^*| \equiv 0 \pmod{2}$.*

Démonstration. Soient C un circuit de $\mathcal{M}$ et C^* un circuit de $\mathcal{M}^*$. La conclusion étant vraie si C et C^* sont disjoints, nous pouvons supposer l'existence d'un élément e contenu à la fois dans C et dans C^* . En particulier, il existe une base B^* de $\mathcal{M}^*$ contenant $C^* - e$. Soit $B := E(\mathcal{M}) \setminus B^*$; l'ensemble B est donc une base de $\mathcal{M}$ dont l'intersection avec C^* est égale à $\{e\}$.

Considérons une représentation standard A de $\mathcal{M}$ sur $\mathbf{F}_2$ correspondant à B , c'est-à-dire une matrice binaire $[I_r | D]$ dont les r premières colonnes correspondent aux éléments de B . Nous pouvons en outre supposer que la première colonne de A correspond à l'élément e . Ainsi, $[D^T | I_{n-r}]$ est une représentation de $\mathcal{M}^*$ sur $\mathbf{F}_2$, en notant n le nombre d'éléments de $\mathcal{M}$.

Comme C est un circuit de $\mathcal{M}$, nous savons que $\sigma_A(C) = \vec{0}$. En effet, comme $C \notin \mathcal{I}(\mathcal{M})$, il existe un sous-ensemble $C' \subseteq C$ tel que $\sigma_A(C') = \vec{0}$; et comme $C - x \in \mathcal{I}(\mathcal{M})$ si $x \in C$, il suit que $C' = C$.

Ainsi, le nombre de colonnes de D dont la première coordonnée vaut 1 est impair. Ces entrées sont les coordonnées non nulles de la première colonne D^T . Elles correspondent donc aux éléments de $C^* - e$. Ainsi, $C - e$ et $C^* - e$ ont un nombre impair d'éléments en commun. Par conséquent, le cardinal de l'intersection de C et C^* est pair, comme annoncé. $\square$