



SUR QUELQUES APPLICATIONS DU POLYNÔME DE TUTTE

par

BORIS ALBAR

M1 MATHÉMATIQUES - INFORMATIQUE

Stage M1 Mathématiques
Encadrant : Jorge Luis Ramírez Alfonsín

17 MAI 2010



TABLE DES MATIÈRES

TABLE DES MATIÈRES	iii
LISTE DES FIGURES	iv
NOTATIONS	1
INTRODUCTION	3
1 MATROÏDES ET POLYNÔME DE TUTTE	5
1.1 MATROÏDES	5
1.2 ISOMORPHISMES DE MATROÏDES	8
1.3 RANG D'UN MATROÏDE	9
1.4 QUELQUES EXEMPLES DE MATROÏDES	11
1.4.1 Matroïde linéaire	11
1.4.2 Matroïde graphique	12
1.4.3 Matroïde algébrique	14
1.5 OPÉRATIONS SUR LES MATROÏDES	15
1.5.1 Supression d'éléments	15
1.5.2 Contraction d'éléments	16
1.5.3 Mineurs d'un matroïde	16
1.5.4 Somme directe	17
1.5.5 Matroïde dual	18
1.6 INVARIANTS DE TUTTE-GROTHENDIECK	19
2 APPLICATIONS DU POLYNÔME DE TUTTE	31
2.1 POLYNÔME DE TUTTE D'UN MATROÏDE	31
2.1.1 Généralités	31
2.1.2 Nombre d'éléments du matroïde	35
2.1.3 Nombres de bases	35
2.1.4 Nombre d'indépendants	36
2.1.5 Polynôme des indépendants	37
2.2 POLYNÔME DE TUTTE D'UN MATROÏDE GRAPHIQUE	38
2.2.1 Polynôme chromatique	38
2.2.2 Le polynôme monochromatique	41
2.2.3 Le polynôme de flots	44
2.2.4 Le polynôme de connectivité	49
2.2.5 Orientations d'un graphe	50
2.2.6 Espace des bicycles et polynôme de Tutte	52
2.3 APPLICATIONS À LA PHYSIQUE STATISTIQUE	55
2.3.1 Le modèle d'Ising	56
2.3.2 Le modèle de Potts	60

2.4	APPLICATIONS À LA THÉORIE DES NOEUDS	60
2.4.1	Généralités	61
2.4.2	Graphe médial et graphe signé d'un entrelacs	62
2.4.3	Mais où est passé le polynôme de Tutte ?	66
2.5	ZONOTOPES ET THÉORIE D'ERHART	69
2.6	PHYSIQUE DU TAS DE SABLE ET JEUX COMBINATOIRES	75
2.7	APPLICATIONS À LA THÉORIE DES CODES	81
2.7.1	Generalités	81
2.7.2	Matroïdes et codes correcteurs	84
	CONCLUSION	91
	BIBLIOGRAPHIE	93

LISTE DES FIGURES

1.1	Exemple de matroïdes isomorphes	9
1.2	Treillis des fermés d'un matroïde vectoriel	10
1.3	Configuration de vecteurs dans \mathbb{R}^3	11
1.4	Un exemple de graphe	13
1.5	Interprétation des éléments du matroïde dans un graphe	14
1.6	Le graphe L	15
1.7	Le graphe C	15
1.8	Contraction dans un matroïde graphique	16
1.9	Somme directe de graphe	18
1.10	Un graphe G et son dual G'	19
2.1	Calcul récursif du polynôme de Tutte	34
2.2	Une 3-coloration propre d'un graphe	39
2.3	Exemple de \mathbb{Z}_4 -flot partout non-nul	45
2.4	Frustration géométrique dans un cristal tétraédrique de molécules d'eau	48
2.5	Tripartition des arcs d'un graphe	53
2.6	Alignement des spins dans le modèle ferromagnétique	56
2.7	Alignement des spins dans le modèle anti-ferromagnétique	56
2.8	Le noeud de trèfle	61
2.9	L'entrelacs borroméen	61
2.10	Mouvements de Reidemeister	62
2.11	Coloration du diagramme du noeud de trèfle	63
2.12	Graphe médial du noeud de trèfle $M(\textcircled{\circ})$	63
2.13	Signature des croisements	63
2.14	Graphe signé du noeud de trèfle droit	64
2.15	Croisements dans un diagramme orienté	65
2.16	Noeud de trèfle droit orienté : $\omega(\textcircled{\circ}) = 3$	65
2.17	Relation de Kauffman et graphe médial	66

2.18	Somme connexe d'un noeud de trèfle et d'un noeud de huit	67
2.19	Exemple de zonotope dans \mathbb{R}^2	72
2.20	Exemple de zonotope dans \mathbb{R}^3	73
2.21	Distance minimale et code correcteur	83
2.22	Arrangement d'hyperplan associé à un code	88

NOTATIONS

\mathbb{N}	ensemble des entiers naturels
\mathbb{Z}	ensemble des entiers relatifs
\mathbb{R}	ensemble des réels
\mathbb{C}	ensemble des nombres complexes
$\mathfrak{P}(E)$	ensemble des parties de E
$ E $	cardinal de l'ensemble E
$E - F$	l'ensemble des éléments de E n'appartenant pas à F
$\text{supp}(f)$	support de la fonction f

INTRODUCTION

En 1954, W.T. Tutte introduit une généralisation à deux variables du polynôme chromatique d'un graphe. Le polynôme chromatique était obtenu en trivialisant la nouvelle variable. Il s'est avéré que ce nouveau polynôme, nommé polynôme dichromate par Tutte, encodait de nombreuses informations sur la combinatoire du graphe. Le polynôme de Tutte a ensuite été étendu au cadre plus général des matroïdes. Les domaines d'application de ce polynôme sont extrêmement nombreux et passent par la théorie des noeuds, la physique statistique ou encore les codes linéaires...

Le but de ce stage est d'étudier certaines des applications du polynôme de Tutte. J'essaierai de mettre en évidence les liens unissant les divers domaines.

Dans un premier temps nous étudierons les matroïdes qui fournissent un cadre général pour l'expression du polynôme de Tutte. J'introduirai ensuite les invariants de Tutte-Grothendieck et le polynôme de Tutte ainsi que certaines de ses propriétés.

Dans un second temps nous verrons quelques-uns de ses domaines d'application.

MATROÏDES ET POLYNÔME DE TUTTE



Dans ce chapitre nous introduisons les principales définitions et théorèmes qui nous seront utiles par la suite. Dans un premier temps, une part sera donnée à l'étude des matroïdes puis à l'introduction des invariants de Tutte-Grothendieck.

1.1 MATROÏDES

La notion de matroïde a été introduite en 1935 par Whitney pour étudier la notion d'indépendance linéaire. Il existe de nombreuses axiomatiques équivalentes pour définir un matroïde. Nous utiliserons principalement la définition suivante :

Définition 1.1.1

Un *matroïde* \mathcal{M} est un couple (E, \mathcal{I}) tel que :

- E est un ensemble fini.
- \mathcal{I} est une collection de sous ensembles de E vérifiant :

$$(I_1) : \emptyset \in \mathcal{I}$$

$$(I_2) : \text{Si } I \subset J \text{ et } J \in \mathcal{I} \text{ alors } I \in \mathcal{I}$$

$$(I_3) : \text{Si } I, J \in \mathcal{I} \text{ et } |I| < |J| \text{ alors il existe } j \in J - I \text{ tel que } I \cup \{j\} \in \mathcal{I}.$$

Le dernier axiome est appelé **axiome d'échange**.

Nous préférons généralement utiliser cette définition qui nous paraît la plus naturelle car très proche de la notion d'indépendance linéaire dans les espaces vectoriels. Néanmoins, nous verrons plus loin une axiomatique équivalente définie à partir des bases du matroïde.

L'ensemble E sera appelé le **support** du matroïde \mathcal{M} et \mathcal{I} l'ensemble des **indépendants**. Un élément de \mathcal{I} sera appelé un indépendant. L'ensemble complémentaire de \mathcal{I} dans $\mathfrak{P}(E)$ sera appelé l'ensemble des dépendants et ses éléments les dépendants.

Notation 1.1.1

Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde. On note $E(\mathcal{M})$ l'ensemble E associé au matroïde \mathcal{M} et $\mathcal{I}(\mathcal{M})$ l'ensemble des indépendants. Lorsqu'il ne peut y avoir de confusion, on identifiera dans la suite \mathcal{I} à $\mathcal{I}(\mathcal{M})$ et E à $E(\mathcal{M})$.

Nous pouvons maintenant définir les bases d'un matroïde comme les indépendants maximaux, c'est à dire :

Définition 1.1.2

Soit \mathcal{M} un matroïde et $B \in \mathcal{I}$ un indépendant. On dit que B est une **base** de \mathcal{M} si $\forall e \in E, B \cup \{e\} \notin \mathcal{I}$.

Corollaire 1.1.1

Toutes les bases d'un matroïde ont la même taille.

PREUVE. Supposons que l'on ait une base B' de \mathcal{M} ayant strictement moins d'éléments que les autres bases. Il existe donc une base B de \mathcal{M} telle que $|B'| < |B|$. Or en utilisant l'axiome d'échange, on peut trouver un élément $j \in B - B'$ tel que $B' \cup \{j\} \in \mathcal{I}$, ce qui contredit la maximalité. ■

De la même manière, on définit les circuits comme les dépendants minimaux :

Définition 1.1.3

Soit \mathcal{M} un matroïde et $C \in \mathfrak{P}(E)$ tel que $C \notin \mathcal{I}$. C est un **circuit** de \mathcal{M} si $\forall e \in C, C - \{e\} \in \mathcal{I}$.

On peut montrer qu'il est équivalent de définir un matroïde par ses bases. Par exemple, la définition suivante définissant un matroïde à partir de ses bases est strictement équivalente à celle de la Définition 1 :

Définition 1.1.4

Un matroïde \mathcal{M} est un couple (E, \mathcal{B}) tel que :

- E est un ensemble fini.
- \mathcal{B} est une collection de sous-ensembles de E vérifiant :
 - (B1) : $\mathcal{B} \neq \emptyset$
 - (B2) : Pour tout $B, B' \in \mathcal{B}$ et $e \in B - B'$, il existe $f \in B' - B$ tel que $(B - \{e\}) \cup f \in \mathcal{B}$.

Nous aurons besoin du lemme suivant pour montrer l'équivalence entre les deux définitions.

Lemme 1.1.1

Tous les éléments de \mathcal{B} construits de la manière précédente, c'est à dire vérifiant les axiomes (B1) et (B2), sont de même cardinal.

PREUVE. Soit \mathcal{M} un matroïde et \mathcal{B} l'ensemble de ses bases. On choisit $B \in \mathcal{B}$ de cardinal minimal. On va montrer que toutes les autres bases sont de même cardinal par récurrence sur $|A - B|$.

- Si $|A - B| = 0$, alors B contient au moins tous les éléments de A donc $A \subseteq B$. Or par minimalité de B , on en déduit que $B = A$ puis que $|A| = |B|$.
- On suppose la propriété vraie au rang $n - 1$, nous allons le montrer au rang n .
Soit $A, B \in \mathcal{B}$ tels que $|A - B| = k > 0$. Il existe donc $a \in A - B$ et on peut donc trouver par (B2), $b \in B - A$ tel que $A - \{a\} \cup \{b\} \in \mathcal{B}$. Or

$|(A - \{a\} \cup \{b\}) - B| = k - 1$ car $b \in B$.

On peut appliquer l'hypothèse de récurrence et on en déduit que $|A - \{a\} \cup \{b\}| = |B|$ et $|A - \{a\} \cup \{b\}| = |A|$.

■

Nous pouvons maintenant montrer l'équivalence entre les deux définitions :

PREUVE. Soit $\mathcal{M} = (E, \mathcal{I})$ un matroïde et \mathcal{B} un ensemble de bases de \mathcal{M} .

On considère l'ensemble des indépendants et on veut montrer que les bases vérifient les axiomes (B1) et (B2) :

La propriété (B1) est évidente.

Considérons maintenant la propriété (B2).

Soit $A, B \in \mathcal{B}(\mathcal{M})$ et $a \in A - B$. Alors $A - \{a\} \in \mathcal{I}$ car A est une base de \mathcal{M} par hypothèse. Or $|A - \{a\}| < |B|$.

On peut donc appliquer l'axiome d'échange (I3) :

il existe $b \in B$ vérifiant $b \notin A - \{a\}$ tel que $A - \{a\} \cup \{b\} \in \mathcal{I}$. On a maintenant $|A - \{a\} \cup \{b\}| = |A|$ donc $A - \{a\} \cup \{b\} \in \mathcal{B}$.

Réciproquement soit \mathcal{B} une collection de bases de \mathcal{M} vérifiant les axiomes (B1) et (B2). On pose

$$\mathcal{I} = \{I \mid I \subset B, B \in \mathcal{B}\}$$

l'ensemble des parties des bases du matroïde. On veut montrer que (E, \mathcal{I}) est un matroïde.

On a clairement que $\emptyset \in \mathcal{I}$ par (B1). La propriété (I1) est donc vérifiée.

Soit maintenant $I \subset J$ et $J \in \mathcal{I}$ alors $J \subset B$ avec $B \in \mathcal{B}$ donc $I \subset B$ donc $I \in \mathcal{I}$. La propriété (I2) est donc vérifiée.

Il reste donc à vérifier l'axiome (I3).

On se donne donc $I, J \in \mathcal{I}$. Par le lemme précédent, les éléments de \mathcal{B} ont tous la même taille que l'on note r . On montre la propriété par récurrence sur $r - |J|$:

Si $r - |J| = 0$ alors $|J| = r$ et $J \in \mathcal{I}$ donc on peut trouver $B \in \mathcal{B}$ tel que $J \subset B$ et comme $|B| = r$ alors $J = B$ est une base. Maintenant on peut trouver $A \in \mathcal{B}$ tel que $I \subset A$. Si $(A - I) \cap J \neq \emptyset$, soit $a \in A \cap J$, alors $I \cup \{a\} \subset A$ donc $I \cup \{a\} \in \mathcal{I}$ et $a \in J - I$.

Par contre si $(A - I) \cap J = \emptyset$. Alors on a deux cas :

- Si $(A - I) - J \neq \emptyset$, soit $a \in (A - I) - J$ et $A, J \in \mathcal{B}$ donc par la propriété d'échange (B2), il existe un élément $j \in J - A$ tel que $A - \{a\} \cup \{j\} \in \mathcal{B}$. Or $I \subset A - \{a\}$ et $I \cup \{j\} \subset A - \{a\} \cup \{j\} \in \mathcal{B}$ donc $I \cup \{j\} \in \mathcal{I}$ et $j \in J - I$.
- Si $A - J = \emptyset$ et $(A - I) \cap J = \emptyset$, alors $A = I$ et $|J| > |I| = |A|$ ce qui est une contradiction avec le lemme précédent car A et J sont des éléments de \mathcal{B} .

Donc la propriété est vraie dans le cas de base.

Supposons la propriété vraie au rang $n - 1$ et montrons-la au rang n .

Soit $I, J \in \mathcal{I}$ tels que $|I| < |J|$ et $r - |J| = k$. On peut trouver $A, B \in \mathcal{B}$ tels que $I \subset A$ et $J \subset B$. On peut aussi trouver, comme dans le cas précédent, $b \in B - I$ tel que $I \cup \{b\} \in \mathcal{I}$.

On a alors deux cas possibles :

- Si $b \in J$ alors c'est fini, on a $I \cup \{b\} \in \mathcal{I}$ et $b \in J - I$.
- Si $b \notin J$ alors comme $J \cup \{b\} \subset B$, on a $J \cup \{b\} \in \mathcal{I}$. De plus $|I \cup \{b\}| < |J \cup \{b\}|$ car $|I| < |J|$. Or $r - |J \cup \{b\}| = k - 1$ donc on peut appliquer l'hypothèse de récurrence :
Il existe $c \in (J \cup \{b\}) - (I \cup \{b\}) = J - I$, c'est à dire que $c \in J - I$, tel que $I \cup \{b\} \cup \{c\} \in \mathcal{I}$. On en déduit donc que $I \cup \{c\} \in \mathcal{I}$.

■

Nous voyons que la démonstration est loin d'être triviale. Il existe encore d'autres manières équivalentes de définir les matroïdes, par exemple à partir de ses circuits :

Définition 1.1.5

Un matroïde \mathcal{M} est un couple (E, \mathcal{C}) tel que :

- E est un ensemble fini.
- \mathcal{C} est une collection de sous-ensembles de E vérifiant :

(C1) : $\emptyset \notin \mathcal{C}$

(C2) : Pour tout $C_1, C_2 \in \mathcal{C}$, si $C_1 \subseteq C_2$ alors $C_1 = C_2$. On dit que les éléments sont incomparables pour l'inclusion.

(C3) : On a la propriété d'élimination :

$\forall C_1, C_2 \in \mathcal{C}$ tels que $C_1 \neq C_2, \forall e \in C_1 \cap C_2, \exists C_3 \in \mathcal{C}, C_3 \in (C_1 \cup C_2) \setminus \{e\}$.

Nous nous réfèrerons à (Oxl) pour la démonstration de l'équivalence de cette définition.

1.2 ISOMORPHISMES DE MATROÏDES

Nous définissons ici un isomorphisme de matroïde qui étend la définition d'isomorphisme de graphe, c'est à dire un réétiquetage des éléments du matroïde qui "conserve" les indépendants.

Définition 1.2.1

Soit $\mathcal{M} = (E, \mathcal{I})$ et $\mathcal{M}' = (E', \mathcal{I}')$ deux matroïdes. \mathcal{M} et \mathcal{M}' sont dit **isomorphes** s'il existe une bijection de E vers E' qui induit une bijection de \mathcal{I} vers \mathcal{I}' .

Dans le cas d'un matroïde graphique, on retrouve bien la définition des isomorphismes de graphe.

Exemple : La figure 1.1 montre un matroïde graphique et un matroïde linéaire isomorphes. Il n'est en effet pas difficile de voir qu'ils ont les même bases.

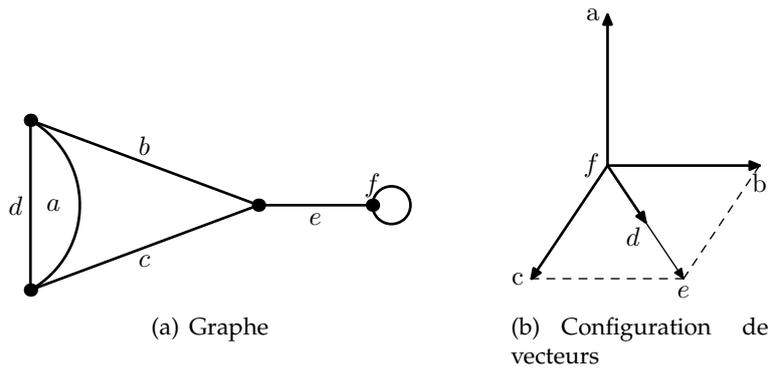


FIG. 1.1 – Exemple de matroïdes isomorphes

1.3 RANG D'UN MATROÏDE

Étant donné un matroïde \mathcal{M} , on peut définir une certaine fonction appelée fonction rang que nous noterons r :

Définition 1.3.1

On appelle fonction de rang $r : 2^{|E|} \rightarrow \mathbb{N}$, la fonction définie par

$$r(X) = \max\{|I| \mid I \subseteq X \text{ et } I \in \mathcal{I}\}.$$

On appelle rang du matroïde et on note $r(\mathcal{M})$ le cardinal des bases de \mathcal{M} .

Cette définition est parfaitement naturelle en algèbre linéaire. On ne sera donc pas perdu lorsque l'on travaillera avec des matroïdes linéaires.

Dans un matroïde graphique $\mathcal{M}(G)$, la fonction de rang correspond à :

$$r(A) = |V(G)| - \kappa(A),$$

avec $\kappa(A)$ le nombre de composantes connexes de A .

La fonction rang vérifie certaines propriétés :

Proposition 1.3.1

Soit \mathcal{M} un matroïde. On appelle fonction de rang une fonction de $r : \mathfrak{P}(E) \rightarrow \mathbb{N}$ vérifiant :

- $r(A) \leq |A|$ pour tous $A \in \mathfrak{P}(A)$,
- Si $A, B \in \mathfrak{P}(E)$ tels que $A \subset B$, alors $r(A) \leq r(B)$,
- Si $A, B \in \mathfrak{P}(E)$ alors $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

PREUVE. Les deux premières propriétés sont triviales.

On va montrer la dernière propriété qui exprime la sous-modularité de la fonction r .

Soit I un indépendant maximal contenu dans $A \cap B$. Alors I est aussi un indépendant de $A \cup B$ que l'on peut compléter en un indépendant I' pour le rendre maximal dans $A \cup B$.

On peut décomposer la partie I' en une partie X uniquement incluse dans A , une partie Y uniquement incluse dans B et une partie Z incluse dans l'intersection de A et B . Donc $r(A \cup B) = |I'| = |X| + |Y| + |Z|$. Or

$r(A \cap B) = |Y|$. De plus par définition, $r(A) \geq |X| + |Y|$ car $X \cup Y \subset A$. De même $r(B) \geq |Z| + |Y|$.

On en déduit que $r(A) + r(B) \geq |X| + 2|Y| + |Z| = r(A \cup B) + r(A \cap B)$. ■

En fait on peut montrer que les trois propriétés ci-dessus sont assez fortes pour définir un matroïde, ce qui permet de donner une définition alternative d'un matroïde à partir d'une telle fonction.

La fonction de rang permet aussi de définir une fonction de fermeture :

Définition 1.3.2

On appelle *opérateur de fermeture* et on note cl la fonction définie par

$$cl : \mathfrak{P}(E) \rightarrow \mathfrak{P}(E)$$

$$X \mapsto \{x \in E \mid r(X \cup \{x\}) = r(X)\}.$$

On appelle *fermé* de \mathcal{M} , un sous-ensemble $F \subset E$ tel que $cl(F) = F$.

L'ensemble des fermés d'un matroïde forme un treillis géométrique (c'est à dire que $cl(\emptyset) = \emptyset$ et pour tout $x \in E$, $cl(\{x\}) = \{x\}$) pour l'inclusion comme le montre la figure 1.2 dans le cas d'un matroïde (c'est-à-dire lorsque les fermés sont les sous-espaces vectoriels).

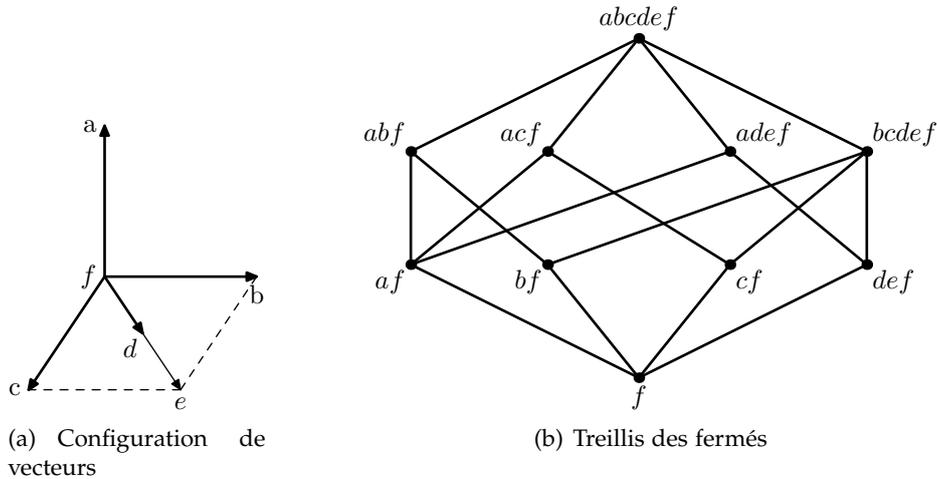


FIG. 1.2 – Treillis des fermés d'un matroïde vectoriel

L'information perdue dans le passage au treillis des fermés consiste uniquement aux boucles et aux éléments en parallèles. En fait nous avons la proposition suivante :

Proposition 1.3.2

Un treillis est géométrique si et seulement si il correspond à un treillis des fermés d'un matroïde.

On a donc une correspondance bijective entre les treillis géométriques et les matroïdes sans boucles ni éléments en parallèles. Nous n'aurons que très rarement par la suite besoin de cette notion donc nous ne développons pas plus ce paragraphe.

1.4 QUELQUES EXEMPLES DE MATROÏDES

On introduit ici plusieurs exemples importants de matroïdes. Certains seront fondamentaux pour la suite.

1.4.1 Matroïde linéaire

Proposition 1.4.1

On considère un ensemble de vecteurs E d'un K -espace vectoriel. On considère maintenant \mathcal{I} l'ensemble des parties de E linéairement indépendantes. Alors (E, \mathcal{I}) est un matroïde que l'on appelle matroïde vectoriel.

PREUVE. On vérifie aisément que les propriétés de la Définition 1 sont vérifiées :

1. Par définition de la notion d'indépendance linéaire, la famille vide est libre donc $\emptyset \in \mathcal{I}$.
2. Soit $J \in \mathcal{I}$ un ensemble de vecteurs linéairement indépendants et $I \subset J$. Alors trivialement I est un ensemble de vecteurs linéairement indépendants donc $I \in \mathcal{I}$.
3. Soit $I = \{i_1, \dots, i_n\}$ et $J = \{j_1, \dots, j_m\}$ deux familles libres de vecteurs tels que $n < m$. Supposons par l'absurde que pour tout $j \in J - I$, la famille $I \cup \{j\}$ soit liée alors comme I est une famille libre il existe des scalaires $(\lambda_1, \dots, \lambda_n)$ non tous nuls tels que $j = \lambda_1 i_1 + \dots + \lambda_n i_n$ alors $j \in \text{Vect}(i_1, \dots, i_n)$ donc $\dim(\text{Vect}(J)) = \dim(\text{Vect}(I))$ or $\dim(\text{Vect}(I)) = n < m = \dim(\text{Vect}(J))$. On a donc une contradiction.

■

Exemple : Si l'on considère l'ensemble de vecteurs de \mathbb{R}^3 donnés par la figure 1.3. Les indépendants sont alors les ensembles de vecteurs linéairement indépendants suivants :

$$\{a, b, c, d, e, ab, ac, ad, ae, bc, bd, be, cd, ce, abc, abd, abe, acd, ace\}.$$

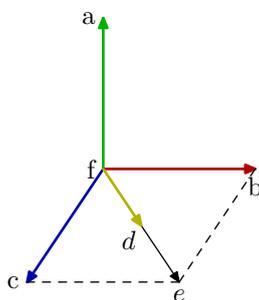


FIG. 1.3 – Configuration de vecteurs dans \mathbb{R}^3

Nous pouvons trouver des matroïdes linéaires dans différents endroits :

Remarque 1.4.1

Soit M une matrice $k \times l$ à coefficients dans un corps \mathbb{K} . Alors on peut considérer le matroïde linéaire engendré par les dépendances des lignes ou des colonnes de la

matrice. Le support du matroïde est alors les lignes (ou les colonnes) de la matrice en supposant que chaque vecteur ne se trouve qu'en un seul exemplaire.

De manière équivalente on peut construire un matroïde à partir d'un sous-espace vectoriel de \mathbb{R}^n en considérant un ensemble de vecteurs engendrant le sous-espace vectoriel.

Si un matroïde M est isomorphe à un matroïde linéaire sur un corps \mathbb{K} alors on dit que M est **représentable** sur \mathbb{K} . Les matroïdes graphiques simples (sans boucles ni éléments parallèles) sont représentables sur le corps à deux éléments, ils sont dit binaires. Nous verrons plus loin des matroïdes réguliers, représentables sur n'importe quel corps.

Un exemple de matroïde linéaire que nous utiliserons par la suite est donné en considérant l'indépendance des formes linéaires associées à un ensemble d'hyperplans :

Exemple : Soit $\mathcal{A}_1, \dots, \mathcal{A}_n$ un arrangement d'hyperplans. On dit que k hyperplans sont indépendants si la codimension de leur intersection est k .

On construit sur ce principe une fonction de rang. Cette fonction est bien définie (en tant que fonction de rang d'un matroïde) lorsque l'intersection des hyperplans est non vide. On dit qu'un arrangement d'hyperplan est **central** lorsque l'intersection des hyperplans est non-vide. A tout arrangement central d'hyperplans \mathcal{A} , on peut lui associer un matroïde $\mathcal{M}_{\mathcal{A}}$.

Nous pouvons définir un ensemble d'hyperplans par leurs vecteurs normaux. On vérifie facilement que le matroïde linéaire défini sur cet ensemble de vecteurs est isomorphe au matroïde d'un arrangement central d'hyperplans.

1.4.2 Matroïde graphique

Nous voyons ici comment définir un matroïde à partir d'un graphe.

Proposition 1.4.2

Soit $G = (V, E)$ un graphe et \mathcal{I} la collection des ensembles d'arêtes ne formant pas de cycles, alors (E, \mathcal{I}) est un matroïde qu'on appelle matroïde graphique.

PREUVE. On montre que (E, \mathcal{I}) vérifie les propriétés de la Définition 1 :

1. L'ensemble vide ne contient aucune arête donc aucun cycle, par suite $\emptyset \in \mathcal{I}$.
2. Soit $J \in \mathcal{I}$ et I tel que $I \subset J$. Les graphe induit par l'ensemble d'arêtes $J, (V, J)$ est sans cycles donc (V, I) est aussi sans cycles car $I \subset J$ donc $I \in \mathcal{I}$.
3. On remarque que si I est un indépendant alors le graphe induit par I a $|V| - |I|$ composantes connexes. En effet lorsqu'on ajoute une nouvelle arête à un indépendant, soit la nouvelle arête forme un cycle et le nombre de composantes connexes reste le même, soit on ne forme pas de cycle et donc l'arête relie deux composantes connexes différentes, donc le nombre de composantes connexes diminue de 1.

Or comme un indépendant ne forme pas de cycle par définition, une récurrence immédiate sur le nombre d'arêtes de I donne le résultat.

Maintenant on peut trouver une arête de J qui relie deux composantes connexes du graphe (V, I) . En effet supposons par l'absurde que, pour toute arête $j \in J$, $I \cup \{j\}$ ne modifie pas le nombre de composantes connexes, alors si on ajoute toutes les arêtes de J , on ne modifie pas non plus le nombre de composantes connexes du graphe (V, I) . On a donc $(V, J \cup I)$ a $|V| - |I|$ composantes connexes. Or par la remarque précédente, (V, J) a $|V| - |J| < |V| - |I|$ composantes connexes car $|I| < |J|$. Et $(V, J \cup I)$ a au moins autant de composantes connexes que (V, J) . On a une contradiction avec le nombre de composantes connexes de $(V, J \cup I)$ trouvé précédemment.

Exemple : Si l'on considère le graphe donné par la figure 1.4 alors les indépendants du matroïde sont $\{1, 2, 3, 4, 12, 13, 14, 23, 24, 34\}$.

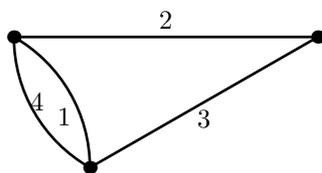


FIG. 1.4 – Un exemple de graphe

Nous pouvons maintenant donner une interprétation des composantes (indépendants, bases, circuits, ...) d'un matroïde graphique en terme de graphe :

Corollaire 1.4.1

Soit G un graphe, et $\mathcal{M}(G)$ le matroïde graphique associé. Nous avons les propriétés suivantes :

1. les indépendants sont les forêts de G .
2. les bases sont les forêts couvrantes maximales de G .
3. les circuits sont les cycles de G .

PREUVE. Le premier point est immédiat par définition, en effet une forêt est un sous-graphe de G sans cycles (mais pas forcément connexe).

Ainsi les indépendants du matroïde graphique correspondent aux forêts du graphe. Nous cherchons désormais une forêt maximale pour l'inclusion. Pour cela on ajoute les arêtes une par une et on ne conserve que celles qui ne forment pas de cycles dans le sous-graphe induit. Ce processus est exactement l'algorithme de création d'une forêt couvrante de G . Si G est connexe, alors les bases du matroïde sont des arbres couvrants de G . Ce qui conclut le deuxième point.

Pour le troisième point, les cycles sont clairement des dépendants minimaux car supprimer n'importe quel arc du cycle revient à le casser donc à le rendre indépendant. Réciproquement supposons que l'on ait un dépendant minimal qui ne soit pas un cycle, alors on peut trouver un cycle strictement contenu dans ce dépendant, ce qui est absurde par minimalité. Les cycles sont donc les circuits du matroïde. ■

Nous pouvons illustrer la propriété précédente sur le graphe suivant :

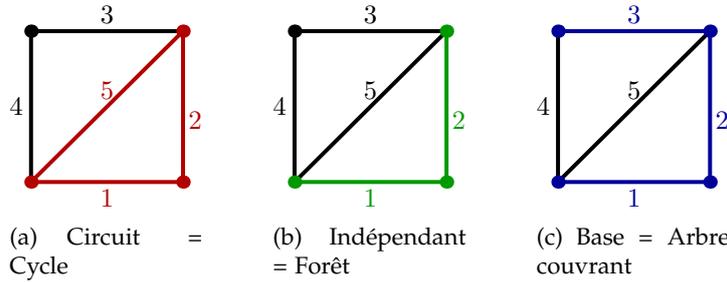


FIG. 1.5 – Interprétation des éléments du matroïde dans un graphe

Néanmoins la classe des matroïdes graphiques n'est pas distincte des matroïdes linéaires vus précédemment. Au contraire, comme le montre la proposition suivante, les matroïdes graphiques peuvent être considérés comme une sous-classe des matroïdes linéaires :

Proposition 1.4.3

Tout matroïde graphique est linéaire.

PREUVE. Soit $G = (V, E)$ un graphe et $\mathcal{M}(G)$ son matroïde associé. Nous allons montrer que $\mathcal{M}(G)$ est un matroïde linéaire. Pour tout $v \in V$ on associe le vecteur :

$$x_v = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow v\text{-ième position}$$

et on considère la transformation $\pi : E \rightarrow \text{Vect}\{x_{v_1}, \dots, x_{v_n}\}$ qui pour tout $e = (v, w) \in E$ associe le vecteur $x_e = x_v - x_w$. Si deux arêtes relient les mêmes sommets alors on associe le premier à x_e et le deuxième à $2 \cdot x_e$ de manière à avoir une bijection entre E et $\pi(E) = \{\pi(e) \mid e \in E\}$. On note $\mathcal{M}(\pi(E))$ le matroïde linéaire associé à l'ensemble de vecteurs $\pi(E)$. On veut maintenant montrer qu'il existe une bijection entre les indépendants de $\mathcal{M}(G)$ et ceux de $\mathcal{M}(\pi(E))$.

Il suffit maintenant de remarquer que les cycles dans le graphe sont équivalents à la donnée d'un ensemble linéairement dépendant des vecteurs construits comme ci-dessus, ce qui nous donne l'isomorphisme entre $\mathcal{M}(G)$ et $\mathcal{M}(\pi(E))$. ■

1.4.3 Matroïde algébrique

Pour terminer cette série (incomplète) d'exemples. Nous avons vu que les matroïdes graphiques formaient une sous-classe des matroïdes linéaires. Il existe une autre classe, plus large, contenant les matroïdes linéaires : les matroïdes algébriques.

On se donne \mathbb{K} un corps quelconque et \mathbb{E} une extension du corps \mathbb{K} . Un élément $u \in \mathbb{E}$ est algébrique sur \mathbb{K} s'il existe un polynôme non-nul $P \in \mathbb{K}[X]$ tel que $P(u) = 0$. De la même manière, on dit que le n -uplet $(a_1, \dots, a_n) \in \mathbb{E}^n$ est algébriquement dépendant sur \mathbb{K} s'il existe un polynôme non-nul $P \in \mathbb{K}[X_1, \dots, X_n]$ tel que $P(a_1, \dots, a_n) = 0$. On peut généraliser cette définition pour obtenir la notion d'ensemble algébrique. Dans ce cas le matroïde ayant comme support un ensemble fini de \mathbb{E} et constitué des sous-ensembles indépendants (au sens algébrique) forme un matroïde.

Il est clair que tout matroïde linéaire sur un corps \mathbb{K} est algébrique sur une extension de \mathbb{K} .

Exemple : Si l'on considère $\mathbb{K} = \mathbb{C}$ et $\mathbb{E} = \mathbb{C}[X, Y, Z]$. En considérant les éléments $Z, (Y + Z)^2, XY + XZ, X, X^{-1}, 1 + i$, on retrouve le matroïde de la figure 1.1 et les éléments précédents correspondent, dans l'ordre, aux arêtes a, b, c, d, e, f . Il est facile de constater que ces deux matroïdes ont les mêmes circuits (par exemple, on a une dépendance algébrique donnée par $X \cdot X^{-1} - 1 = 0$ donc les arêtes d et e forment un circuit).

1.5 OPÉRATIONS SUR LES MATROÏDES

Certaines opérations sur le support d'un matroïde permettent de construire de nouveaux matroïdes. On définit ici certaines de ces constructions qui nous seront utiles par la suite.

Deux types d'éléments jouent un rôle particulier (qui sera très important par la suite) :

- les boucles qui sont les éléments du matroïde qui n'appartiennent à aucun indépendant. Par la suite nous noterons L le matroïde avec une seule boucle, ce qui en terme de matroïde graphique donne le graphe :



FIG. 1.6 – Le graphe L

- les co-boucles ou isthmes sont les éléments du matroïde qui appartiennent à toutes les bases. Dans la suite nous noterons C , le matroïde avec un seul isthme, ce qui en terme de matroïde graphique donne le graphe :



FIG. 1.7 – Le graphe C

On note $\mathcal{M} = (E, \mathcal{I})$ un matroïde dans la suite.

1.5.1 Suppression d'éléments

Définition 1.5.1

Soit $e \in E$ un élément du matroïde qui ne soit pas un isthme. On définit le

matroïde obtenu par suppression de e par

$$\mathcal{M} - e = (E - \{e\}, \{I \in \mathcal{I} : e \notin I\}).$$

PREUVE. La preuve qu'il s'agit d'un matroïde est immédiate à partir du moment où l'on remarque que les indépendants de \mathcal{M} ne contenant pas e sont bien des indépendants de $\mathcal{M} - e$. ■

La suppression dans un matroïde vectoriel ou graphique s'exprime naturellement par la suppression d'un vecteur ou d'un arc.

On peut généraliser cette propriété de suppression à tout un ensemble d'éléments puis définir la **restriction** $\mathcal{M}|_F$ d'un matroïde \mathcal{M} à un sous-ensemble F du support de \mathcal{M} par :

$$\mathcal{M}|_F = \mathcal{M} - (E - A).$$

Dans le cas des matroïdes associés à un sous-espace vectoriel, cette propriété consiste à prendre un sous-espace vectoriel et à considérer le matroïde linéaire associé.

1.5.2 Contraction d'éléments

De la même manière on peut considérer la contraction d'éléments du matroïde :

Définition 1.5.2

Soit $e \in E$ un élément du matroïde qui ne soit pas une boucle. On définit le matroïde obtenu par suppression de e par

$$\mathcal{M}/e = (E - \{e\}, \{I - \{e\} : e \in I \in \mathcal{I}\}).$$

Dans un matroïde graphique la contraction d'un élément s'exprime en supprimant l'arête et en assimilant les deux sommets de cette arête :

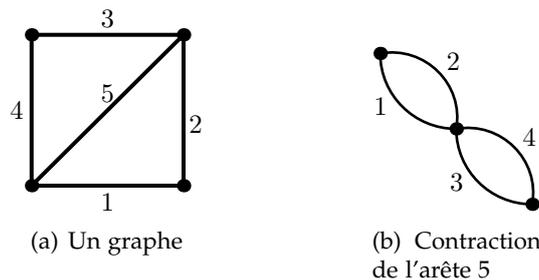


FIG. 1.8 – Contraction dans un matroïde graphique

En terme de matroïde vectoriel, la suppression correspond à la projection orthogonale sur le sous-espace vectoriel engendré par $E - \{e\}$.

1.5.3 Mineurs d'un matroïde

Les matroïdes obtenus par une suite finie de suppressions et de contractions d'éléments sont appelés des mineurs de M . Cette classe de ma-

troïdes est particulièrement importante dans l'étude des invariants de Tutte-Grothendieck comme nous le verrons par la suite.

La propriété fondamentale de ces constructions est qu'elles ne dépendent pas de l'ordre dans lequel les opérations de suppression et de contraction sont effectuées. De manière plus formelle, on a la propriété suivante :

Proposition 1.5.1

Soit $e, f \in E(\mathcal{M})$ deux éléments distincts du support de \mathcal{M} . Alors on a :

$$(\mathcal{M} - e)/f \simeq (\mathcal{M}/f) - e$$

autrement dit les opérations de suppression et de contraction commutent.

PREUVE. Premièrement, les deux matroïdes ont le même support qui est $E - \{e, f\}$.

On considère maintenant l'ensemble des indépendants. Dans le premier cas, l'ensemble des indépendants correspond aux éléments de I ne contenant pas e et privés de f . Dans le deuxième cas ils s'agit des indépendants de I privés de l'éléments f et ne contenant pas e . Comme les éléments sont supposés distincts alors ces deux ensembles sont égaux donc la propriété est démontrée. ■

De plus les opérations de contractions et suppressions sont "duales" (nous verrons par la suite la définition de dualité) :

Proposition 1.5.2

Soit e un élément du matroïde, on a la relation :

$$\mathcal{M}/e = (\mathcal{M}^* - e)^*.$$

1.5.4 Somme directe

On peut aussi définir une somme directe sur les matroïdes :

Proposition 1.5.3

Soient deux matroïdes $\mathcal{M}_1 = (E_1, \mathcal{I}_1)$ et $\mathcal{M}_2 = (E_2, \mathcal{I}_2)$. On définit la somme directe $\mathcal{M}_1 \oplus \mathcal{M}_2$ comme le matroïde de support $E_1 \sqcup E_2$ et comme ensemble d'indépendants $\mathcal{I}_1 \times \mathcal{I}_2$.

En terme de matroïde graphique, la somme directe peut se voir avec deux composantes connexes d'un graphe ou bien avec deux graphes partageant un unique sommet comme le montre la figure 1.9.

La somme directe de deux matroïdes linéaires de deux configurations de vecteurs $\mathcal{V}_1 \subset V_1$ et $\mathcal{V}_2 \subset V_2$ peut se voir comme le matroïde associé à la configuration de vecteurs $(0 \oplus \mathcal{V}_1) \sqcup (\mathcal{V}_2 \oplus 0)$ de $V_1 \oplus V_2$.

En terme de rang, un corollaire de la définition est :

Corollaire 1.5.1

Soit $\mathcal{M}_1 \oplus \mathcal{M}_2$ la somme directe de deux matroïdes, alors on a

$$r(\mathcal{M}_1 \oplus \mathcal{M}_2) = r(\mathcal{M}_1) + r(\mathcal{M}_2).$$

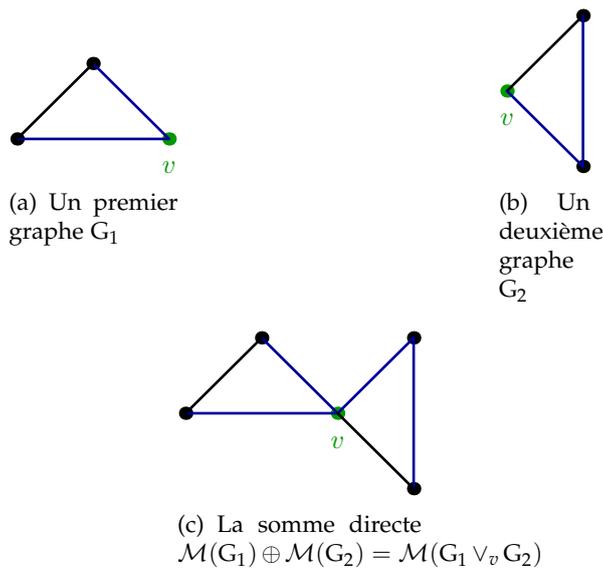


FIG. 1.9 – Somme directe de graphe

1.5.5 Matroïde dual

En théorie des graphes, la dualité joue un rôle extrêmement important dans l'étude des graphes planaires, c'est à dire des graphes admettant un plongement plan sans croisement des arêtes.

Nous voyons ici comment on peut généraliser cette notion aux matroïdes. On définit un matroïde à partir de ses bases. Dans ce cas, les complémentaires des bases forment un nouvel ensemble de bases qui caractérise le matroïde dual.

Théorème 1.5.1

Soit $\mathcal{M} = (E, \mathcal{B})$ un matroïde. Soit

$$\mathcal{B}^* = \{E - B \mid B \in \mathcal{B}\}.$$

Alors (E, \mathcal{B}^*) est un matroïde appelé **matroïde dual**.

PREUVE. On cherche à vérifier les axiomes (B1) et (B2).

Il est clair que (B1) est vérifié car l'ensemble des éléments de E n'est pas une base.

Soit $A^*, B^* \in \mathcal{B}^*$, alors il existe par définition des bases A et B de \mathcal{M} telles que $A^* = E - A$ et $B^* = E - B$. Soit $e \in A^* - B^* = E - A - (E - B) = B - A$. Or B et A sont des bases de \mathcal{M} et $e \in B - A$ donc il existe $f \in A - B$ tel que $A - \{e\} \cup \{f\} \in \mathcal{B}$. Donc le complémentaire de cette base de \mathcal{M} $A^* - \{f\} \cup \{e\}$ est une base de \mathcal{M}^* . Donc la propriété (B2) est bien vérifiée. ■

On peut exprimer le rang du matroïde dual en fonction du rang du matroïde :

Corollaire 1.5.2

On note r^* la fonction rang du matroïde dual. On a la relation :

$$r^*(E - A) = |E| - r(E) - |A| + r(A).$$

On regarde ce qui se passe dans le cas des matroïdes linéaires :

Proposition 1.5.4

Si \mathcal{M} est le matroïde linéaire associé à un sous-espace de \mathbb{R}^n alors le matroïde dual est isomorphe au matroïde linéaire associé au complémentaire orthogonal du sous-espace dans \mathbb{R}^n .

De manière plus générale on peut étendre cette propriété aux matroïdes représentables sur un corps. Si un matroïde est représentable sur un corps \mathbb{K} quelconque alors son dual est aussi représentable sur \mathbb{K} .

La notion de dualité généralise aussi la notion de dualité dans les graphes planaires :

Proposition 1.5.5

Soit G un graphe planaire et G^* son graphe dual, alors le dual du matroïde graphique associé à G est isomorphe au matroïde graphique associé à G^* .

La figure 1.9 donne un exemple de graphe dual. Et on peut montrer que le matroïde de la figure 1.1 est autodual, c'est à dire que son dual est isomorphe à lui même.

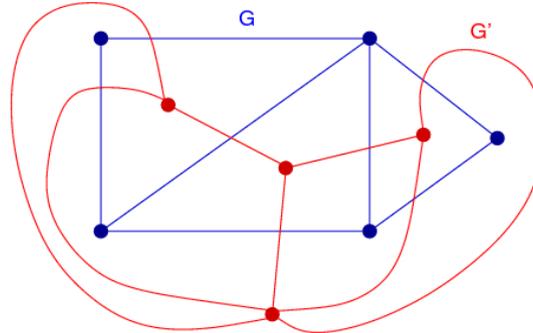


FIG. 1.10 – Un graphe G et son dual G'

1.6 INVARIANTS DE TUTTE-GROTHENDIECK

Nous définissons ici des invariants de matroïdes construits à partir de suppressions et contractions d'éléments.

Nous introduisons formellement les anneaux de Tutte-Grothendieck de manière catégorique en partant de la notion de décomposition introduite par Brylawski [].

On a besoin pour cela d'un peu de théorie des multiensembles. Les multiensembles sont une généralisation des ensembles où les éléments d'un ensemble peuvent apparaître plus d'une fois.

Définition 1.6.1

On appelle **multiensemble** les couples (A, m) tels que A soit un ensemble non-vide appelé **support** de A et m une fonction de A dans l'ensemble des entiers naturels. Pour tout élément $a \in A$, $m(a)$ est appelé **multiplicité** de a .

Le cas des multiensembles à support fini nous permet de définir une notion de cardinalité d'un ensemble qui étend la notion classique :

Définition 1.6.2

On dit qu'un multiensemble est fini si c'est un multiensemble à support fini. Dans ce cas la somme $\sum_{e \in E} f(e)$ est bien définie et on l'appelle la **cardinalité** de f et on note $|f|$. On dit que f est vide si $|f| = 0$.

La notation classique des multiensembles est la suivante :

Notation 1.6.1

On note $\{\{2, 2, 3, 2, 4\}\}$ le multiensemble fini de support $\{2, 3, 4\}$ et avec la multiplicité : $f(2) = 3$, $f(3) = 1$, $f(4) = 1$. Lorsque le multiensemble f est de cardinal fini, on peut écrire le multiensemble sous la forme $\sum_{i=0}^{|f|} a_i$ avec $a_i \in A$, par exemple dans le cas précédent, on l'écrira $2 + 2 + 3 + 2 + 4$.

On remarque que si f ne prend pas de valeurs supérieures à 1, alors on peut voir f comme un sous-ensemble de A puisque les éléments apparaissent au plus une fois.

On peut définir une opération commutative sur l'ensemble des multiensembles finis notée $a + b$ où le support est donné par l'union des supports de a et b et la fonction de multiplicité est donnée par :

$$\forall a, b \in M, f(a + b) = f(a) + f(b).$$

Ainsi on a muni les multiensembles finis d'une structure de monoïde commutatif libre engendré par A et l'élément identité correspond au multiensemble vide, c'est-à-dire dont la fonction de multiplicité est identiquement nulle.

On peut maintenant introduire la notion de décomposition d'une ensemble :

Définition 1.6.3

Une **décomposition** $D(A)$ sur un ensemble A est une catégorie ayant comme objets les multiensembles finis non-vides de A et les morphismes de multiensembles vérifiant :

1. $\text{Hom}(f, g) = \begin{cases} \{(f, g)\} & \text{si } |f| < |g| \text{ ou si } f = g \\ \emptyset & \text{sinon} \end{cases}$
2. $\text{Hom}(f + g, h) \neq \emptyset$ si et seulement si il existe h_1 et h_2 tels que $h_1 + h_2 = h$, $\text{Hom}(f, h_1) \neq \emptyset$ et $\text{Hom}(g, h_2) \neq \emptyset$.

Si $\text{Hom}(f, g) \neq \emptyset$ alors on dit que f se **décompose** dans g et on note $f < g$. En effet, on a construit une relation d'ordre partielle sur les sous-

multiensemble, en utilisant la cardinalité, de manière à ce que cette relation d'ordre se comporte bien pour la relation $+$. Pour cet ordre, les plus petits éléments sont les éléments de A .

On peut voir la cardinalité comme un foncteur dans la catégorie des entiers naturels ordonnés. En effet l'ensemble des entiers naturels muni de la relation d'ordre canonique forme une catégorie dont les morphismes sont donnés par les fonctions préservant l'ordre. Les morphismes de la catégorie sont alors donnés par :

$$\text{Hom}(a, b) = \begin{cases} \{(a, b)\} & \text{si } a \leq b \\ \emptyset & \text{sinon} \end{cases}$$

La reflexivité assure l'existence de l'identité tandis que la transitivité de la relation d'ordre donne une composition naturelle de ces morphismes. De plus comme les classes de morphismes possèdent un unique élément alors cette composition est associative.

Définition 1.6.4

On dit qu'un élément $a \in A$ est **irréductible** ou **indécomposable** si $\forall b \in D(A)$, $a \not\leq b$.

Ces éléments vont jouer un rôle important puisque l'on va chercher à décomposer les éléments de A en un multiensemble formé d'éléments irréductibles. On dit qu'une telle décomposition est **complète**.

Dans le cas des matroïdes nous nous plaçons en considérant l'ensemble S des classes d'isomorphismes de matroïde :

Si e est un élément d'un matroïde M qui n'est ni un isthme ni une boucle, alors on peut définir, comme on l'a vu précédemment, la contraction et la suppression de l'élément e . Par suite on a une première décomposition des classes d'isomorphismes de matroïdes donné par $[M] < [M - e] + [M/e]$. On appelle cette décomposition **décomposition de Tutte**.

Dans ce cas les éléments irréductibles coïncident par construction avec les classes de matroïdes formés uniquement par des isthmes et des boucles.

Il existe une deuxième décomposition possible des classes d'isomorphismes de matroïdes donnée par la décomposition par somme directe. Soit $[M] = [M_1] \oplus [M_2]$, on considère la décomposition donnée par $[M] < [M_1] \times [M_2]$. Les éléments irréductibles correspondent alors aux matroïdes ne pouvant s'écrire sous forme de somme directe. On appelle ces éléments **éléments connectés**.

Notation 1.6.2

Lorsque nous utilisons plusieurs décompositions, nous noterons par $\sum_{i=0}^n a_i$ les ob-

jets de la catégorie D_2 et $\prod_{i=0}^n a_i$ les objets de la catégorie D_1 . Nous verrons par

la suite que cette notation n'est pas innocente. De même nous préciserons la décomposition utilisée pour parler des éléments irréductibles. Un élément sera dit D_1 -irréductible s'il est irréductible pour la décomposition D_1 . S'il est irréductible pour les décompositions D_1 et D_2 alors il sera dit D_1, D_2 -irréductible.

Définition 1.6.5

On dit qu'une décomposition est **finie** si pour tout $a \in A$, $s < I$ avec I un multiensemble formé d'éléments irréductibles.

Définition 1.6.6

On dit qu'une décomposition est **raffinable** si et seulement si

$$(f < g \text{ et } f < h \Rightarrow \exists j \text{ tel que } g < j \text{ et } h < j).$$

Ces éléments irréductibles sont les éléments maximaux pour la relation d'ordre donnée par $D(A)$:

Proposition 1.6.1

Un multiensemble est **indécomposable** si et seulement si il est composé d'éléments irréductibles.

PREUVE. On reformule la propriété 2) de la définition 1.6.3 avec la notation de relation d'ordre $<$:

$$f + g < h \text{ si et seulement si } \exists h_1, h_2, h = h_1 + h_2 \text{ et } f < h_1, g < h_2.$$

Supposons qu'on ait un multiensemble formé d'éléments irréductibles alors par la propriété précédente, en écrivant le multiensemble comme somme de ses éléments, pour tout élément irréductible i , il existe h_i tel que $i < h_i$ ce qui est impossible.

Réciproquement si un multiensemble n'est pas décomposable mais n'est pas composé que d'éléments irréductibles, c'est-à-dire qu'il existe un élément k décomposable alors on peut décomposer le multiensemble ce qui est une contradiction. ■

Si la décomposition est raffinable alors il existe une unique décomposition en éléments irréductibles. On appelle décomposition **unique** une décomposition finie et raffinable. Autrement dit les décompositions uniques sont celles où tout élément de A admet une et une seule décomposition en éléments irréductibles.

Définition 1.6.7

Soit N un sous-ensemble des entiers naturels. On appelle **décomposition entière** une décomposition sur un sous-ensemble N des entiers naturels et pour toute décomposition $n < \sum_i n_i$ alors $n_i <_{\mathbb{N}} n$.

Définition 1.6.8

Une décomposition D est dite **strictement finie** s'il existe un foncteur de la catégorie D dans une décomposition entière envoyant les éléments différents de l'identité sur des éléments différents de l'identité.

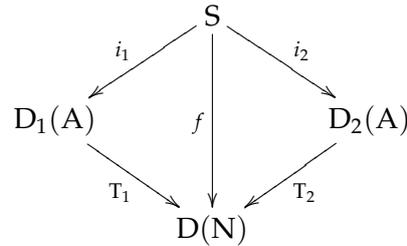
Il est clair que les décompositions uniques sont strictement finies. En effet on peut définir le foncteur tel que, pour tout $a \in A$, $T(a) = |I|$ avec I la décomposition de a en éléments irréductibles.

Nous voulons maintenant faire cohabiter deux décompositions de la meilleure manière possible, on définit donc les bidécompositions et les

bidécompositions distributives qui sont celles vérifiant de "bonnes" propriétés. C'est-à-dire qu'il faut pouvoir décomposer les éléments de S en éléments D_1, D_2 -irréductibles, et ce de manière unique.

Définition 1.6.9

Soit A un ensemble. On appelle bidécomposition tout couple de décompositions strictement finies $D_1(A)$ et $D_2(A)$ tel qu'il existe deux foncteurs T_1 et T_2 envoyant les deux décompositions dans la même décomposition entière $D(N)$ et tel que le diagramme suivant soit commutatif :



Définition 1.6.10

Une bidécomposition (D_1, D_2) est dite **distributive** si elle vérifie les propriétés :

1. D_1 et D_2 sont uniques.
2. Soit $s < \prod_{j=1}^n s_j \in D_1(S)$ avec s_j des éléments D_2 -irréductibles alors s est D_2 -irréductible.
3. Si $f < \prod_{i=1}^n f_i \in D_1(S)$ et pour un $k < n$, $f_k < \sum_{j=1}^m h_j \in D_2(S)$ alors il existe m multiensembles g_j tels que $s < \sum_{j=1}^m g_j \in D_2(S)$ et pour tout j on ait $g_j < \prod_{i=k} f_i \times h_j$.

La propriété 2) exprime simplement le fait que tout élément décomposable par D_1 en éléments D_2 -irréductibles est lui même D_2 -irréductible.

La propriété 3) exprime la distributivité de la décomposition D_1 sur la décomposition D_2 d'une manière similaire à la distributivité de l'addition sur la multiplication, ce qui justifie la terminologie et la notation utilisée pour les morphismes des deux catégories.

Ainsi ceci implique bien l'existence d'une unique décomposition en éléments D_1, D_2 -irréductibles.

La propriété suivante permet si l'on a deux décompositions qui vérifient les axiomes d'une bidécomposition distributive, de ne pas avoir à montrer que cela forme une bidécomposition dans un premier temps.

Proposition 1.6.2

Si D_1 et D_2 sont deux décompositions vérifiant les axiomes 1), 2) et 3) de la définition ci-dessus, alors (D_1, D_2) est une bidécomposition distributive.

PREUVE. On construit une fonction f faisant commuter le diagramme ci-dessus :

$$\forall s \in S, f(s) = \sum_{i=1}^n k_i$$

où pour tout i , $k_i = 2^{m_i}$ obtenu en considérant $s < \sum_{i=1}^n s_i$ la décomposition en éléments D_2 -irréductibles (elle existe car D_2 est unique) et $s_i < \prod_{j=1}^{m_i} s_{ij}$ la décomposition en éléments D_1 -irréductibles.

On vérifie que cette fonction induit bien une décomposition. ■

Ainsi si l'on revient aux matroïdes et si l'on considère D_1 la décomposition en somme directe et D_2 la décomposition de Tutte. Les deux décompositions décomposent un élément en élément de cardinalité inférieure. Par suite les décompositions sont uniques. De plus tout élément se décomposant en somme directe de boucles et d'isthmes est bien D_1 -irréductible, ce qui vérifie le deuxième axiome.

Soit $M = M_1 \oplus M_2$ un matroïde. La distributivité se montre en considérant la décomposition dans D_1 : $[M] < [M_1] \times [M_2]$, soit e un élément de M_1 qui ne soit ni une boucle ni un isthme alors on a la décomposition dans D_2 : $[M_1] < [M_1 - e] + [M_1/e]$. De plus on a les décompositions dans D_1 de $[M - e] < [M_1 - e] \times [M_2]$ et $[M/e] < [M_1/e] \times [M_2]$. Par construction de la somme directe, on en déduit la décomposition dans D_1 :

$$[M] < [M_1 - e] \times M_2 + [M_1/e] \times M_2$$

ce qui prouve la distributivité de D_1 sur D_2 .

On a bien une bidécomposition distributive. On l'appelle **bidécomposition de Tutte**.

Nous avons vu précédemment que les éléments irréductibles sont les matroïdes formés de boucles et d'isthmes. Comme une boucle ou un isthme dans un tel matroïde (non réduit à un élément car les multiensembles doivent être non vides par hypothèse) permet d'écrire ce matroïde sous forme d'une somme directe, alors les éléments irréductibles et indécomposables sont le matroïde L et le matroïde C que nous avons vu précédemment.

On s'intéresse maintenant aux fonctions se comportant "bien" pour une décomposition.

Définition 1.6.11

On appelle un invariant de décomposition associé à la décomposition D (ou D -invariant), une fonction $f : S \rightarrow A$ à valeur dans un groupe abélien tel que pour toute décomposition d'un élément $s \in S$: $s < \sum_{i=1}^n s_i$, on ait la relation :

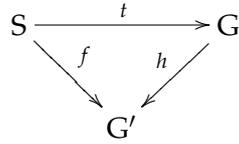
$$f(s) = \sum_{i=1}^n f(s_i).$$

Le théorème suivant donne la propriété universelle que vérifient les D -invariant :

Théorème 1.6.1

Soit $D(S)$ une décomposition unique, alors il existe un groupe abélien G appelé

groupe de Tutte-Grothendieck et un D-invariant t tel que tout homomorphisme de groupe engendre un unique D-invariant par composition avec t et tel que le diagramme :



soit commutatif pour tout D-invariant f à valeur dans un groupe abélien G' . De plus G est isomorphe au groupe libre avec pour générateurs les éléments irréductibles de $D(S)$.

Nous démontrons ce théorème dans le cas de l'extension au cas des bidécompositions.

On généralise d'abord la notion de D-invariants au cas des bidécompositions :

Définition 1.6.12

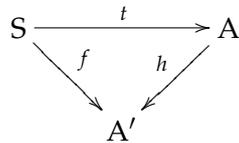
Un invariant de bidécomposition est une fonction $f : S \rightarrow R$ avec R un anneau commutatif tel que pour toute décomposition dans D_1 d'un élément $s \in S$: $s < \prod_{i=1}^n s_i$ on ait $f(s) = \prod_{i=1}^n f(s_i)$ et pour toute décomposition dans D_2 : $s < \sum_{i=1}^n s_i$, on ait $f(s) = \sum_{i=1}^n f(s_i)$.

Tout invariant associé à la bidécomposition de Tutte sera appelé **invariant de Tutte-Grothendieck**.

De la même manière on a la propriété universelle pour une bidécomposition :

Théorème 1.6.2

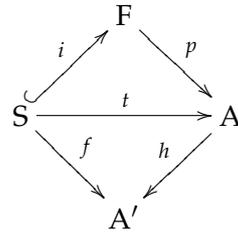
Soit $B(S)$ une bidécomposition distributive alors il existe un anneau commutatif A appelé anneau de Tutte-Grothendieck et un invariant t tel que tout homomorphisme d'anneau engendre un unique D-invariant par composition avec t et tel que le diagramme :



soit commutatif pour tout D-invariant f à valeur dans un anneau A' . De plus A est isomorphe à l'anneau commutatif libre engendré par les éléments irréductibles pour les deux décompositions D_1 et D_2 (i.e. l'anneau des polynômes à coefficients entiers dont les indéterminés sont donnés par les éléments irréductibles).

PREUVE. Soit F l'anneau commutatif libre ayant pour générateurs l'ensemble S . On considère I l'idéal de F engendré par les éléments de la forme $s - \prod_i s_i$ pour toute décomposition $s < \prod_i s_i$ et par les éléments $s - \sum_j s_j$ pour toute décomposition $s < \sum_j s_j$.

On note alors $R = F/I$ l'anneau quotient. On a les diagrammes commutatifs suivants :



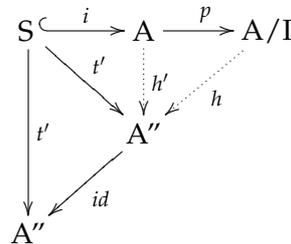
où i est l'injection canonique et p la surjection canonique qui à un élément de P associe sa classe d'équivalence dans F/I .

On a, pour tout homomorphisme d'anneau h , que $h \circ t$ est un B -invariant. En effet, si l'on utilise (par exemple) la décomposition D_2 , soit $s = \sum_i s_i$. Alors $s - \sum_i s_i$ est dans le noyau de p , c'est à dire que $p(s - \sum_i s_i) = 0$ donc $p(s) = \sum_i p(s_i)$. Par suite on a $t(s) = \sum_i t(s_i)$ puis que

$$h \circ t(s) = \sum_i h \circ t(s_i).$$

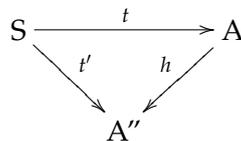
Nous allons maintenant montrer que (A, t) est universel dans l'ensemble des objets vérifiant cette propriété.

Pour tout couple (A', t') tel que pour tout homomorphisme h , $h \circ t$ est un B -invariant, on a le diagramme



On peut construire h' de manière à avoir $h' \circ i = t'$ en posant $h'(s) = t'(s)$. Comme les générateurs de A sont les éléments de S , on a bien défini h' sur tout A et c'est un homomorphisme d'anneaux. Par hypothèse, on a montré que tout homomorphisme d'anneau h composé avec t' est un B -invariant. Or comme l'identité est un homomorphisme d'anneau, alors t' est aussi un B -invariant. Par définition, cela signifie que tous les éléments de I sont contenus dans le noyau de h' donc on peut étendre l'homomorphisme h' à un homomorphisme $h : A/I \rightarrow A''$.

Donc (A, t) vérifie la propriété universelle et pour tout couple (A'', t') avec cette propriété, il existe $h : A \rightarrow A''$ tel que le diagramme suivant soit commutatif :



Ce qui montre le premier point.

Soit A'' l'anneau libre commutatif engendré par les éléments irréductibles pour D_1 et D_2 . Soit $s \in S$ et soit la décomposition $s < \sum_{j=1}^n \prod_{i=1}^n s_{ij}$ où les s_{ij} sont des irréductibles pour D_1 et D_2 . On pose $t'(s) = \sum_{j=1}^n \prod_{i=1}^n s_{ij} \in A''$.

Nous voulons montrer que t' est un B-invariant :

Soit $s < \sum_{j=1}^m s_j$ un morphisme de D_2 . Alors en décomposant complètement les s_i et en composant les morphismes, on a

$$t(s') = \sum_{j=1}^m \sum_{k=1}^{n_j} s_{jk} = \sum_{j=1}^m t'(s_j).$$

Maintenant soit $s < \prod_{j=1}^m s_j$ un morphisme de D_1 . Soit pour tout k , on pose

$s_k < \sum_{i_k=1}^{n_k} s_{k i_k}$ la décomposition des s_k en D_2 -irréductibles. De même soit $s_{k i_k} < \prod_{j=1}^{n_{i_k}} s_{k i_k j}$ la décomposition des $s_{k i_k}$ en éléments D_1 -irréductibles. On a enfin notre décomposition en éléments D_1, D_2 -irréductibles et de plus :

$$\prod_{k=1}^m t'(s_k) = \prod_{k=1}^m \sum_{i_k=1}^{n_k} \prod_{j=1}^{n_{i_k}} t'(s_{k i_k j}) \in A''.$$

En appliquant la distributivité dans A'' , on en déduit :

$$\prod_{k=1}^m t'(s_k) = \sum_{i_1=1}^{n_1} \dots \sum_{i_n=1}^{n_n} \prod_{k=1}^n \prod_{j=1}^{n_{i_k}} t'(s_{k i_k j}) \in A''.$$

Or en appliquant la distributivité sur les décompositions, on obtient aussi :

$$s < \sum_{i_1=1}^{n_1} \dots \sum_{i_n=1}^{n_n} \prod_{k=1}^n \prod_{j=1}^{n_{i_k}} s_{k i_k j}$$

la décomposition en éléments D_1, D_2 -irréductibles. Par unicité de cette décomposition, on en déduit

$$t'(s) = \prod_{i=1}^n t'(s_i).$$

Donc t' est un B-invariant et comme (A, t) est un élément universel, on peut trouver un homomorphisme h tel que $h \circ t = t'$. Or comme pour tout élément D_2 -irréductible, on a $t'(i) = i$ donc $h \circ t(i) = i$ et comme A'' est libre, il ne peut y avoir de relation non-triviale entre les classes des éléments irréductibles dans A . De plus F est engendré par S et pour tout élément $s \in S$, $p(s) \in F/I$ peut s'écrire en utilisant uniquement des éléments D_1, D_2 -irréductibles. Par suite $A \simeq A''$.

■

On appelle **invariant de Tutte-Grothendieck** tout invariant pour la décomposition de Tutte. Dans le cas des classes d'isomorphismes de matroïdes on peut définir explicitement l'anneau de Tutte-Grothendieck et l'invariant universel.

Théorème 1.6.3

Il existe une unique fonction $T : \mathcal{M} \rightarrow \mathbb{Z}[x, y]$ telle que :

$$T(C, x, y) = x,$$

$$T(L, x, y) = y,$$

$$T(M, x, y) = T(M - e, x, y) + T(M/e, x, y)$$

si e n'est ni une boucle ni un isthme et

$$T(M_1 \oplus M_2, x, y) = T(M_1, x, y)T(M_2, x, y).$$

De plus tout autre invariant de Tutte-Grothendieck f est une évaluation de cette fonction :

$$f(M) = T(f(C), f(L)).$$

PREUVE. La preuve est immédiate par construction. En effet l'anneau de Tutte-Grothendieck est isomorphe à l'anneau libre commutatif à deux générateurs par le théorème précédent donc à $\mathbb{Z}[x, y]$. On en déduit que :

$$T(C, x, y) = x,$$

$$T(L, x, y) = y,$$

De plus la fonction T est un invariant pour la bidécomposition de Tutte, c'est à dire :

$$T(M, x, y) = T(M - e, x, y) + T(M/e, x, y)$$

si e n'est ni une boucle ni un isthme et

$$T(M_1 \oplus M_2, x, y) = T(M_1, x, y)T(M_2, x, y).$$

La démonstration de l'universalité de cette fonction est identique à celle faite ci-dessous pour les invariants de Tutte-Grothendieck généralisés. On montre que l'on a bien la correspondance sur les classes de matroïdes $[C]$ et $[L]$ ce qui est trivialement vrai puis par induction on montre que l'universalité est conservée pour la bidécomposition.

Cette fonction est appelée **polynôme de Tutte**. On notera que \mathcal{M} désigne ici les classes d'isomorphismes de matroïdes ce qui n'est pas très pratique. On peut donc ajouter une condition supplémentaire qui définit cette fonction comme un invariant sur les matroïdes, c'est-à-dire :

$$M \simeq N \Rightarrow T(M, x, y) = T(N, x, y).$$

Néanmoins cette classe d'invariants est assez réduite et généralement les fonctions que nous rencontrerons vérifient au niveau de la décomposition par mineur, une relation de la forme :

$$f(M) = af(M - e) + bf(M/e)$$

avec a et b des entiers.

Nous définissons donc une autre classe d'invariants qui étendent les invariants de Tutte-Grothendieck et que nous appellerons invariants de Tutte-Grothendieck généralisés. On en déduit un théorème similaire pour ces invariants :

Théorème 1.6.4

Il existe une unique fonction $\bar{T}_M : \mathcal{M} \rightarrow \mathbb{Z}[x, y, a, b]$ telle que :

$$\bar{T}(C, x, y) = x,$$

$$\bar{T}(L, x, y) = y,$$

$$\bar{T}(M, x, y) = a\bar{T}(M - e, x, y) + b\bar{T}(M/e, x, y)$$

si e n'est ni une boucle ni un isthme et

$$\bar{T}(M_1 \oplus M_2, x, y) = \bar{T}(M_1, x, y)\bar{T}(M_2, x, y).$$

De plus tout autre invariant de Tutte-Grothendieck généralisé f est une évaluation de cette fonction :

$$f(M) = a^{|\mathbb{E}|-r(\mathbb{E})}b^{r(\mathbb{E})}\bar{T}(M, \frac{f(C)}{b}, \frac{f(L)}{a}).$$

PREUVE. L'existence d'une telle fonction est assurée par le théorème de Brylawski. L'unicité provient du fait que $\bar{T}(M, x, y)$ est uniquement déterminé par $\bar{T}(M - e, x, y)$ et $\bar{T}(M/e, x, y)$ et nous avons vu que les opérations de contractions-suppressions sont commutatives.

Maintenant si nous avons un invariant de Tutte-Grothendieck généralisé f , on montre par induction f peut s'obtenir comme une évaluation de cette fonction :

On remarque que si l'on considère le matroïde L ,

$$a^{|\mathbb{E}|-r(\mathbb{E})}b^{r(\mathbb{E})}\bar{T}(L, \frac{f(C)}{b}, \frac{f(L)}{a}) = a^1 \frac{f(L)}{a} = f(L).$$

De même si l'on considère le matroïde C ,

$$a^{|\mathbb{E}|-r(\mathbb{E})}b^{r(\mathbb{E})}\bar{T}(C, \frac{f(C)}{b}, \frac{f(L)}{a}) = b^1 \frac{f(C)}{b} = f(C).$$

Ainsi les fonctions correspondent sur les boucles et isthmes.

Soit maintenant e qui ne soit ni une boucle ni un isthme, on suppose que :

$$f(M - e) = a^{|\mathbb{E}'|-r(\mathbb{E}')}b^{r(\mathbb{E}')} \bar{T}(M - e, \frac{f(C)}{b}, \frac{f(L)}{a})$$

$$f(M/e) = a^{|\mathbb{E}''|-r(\mathbb{E}'')}b^{r(\mathbb{E}'')} \bar{T}(M/e, \frac{f(C)}{b}, \frac{f(L)}{a})$$

or comme $r(\mathbf{M} - e) = r(\mathbf{M}) = r(\mathbf{E}')$ et $r(\mathbf{M}/e) = r(\mathbf{M}) - 1 = r(\mathbf{E}'')$,

$$\begin{aligned}
af(\mathbf{M} - e) + bf(\mathbf{M}/e) &= a \cdot a^{|\mathbf{E}|-1-r(\mathbf{E})} b^{r(\mathbf{E})} \bar{\mathbf{T}}(\mathbf{M} - e, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&\quad + b \cdot a^{|\mathbf{E}|-1-(r(\mathbf{E})-1)} b^{r(\mathbf{E})-1} \bar{\mathbf{T}}(\mathbf{M}/e, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&= a^{|\mathbf{E}|-r(\mathbf{E})} b^{r(\mathbf{E})} \bar{\mathbf{T}}(\mathbf{M} - e, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&\quad + a^{|\mathbf{E}|-r(\mathbf{E})} b^{r(\mathbf{E})} \bar{\mathbf{T}}(\mathbf{M}/e, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&= a^{|\mathbf{E}|-r(\mathbf{E})} b^{r(\mathbf{E})} \bar{\mathbf{T}}(\mathbf{M}, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&= f(\mathbf{M})
\end{aligned}$$

De même, si $\mathbf{M} = \mathbf{M}_1 \oplus \mathbf{M}_2$ alors $|\mathbf{M}| = |\mathbf{M}_1| + |\mathbf{M}_2|$ et $r(\mathbf{M}) = r(\mathbf{M}_1) + r(\mathbf{M}_2)$,

$$\begin{aligned}
f(\mathbf{M}_1)f(\mathbf{M}_2) &= a^{|\mathbf{M}_1|-r(\mathbf{M}_1)} b^{r(\mathbf{M}_1)} \bar{\mathbf{T}}(\mathbf{M}_1, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \cdot a^{|\mathbf{M}_2|-r(\mathbf{M}_2)} b^{r(\mathbf{M}_2)} \bar{\mathbf{T}}(\mathbf{M}_2, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&= a^{|\mathbf{M}_1|+|\mathbf{M}_2|-r(\mathbf{M}_1)-r(\mathbf{M}_2)} b^{r(\mathbf{M}_1)+r(\mathbf{M}_2)} \bar{\mathbf{T}}(\mathbf{M}_1, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \bar{\mathbf{T}}(\mathbf{M}_2, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&= a^{|\mathbf{M}|-r(\mathbf{M})} b^{r(\mathbf{M})} \bar{\mathbf{T}}(\mathbf{M}_1 \oplus \mathbf{M}_2, \frac{f(\mathbf{C})}{b}, \frac{f(\mathbf{L})}{a}) \\
&= f(\mathbf{M})
\end{aligned}$$

On a donc montré l'universalité de la fonction $\bar{\mathbf{T}}$. ■

De manière pratique, nous parlerons d'invariants de Tutte-Grothendieck même s'il s'agit en fait d'invariants de Tutte-Grothendieck généralisés.

APPLICATIONS DU POLYNÔME DE TUTTE

Nous commençons ici, le cœur du sujet, qui est l'étude de certaines propriétés combinatoires encodées par le polynôme de Tutte. Nous avons vu dans le chapitre les théorèmes d'universalité qui seront un outil fondamental par la suite. Les sujets touchant au polynôme de Tutte sont très variés et certains sujets peuvent être reliés entre eux plus ou moins directement. C'est pourquoi nous n'avons pas traité les sections suivantes dans un ordre linéaire.

2.1 POLYNÔME DE TUTTE D'UN MATROÏDE

Nous commençons par quelques propriétés générales sur les matroïdes et de leur interprétation combinatoire.

2.1.1 Généralités

Dans le chapitre précédent, nous avons vu la propriété universelle que vérifiaient les invariants de matroïdes ainsi que la définition des invariants de Tutte-Grothendieck. Dans le cas des classes d'isomorphismes de matroïdes, nous avons aussi vu que l'invariant de Tutte-Grothendieck coïncidait avec le polynôme de Tutte. Nous reprenons ici les différentes définitions du polynôme de Tutte et commençons à étudier ses différentes propriétés.

Nous avons vu dans le chapitre précédent que la définition du polynôme de Tutte comme un morphisme respectant la décomposition de Tutte mais nous pouvons aussi le voir d'une manière différente via la fonction de rang d'un matroïde :

Proposition 2.1.1

Le polynôme de Tutte peut s'exprimer grâce à la fonction de rang d'un matroïde :

$$T(\mathcal{M}, x, y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{|A|-r(A)}$$

Pour cela on va montrer que la fonction définie comme ci-dessus est un invariant de Tutte-Grothendieck (non généralisé dans ce cas).

PREUVE. On note $t(G, x, y)$ la fonction définie comme ci-dessus.

On commence déjà par remarquer que la fonction $t(G, x, y)$ est entièrement définie par la fonction de rang donc c'est un invariant de matroïdes.

On déduit le reste des propriétés du rang et en particulier :

$$r(\mathcal{M}_1 \oplus \mathcal{M}_2) = r(\mathcal{M}_1) + r(\mathcal{M}_2)$$

que :

$$t(\mathcal{M}_1 \oplus \mathcal{M}_2, x, y) = t(\mathcal{M}_1, x, y)t(\mathcal{M}_2, x, y).$$

De plus

$$r(\mathcal{M} - e) = r(\mathcal{M}) \text{ et } r(\mathcal{M}/e) = r(\mathcal{M}) - 1$$

pour e n'étant ni une boucle ni un isthme, d'où l'on déduit :

$$\begin{aligned} t(\mathcal{M}, x, y) &= \sum_{A \subseteq E - \{e\}} (x-1)^{r(E) - r(A \cup \{e\})} (y-1)^{|A \cup \{e\}| - r(A \cup \{e\})} \\ &+ \sum_{A \subseteq E - \{e\}} (x-1)^{r(E) - r(A)} (y-1)^{|A| - r(A)} \\ &= t(\mathcal{M}/e, x, y) + t(\mathcal{M} - e, x, y) \end{aligned}$$

Ainsi la fonction t est un invariant de Tutte-Grothendieck et

$$t(\mathcal{M}, x, y) = T(\mathcal{M}, t(\mathcal{C}, x, y), t(\mathcal{L}, x, y))$$

or $t(\mathcal{C}, x, y) = x$ et $t(\mathcal{L}, x, y) = y$ donc

$$t(\mathcal{M}, x, y) = T(\mathcal{M}, x, y)$$

On remarque maintenant, via la définition récursive du polynôme de Tutte, que les coefficients du polynôme de Tutte sont tous positifs. Nous donnons maintenant une interprétation combinatoire des coefficients du polynôme de Tutte.

Soit $M = (E, \mathcal{B})$ un matroïde avec \mathcal{B} l'ensemble de ses bases. On ordonne arbitrairement les éléments de E et on considère les bases du matroïde.

Définition 2.1.1

Soit $B \in \mathcal{B}$ et $e \notin B$. On dit que e est extérieurement actif s'il est le plus petit élément du circuit $B \cup \{e\}$.

On note $E(B)$ l'ensemble des éléments extérieurement actifs de la base B et $j(B)$ son cardinal.

Définition 2.1.2

Soit $B \in \mathcal{B}$ et $i \in B$. On dit que i est intérieurement actif s'il est le plus petit élément du circuit $B^* \cup \{e\}$ de \mathcal{M}^* avec B^* la base de \mathcal{M}^* obtenu en prenant le complémentaire de la base B .

On note $I(B)$ l'ensemble des éléments intérieurement actifs de la base B et $i(B)$ son cardinal.

Exemple : Si l'on considère le graphe de la figure 1.4 avec les arcs ordonnés par leurs numéros, le tableau suivant récapitule les éléments extérieurement actifs et intérieurement actifs :

B	12	13	23	24	34
E(B)	-	-	1	1	12
I(B)	12	1	-	2	-
B*	34	24	14	13	12

Le théorème suivant qui donne l'interprétation du polynôme de Tutte en termes d'activité interne et externe :

Théorème 2.1.1

$$T(\mathcal{M}, x, y) = \sum_{B \in \mathcal{B}} x^{i(B)} y^{j(B)}.$$

Le coefficient du monôme $x^i y^e$ correspond au nombre de base d'activité interne i et d'activité externe e . On donne l'idée de la preuve. Pour plus de détails, nous nous référerons à (Cra69).

PREUVE. Tout sous-ensemble A de E peut s'écrire sous la forme $A = B - I \cup E$ où B est une base, $I \subseteq I(B)$, $E \subseteq E(B)$. (On peut par exemple montrer que les intervalles du type $[B - I(B), B \cup E(B)]$ où B est une base forment une partition du treillis des sous-ensembles de E pour l'inclusion.)

Ensuite, on a $A = B - I \cup E$ donc $r(A) = r(\mathcal{M}) - i(B)$ et donc

$$\begin{aligned} T(\mathcal{M}, x, y) &= \sum_{A \subseteq E} (x-1)^{r(\mathcal{M})-r(A)} (y-1)^{|S|-r(A)} \\ &= \sum_{A=B-I+E} (x-1)^{r(\mathcal{M})-r(\mathcal{M})+|I|} (y-1)^{|S|-r(\mathcal{M})+|I|} \\ &= \sum_{A=B-I+E} (x-1)^{|I|} (y-1)^{|E|} \\ &= \sum_{B \in \mathcal{B}} \left(\sum_{I \subseteq I(B)} (x-1)^{|I|} \right) \left(\sum_{E \subseteq E(B)} (y-1)^{|E|} \right) \\ &= \sum_{B \in \mathcal{B}} \left(\sum_{k=0}^{i(B)} \binom{i(B)}{k} (x-1)^k \right) \left(\sum_{k=0}^{j(B)} \binom{j(B)}{k} (y-1)^k \right) \\ &= \sum_{B \in \mathcal{B}} (1 + (x-1)^{i(B)}) (1 + (y-1)^{j(B)}) \\ &= \sum_{B \in \mathcal{B}} x^{i(B)} y^{j(B)} \end{aligned}$$

■

La notion de dualité pour le polynôme de Tutte s'exprime très simplement :

Proposition 2.1.2

Soit \mathcal{M} un matroïde alors

$$T(\mathcal{M}, x, y) = T(\mathcal{M}^*, y, x)$$

PREUVE. La preuve est assez directe, on a

$$T(\mathcal{M}^*, x, y) = \sum_{A \subseteq E} (x-1)^{r(\mathcal{M}^*)-r^*(A)} (y-1)^{|A|-r^*(A)}$$

Or on a les relations :

$$r^*(A) = |A| - r(\mathcal{M}) + r(E - A),$$

donc

$$|A| - r^*(A) = r(\mathcal{M}) - r(E - A),$$

$$r(\mathcal{M}^*) - r^*(A) = |E| - r(\mathcal{M}) - r^*(A) = |E| - |A| - r(E - A).$$

On en déduit

$$T(\mathcal{M}^*, x, y) = \sum_{A \subseteq E} (x-1)^{|E-A|-r(E-A)} (y-1)^{r(E)-r(E-A)} = T(\mathcal{M}, y, x)$$

■

Une autre forme sous laquelle nous pouvons trouver le polynôme de Tutte est sa forme récursive :

Définition 2.1.3

On définit le polynôme de Tutte d'un matroïde \mathcal{M} comme le polynôme à deux variables vérifiant :

1. Si $|E(\mathcal{M})| = 0$, $T(\mathcal{M}, x, y) = 1$,
2. $T(\mathcal{M}, x, y) = T(\mathcal{M} - e, x, y) + T(\mathcal{M}/e, x, y)$ si e n'est ni une boucle ni un isthme,
3. $T(\mathcal{M}, x, y) = xT(\mathcal{M}/e, x, y)$ si e est un isthme
4. $T(\mathcal{M}, x, y) = yT(\mathcal{M} - e, x, y)$ si e est une boucle.

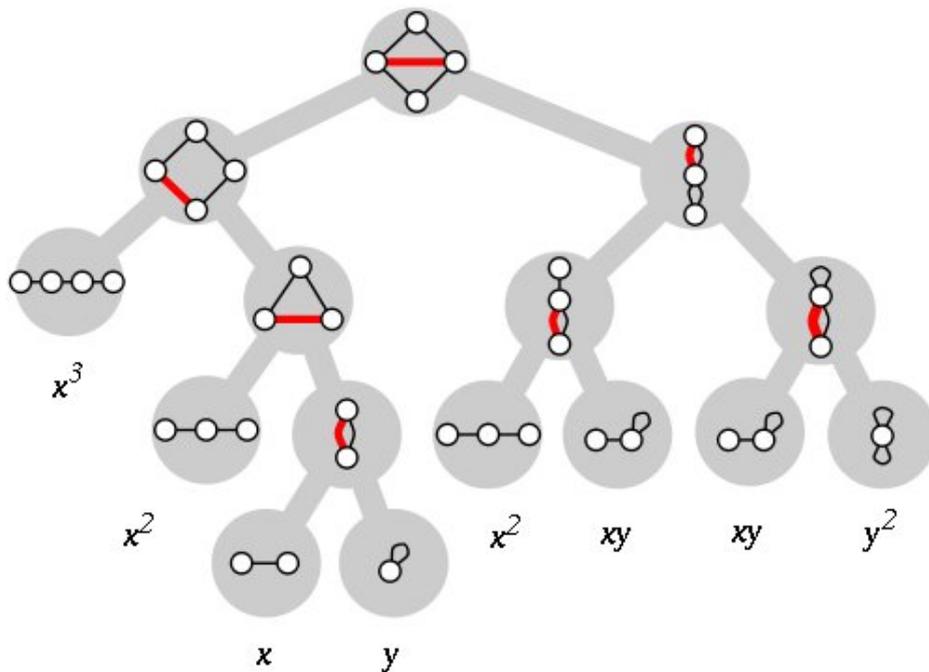


FIG. 2.1 – Calcul récursif du polynôme de Tutte

Nous ne l'utiliserons généralement pas pour faire les démonstrations (sauf dans certains cas particuliers). La démonstration de l'équivalence

se fait assez rapidement en montrant que c'est un invariant de Tutte-Grothendieck. On voit en effet que la fonction est bien un invariant pour la décomposition de Tutte et qu'elle est bien définie sur les éléments irréductibles de la décomposition en somme directe.

Cette définition est par contre très utile pour calculer explicitement le polynôme de Tutte. Par exemple le polynôme de Tutte du graphe de la figure 2.2 est donné par la figure 2.1.

2.1.2 Nombre d'éléments du matroïde

Proposition 2.1.3

Soit \mathcal{M} un matroïde et $T(x, y)$ son polynôme de Tutte, alors $T(\mathcal{M}, 2, 2)$ compte $2^{|\mathcal{M}|}$ avec $|\mathcal{M}|$ le nombre d'éléments de \mathcal{M} .

PREUVE. Soit e un élément qui ne soit ni une boucle ni un isthme alors

$$\begin{aligned} 2^{|\mathcal{M}-e|} + 2^{|\mathcal{M}/e|} &= 2^{|\mathcal{M}|-1} + 2^{|\mathcal{M}|-1} \\ &= 2^{|\mathcal{M}|} \end{aligned}$$

De même on a clairement que

$$2^{|\mathcal{M}_1 \oplus \mathcal{M}_2|} = 2^{|\mathcal{M}_1|} \cdot 2^{|\mathcal{M}_2|}.$$

Donc c'est un invariant de Tutte-Grothendieck et $2^{|\mathcal{C}|} = 2^{|\mathcal{L}|} = 2$ donc on en déduit que :

$$T(\mathcal{M}, 2, 2) = 2^{|\mathcal{M}|}.$$

■

On peut donc trouver le nombre d'éléments du matroïde en utilisant le polynôme de Tutte :

$$|\mathcal{M}| = \log_2(T(\mathcal{M}, 2, 2)).$$

2.1.3 Nombres de bases

Proposition 2.1.4

$T(\mathcal{M}, 1, 1)$ compte le nombre de bases du matroïde.

PREUVE. Nous avons, par définition,

$$T(\mathcal{M}, x, y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{|A|-r(A)}$$

avec r la fonction de rang associée au matroïde.

On en déduit que

$$T(\mathcal{M}, 1, 1) = \sum_{A \subseteq E} 0^{r(E)-r(A)} 0^{|A|-r(A)}$$

or $0^{r(E)-r(A)} 0^{|A|-r(A)}$ vaut 1 si $r(E) - r(A) = 0$ et $|A| - r(A) = 0$ et 0 sinon. On a donc que $T(\mathcal{M}, 1, 1)$ correspond au nombre de sous-ensemble

de E vérifiant les conditions $|A| = r(A)$, c'est-à-dire que l'ensemble A est un indépendant, et $r(E) = r(A)$, c'est-à-dire que E est un indépendant maximal. Par définition, c'est une base de \mathcal{M} . ■

Remarque 2.1.1

Nous avons vu dans le chapitre précédent que les bases d'un matroïde graphique sont les arbres couvrants. Si G est un graphe connexe alors $T(G, 1, 1)$ compte le nombre d'arbres couvrants. Si G n'est pas connexe, $T(G, 1, 1)$ compte le nombre de forêts maximales couvrantes.

En théorie algébrique des graphes, nous disposons d'une autre méthode pour calculer le nombre d'arbres couvrants utilisant la matrice laplacienne d'un graphe :

Définition 2.1.4

Soit G un graphe connexe non orienté. On appelle matrice laplacienne de G la matrice $L = (l_{ij})_{ij}$ définie par :

$$l_{ij} = \begin{cases} \deg(v_i) & \text{si } i = j \\ -1 & \text{si } i \neq j \text{ et si les sommets } v_i \text{ et } v_j \text{ sont adjacents} \\ 0 & \text{sinon} \end{cases}$$

On remarque que cette matrice peut s'écrire comme la différence de la matrice diagonale des degrés et de la matrice d'adjacence.

Nous pouvons maintenant énoncer le théorème de Kirshhoff :

Théorème 2.1.2

Soit G un graphe connexe étiqueté à n sommets et soit L la matrice laplacienne de G et $\lambda_1, \dots, \lambda_{n-1}$ les valeurs propres positives de L . Alors le nombre d'arbres couvrants de G est donné par

$$t(G) = \frac{1}{n} \lambda_1 \lambda_2 \dots \lambda_{n-1}.$$

La démonstration est assez longue donc nous ne l'incluons pas ici. Nous renvoyons à (C.G) pour plus de détails à ce sujet. Le point important que cela apporte est que l'évaluation du polynôme de Tutte au point $(1, 1)$ revient au calcul d'un déterminant, ce qui fait du point $(1, 1)$ l'un des quelques points du plan où l'évaluation du polynôme de Tutte se fait en temps polynomial.

2.1.4 Nombre d'indépendants

Une autre propriété du polynôme de Tutte est que :

Proposition 2.1.5

$T(\mathcal{M}, 2, 1)$ compte le nombre d'indépendants d'un matroïde.

PREUVE. La démonstration est similaire à la précédente :

$$T(\mathcal{M}, 2, 1) = \sum_{A \subseteq E} 1^{r(E)-r(A)} 0^{|A|-r(A)}$$

or $1^{r(E)-r(A)} 0^{|A|-r(A)}$ vaut 1 seulement si $|A| - r(A) = 0$, c'est-à-dire que l'ensemble A est un indépendant. Donc $T(\mathcal{M}, 2, 1)$ compte bien le nombre d'indépendants d'un matroïde. ■

Remarque 2.1.2

Si G est un graphe alors $T(G, 2, 1)$ compte le nombre de forêts du graphe.

On introduit ici l'interprétation duale :

Proposition 2.1.6

$T(\mathcal{M}, 1, 2)$ compte le nombre de sous-ensembles de E de rang maximal.

PREUVE. Encore une fois

$$T(\mathcal{M}, 1, 2) = \sum_{A \subseteq E} 0^{r(E)-r(A)} 1^{|A|-r(A)}$$

et $0^{r(E)-r(A)} 1^{|A|-r(A)}$ vaut 1 si $r(E) = r(A)$, c'est-à-dire que A est de rang maximal, et 0 sinon. Donc $T(\mathcal{M}, 1, 2)$ compte bien le nombre de sous-ensembles de E de rang maximal. ■

En terme de graphe $T(\mathcal{M}, 1, 2)$ compte le nombre de sous-graphes couvrants pour un graphe connexe.

2.1.5 Polynôme des indépendants

Nous venons juste de voir que l'on pouvait compter le nombre d'indépendants d'un matroïde. Nous nous intéressons maintenant aux indépendants de taille fixée et plus particulièrement au polynôme suivant.

Définition 2.1.5

On appelle *polynôme des indépendants* la série génératrice

$$F(\mathcal{M}, s) = \sum_{i=0}^{|E|-1} f_i s^i,$$

où f_i correspond au nombre d'indépendants de taille i .

Nous allons montrer qu'il existe une interprétation du polynôme de Tutte généralisant l'interprétation précédente.

Proposition 2.1.7

Le polynôme des indépendants $F(\mathcal{M}, s)$ est lié au polynôme de Tutte via la relation

$$F(\mathcal{M}, s) = s^{r(\mathcal{M})} T(\mathcal{M}, \frac{1}{s} + 1, 1).$$

PREUVE. On pourrait le montrer en utilisant les relations de Tutte-Grothendieck et en trouvant des relations entre les coefficients du polynôme (il faudrait dans ce cas partitionner les forêts de taille i en celles qui contiennent un arc e et celles qui ne le contiennent pas puis trouver des bijections entre ces forêts et les forêts de taille $i, i - 1$ de $G - e$ ou G/e)

Néanmoins nous allons encore une fois utiliser une méthode plus directe :

$$\begin{aligned}
T\left(\frac{1}{s} + 1, 1\right) &= \sum_{A \subseteq E} \left(\frac{1}{s} + 1 - 1\right)^{r(E)-r(A)} (1 - 1)^{|A|-r(A)} \\
&= \sum_{A \text{ forêt}} \left(\frac{1}{s}\right)^{r(E)-|A|} \\
&= \sum_{A \text{ forêt}} s^{|A|-r(E)} \\
&= \left(\frac{1}{s}\right)^{r(E)} \sum_{A \text{ forêt}} s^{|A|} \\
&= \left(\frac{1}{s}\right)^{r(E)} F(G, s)
\end{aligned}$$

Ce qui conclut la preuve. ■

De plus nous pouvons donner l'interprétation duale (nous l'avons déjà vu, il s'agit des sous-ensembles de rang maximal) :

Proposition 2.1.8

La série génératrice des sous-ensembles de rang maximal est liée au polynôme de Tutte via la relation :

$$\sum_{k=0}^{|\mathcal{E}|-|V|+1} c_k s^k = T(\mathcal{M}, 1, \frac{1}{s} + 1)$$

où c_k compte le nombre de sous-ensembles de E de rang maximal et de taille k .

PREUVE. Immédiate par ce qui précède en utilisant la dualité. ■

2.2 POLYNÔME DE TUTTE D'UN MATROÏDE GRAPHIQUE

Intéressons nous maintenant aux matroïdes graphiques. Les graphes seront supposés, sauf mention du contraire, non-orientés.

2.2.1 Polynôme chromatique

Nous montrons ici la relation entre le polynôme chromatique d'un graphe et son polynôme de Tutte. Nous rappelons ici la définition d'une coloration d'un graphe :

Définition 2.2.1

Soit $G = (V, E)$ un graphe. Une λ -coloration est une fonction $\phi : V \rightarrow [\lambda] = \{1, \dots, \lambda\}$.

Définition 2.2.2

Une λ -coloration ϕ est dite propre si $\forall (v_i, v_j) \in E, \phi(v_i) \neq \phi(v_j)$.

La figure 2.2 donne un exemple d'une telle coloration.

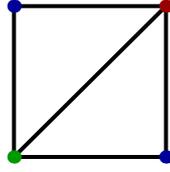


FIG. 2.2 – Une 3-coloration propre d'un graphe

Nous considérons maintenant le nombre de λ -colorations propres possibles que nous notons $\chi_G(\lambda)$. Nous verrons que la fonction $\chi(G; \lambda)$ est une fonction polynomiale en λ .

Théorème 2.2.1

Si $G = (V, E)$ est un graphe, alors

$$\chi(G; \lambda) = \sum_{A \subseteq E} (-1)^{|A|} \lambda^{\kappa(A)}$$

avec $\kappa(A)$ le nombre de composantes connexes du sous-graphe engendré par A .

PREUVE. On considère P_{ij} l'ensemble des λ -colorations telles que les sommets i et j reçoivent la même couleur et \bar{P}_{ij} l'ensemble des colorations telles que i et j ont des couleurs différentes. On a ainsi

$$\begin{aligned} \chi(G, \lambda) &= \left| \bigcap_{i,j \in E} \bar{P}_{ij} \right| \\ &= \lambda^n - \sum_{i,j \in E} |P_{ij}| + \sum_{\substack{i,j,k,l \in E \\ i,j \neq k,l}} |P_{ij} \cap P_{kl}| \\ &\quad - \dots + (-1)^{|E|} \left| \bigcap_{i,j \in E} P_{ij} \right| \end{aligned}$$

Tous les termes de cette somme sont de la forme $|\sum_{A \subseteq E} P_{ij}|$ où A est l'ensemble des couples d'indices ij parcourus dans chaque terme. Chaque élément de ces ensembles correspond à une λ -coloration telle qu'elle prenne une valeur propre sur chacune des composantes connexes de (V, A) , c'est-à-dire λ . Comme il y a $\kappa(A)$ composantes, chaque terme est de la forme $(-1)^{|A|} \lambda^{\kappa(A)}$. ■

De plus nous montrons la propriété suivante :

Propriété 2.2.1

Soit G un graphe et $\chi(G, \lambda)$ son polynôme chromatique, alors

1. $\chi(G, \lambda) = \chi(G - e, \lambda) - \chi(G/e, \lambda)$
2. $\chi(G, \lambda) = 0$ si G contient une boucle
3. $\chi(G, \lambda) = (\lambda - 1)\chi(G/e, \lambda)$ si e est un isthme

PREUVE. Pour le premier point, soit e un arc de G et soit u et v ses extrémités. Alors soit une λ -coloration propre de $G - e$. Si u et v ont une couleur différente alors c'est une λ -coloration propre de G , et réciproquement une λ -coloration de G est une λ -coloration propre de $G - e$ avec u et v de couleurs différentes. Si u et v ont la même couleur alors on en déduit

une λ -coloration propre de G/e induite et réciproquement si on a une λ -coloration propre de G/e alors on en déduit une λ -coloration propre de $G - e$ en coloriant u et v de la même couleur.

Par ces correspondances, on en déduit que

$$\chi(G - e, \lambda) = \chi(G, \lambda) + \chi(G/e, \lambda)$$

puis le résultat.

Si G contient une boucle alors clairement il n'existe pas de λ -coloration propre donc $\chi(G, \lambda) = 0$, ce qui montre le deuxième point.

Soit e un isthme et u et v les extrémités de cet isthme. On note G_1 et G_2 les deux composantes connexes obtenues après suppression de l'arête e telles que $u \in G_1$ et $v \in G_2$. Une λ -coloration de G/e est une λ -coloration de G_1 et G_2 telle que la couleur de u et v soit la même. Pour tout couple de ces λ -coloration de G_1 et G_2 , on peut associer $\lambda - 1$ colorations telles que les couleurs de u et v soient différentes. Ces nouvelles λ -coloration sont des colorations de G donc on a :

$$\chi(G, \lambda) = (\lambda - 1)\chi(G/e, \lambda).$$

Ce qui montre le troisième point. ■

Le polynôme chromatique peut donc se calculer récursivement par suppression-contraction. Nous voudrions donc montrer que cette fonction est un invariant de Tutte-Grothendieck, néanmoins si nous considérons le graphe suivant :



Les deux sous-graphes $\bullet \text{ --- } \bullet$ sont en somme directe et de polynôme chromatique $\chi(\lambda) = \lambda(\lambda - 1)$, pourtant le polynôme chromatique de ce graphe est $\chi_G(\lambda) = \lambda(\lambda - 1)^2$. Ce qui contredit la propriété de multiplicativité des invariants de Tutte-Grothendieck.

De manière plus générale nous avons la propriété :

Théorème 2.2.2

Soit G un graphe et H_1, H_2 deux sous graphes de G tels que $H_1 \cap H_2 \simeq K_p$ avec K_p le graphe complet à p éléments, alors

$$\chi(G, \lambda) = \frac{\chi(H_1, \lambda)\chi(H_2, \lambda)}{\chi(K_p, \lambda)}.$$

Pour contourner ce problème, on pose $\hat{\chi}(G, \lambda) = \lambda^{-\kappa(G)}\chi(G, \lambda)$ avec $\kappa(G)$ le nombre de composantes connexes de G .

Théorème 2.2.3

$\hat{\chi}(G, \lambda)$ est un invariant de Tutte-Grothendieck.

PREUVE. On vérifie juste la multiplicativité, le reste se déduit de la proposition précédente. Soient H_1 et H_2 tels que $G = H_1 \oplus H_2$. Si H_1 et H_2 sont

disjoints alors $\kappa(G) = \kappa(H_1) + \kappa(H_2)$ et $\chi(G, \lambda) = \chi(H_1, \lambda)\chi(H_2, \lambda)$ et on a donc

$$\begin{aligned}\widehat{\chi}(G, \lambda) &= \lambda^{-\kappa(G)}\chi(G, \lambda) \\ &= \lambda^{-\kappa(H_1)-\kappa(H_2)} \cdot \chi(H_1, \lambda)\chi(H_2, \lambda) \\ &= \lambda^{-\kappa(H_1)}\chi(H_1, \lambda) \cdot \lambda^{-\kappa(H_2)}\chi(H_2, \lambda) \\ &= \widehat{\chi}(H_1, \lambda) \cdot \widehat{\chi}(H_2, \lambda)\end{aligned}$$

Maintenant si $H_1 \cap H_2 = \{e\} \simeq K_1$ alors $\kappa(G) = \kappa(H_1) + \kappa(H_2) - 1$ donc

$$\widehat{\chi}(G, \lambda) = \lambda^{-\kappa(H_1)-\kappa(H_2)+1}\chi(G, \lambda)$$

Or par le théorème précédent,

$$\chi(G, \lambda) = \frac{\chi(H_1, \lambda)\chi(H_2, \lambda)}{\chi(K_1, \lambda)}$$

et $\chi(K_1, \lambda) = \lambda$ donc

$$\begin{aligned}\widehat{\chi}(G, \lambda) &= \lambda^{-\kappa(H_1)} \cdot \lambda^{-\kappa(H_2)} \cdot \lambda \cdot \frac{\chi(H_1, \lambda)\chi(H_2, \lambda)}{\lambda} \\ &= \lambda^{-\kappa(H_1)}\chi(H_1, \lambda) \cdot \lambda^{-\kappa(H_2)}\chi(H_2, \lambda) \\ &= \widehat{\chi}(H_1, \lambda) \cdot \widehat{\chi}(H_2, \lambda)\end{aligned}$$

Nous pouvons donc exprimer $\widehat{\chi}(G, \lambda)$ en fonction du polynôme de Tutte :

$$\begin{aligned}\widehat{\chi}(G, \lambda) &= (-1)^{|E|-r(E)} \cdot 1^{|E|} \cdot T\left(G, \frac{\lambda-1}{-1}, \frac{0}{1}\right) \\ \iff \lambda^{-\kappa(G)}\chi(G, \lambda) &= (-1)^{|E|-r(E)} \cdot T(G, 1-\lambda, 0) \\ \iff \chi(G, \lambda) &= (-1)^{|E|-r(E)}\lambda^{\kappa(G)} \cdot T(G, 1-\lambda, 0)\end{aligned}$$

Ce qui conclut la preuve ■

On en déduit que le polynôme chromatique est lui aussi une évaluation du polynôme de Tutte :

$$\chi(G, \lambda) = (-1)^{r(E)}\lambda^{\kappa(G)}T(G, 1-\lambda, 0).$$

2.2.2 Le polynôme monochromatique

Une manière de généraliser le polynôme chromatique est de considérer, contrairement à la partie précédente, toutes les λ -colorations possibles et pas seulement les λ -colorations admissibles. Autrement dit on admet quelques "défauts" de coloration dans le graphe.

On définit un nouveau polynôme, appelé polynôme monochromatique, par sa série génératrice :

Définition 2.2.3

Soit G un graphe, on définit le polynôme chromatique avec défauts $B(G, \lambda, s)$ comme la série génératrice

$$B(G, \lambda, s) = \sum_i b_i(G, \lambda) s^i$$

avec $b_i(G, \lambda)$ le nombre de λ -colorations de G comportant exactement i arcs dont les extrémités sont de la même couleur.

Nous avons le même problème concernant la multiplicativité de ce polynôme pour deux graphes en somme directe. Nous posons donc à nouveau $\widehat{B}(G, \lambda, s) = \lambda^{-\kappa(G)} B(G, \lambda, s)$.

La propriété suivante nous montre que c'est un invariant de Tutte-Grothendieck :

Théorème 2.2.4

Soit G un graphe, e un arc de G et $B(G, \lambda, s)$ son polynôme monochromatique, alors $\widehat{B}(G, \lambda, s)$ est un invariant de Tutte-Grothendieck :

1. $\widehat{B}(G, \lambda, s) = \widehat{B}(G - e, \lambda, s) + (s - 1)\widehat{B}(G/e, \lambda, s)$.
2. $\widehat{B}(G_1 \oplus G_2, \lambda, s) = \widehat{B}(G_1, \lambda, s)\widehat{B}(G_2, \lambda, s)$.

En particulier, on a

$$\widehat{B}(G, \lambda, s) = (s - 1)^{r(G)} T\left(G, \frac{s + \lambda - 1}{s - 1}, s\right).$$

L'idée de la preuve est similaire à celle du polynôme chromatique :

PREUVE. On veut montrer le premier point. Montrons d'abord que pour $i \geq 1$ on a la relation de récurrence suivante :

$$b_i(G, \lambda) = b_i(G - e, \lambda) - b_i(G/e, \lambda) + b_{i-1}(G/e, \lambda).$$

Soit donc ϕ une λ -coloration de $G - e$ avec i défauts. Soient (u, v) les extrémités de e . Si $\phi(u) \neq \phi(v)$, alors c'est une λ -coloration avec i défauts de G . Par contre si on prend une λ -coloration de G avec i défauts, alors on doit de plus supposer que cette coloration ne comporte pas de défaut sur l'arc e , autrement dit si ce n'est pas une coloration de G/e avec $i - 1$ défauts (c'est-à-dire que si l'on contracte e , on ne supprime pas l'un des défauts de coloration). De plus les colorations de G/e avec i défauts induisent des colorations de $G - e$ avec i défauts donc $b_i(G/e, \lambda) \leq b_i(G - e, \lambda)$.

On en déduit une correspondance biunivoque qui se traduit par la relation :

$$b_i(G, \lambda) = b_i(G - e, \lambda) - b_i(G/e, \lambda) \text{ pour } \phi(u) \neq \phi(v)$$

Si maintenant $\phi(u) = \phi(v)$, alors cette coloration induit, de manière biunivoque, une coloration de G/e avec i défauts. On en déduit la relation de récurrence ci-dessus.

Par suite, sommant entre 1 et $|E|$ et en multipliant par s^i , on obtient :

$$\sum_{i=1}^{|E|} b_i(G, \lambda) s^i = \sum_{i=1}^{|E|} b_i(G - e, \lambda) s^i - \sum_{i=1}^{|E|} b_i(G/e, \lambda) s^i + \sum_{i=1}^{|E|} b_{i-1}(G/e, \lambda) s^i$$

De plus, si $i = 0$, alors $b_0(G, \lambda) = \chi(G, \lambda)$ donc on a la relation

$$b_0(G, \lambda) = b_0(G - e, \lambda) - b_0(G/e, \lambda).$$

On en déduit que :

$$\begin{aligned} B(G, \lambda, s) &= \sum_{i=0}^{|\mathbb{E}|} b_i(G, \lambda) s^i \\ &= \sum_{i=1}^{|\mathbb{E}|} b_i(G - e, \lambda) s^i - \sum_{i=0}^{|\mathbb{E}|} b_i(G/e, \lambda) s^i + \sum_{i=1}^{|\mathbb{E}|} b_{i-1}(G/e, \lambda) s^i \\ &= \sum_{i=1}^{|\mathbb{E}|} b_i(G - e, \lambda) s^i - \sum_{i=0}^{|\mathbb{E}|} b_i(G/e, \lambda) s^i + \sum_{i=0}^{|\mathbb{E}|} b_i(G/e, \lambda) s^{i+1} \\ &= \sum_{i=1}^{|\mathbb{E}|} b_i(G - e, \lambda) s^i - \sum_{i=0}^{|\mathbb{E}|} b_i(G/e, \lambda) s^i + s^{i+1} \\ &= \sum_{i=1}^{|\mathbb{E}|} b_i(G - e, \lambda) s^i + \sum_{i=0}^{|\mathbb{E}|} b_i(G/e, \lambda) (s - 1) s^i \\ &= \sum_{i=1}^{|\mathbb{E}|} b_i(G - e, \lambda) s^i + (s - 1) \sum_{i=0}^{|\mathbb{E}|} b_i(G/e, \lambda) s^i \\ &= B(G - e, \lambda) + (s - 1) B(G/e, \lambda) \end{aligned}$$

d'où le premier point.

La démonstration de la multiplicativité est identique à celle faite pour le polynôme chromatique. On a donc un invariant de Tutte-Grothendieck.

De plus, $\widehat{B}(L, \lambda, s) = s$ on peut colorier la boucle en admettant un défaut de coloration. De même, $\widehat{B}(C, \lambda, s) = (s + \lambda - 1)$.

On en déduit

$$\widehat{B}(G, \lambda, s) = (s - 1)^{r(G)} T \left(G, \frac{s + \lambda - 1}{s - 1}, s \right).$$

■

Par suite on peut retrouver le polynôme monochromatique

$$B(G, \lambda, s) = \lambda^{\kappa(G)} (s - 1)^{r(G)} T \left(G, \frac{s + \lambda - 1}{s - 1}, s \right).$$

En posant $x = \frac{s + \lambda - 1}{s - 1}$ et $y = s$, on a $(x - 1)(y - 1) = \lambda$ et on peut exprimer le polynôme de Tutte en fonction de $B(G, \lambda, s)$:

$$T(G, x, y) = \frac{1}{(y - 1)^{r(G) + \kappa(G)} (x - 1)^{\kappa(G)}} \cdot B(G, (x - 1)(y - 1), y).$$

Cette dernière relation sera particulièrement utile plus tard lorsque nous étudierons la fonction de partition en physique statistique ou la théorie des codes linéaires. Elle nous permet au moins de mettre en évidence l'importance de l'hyperbole $H_\alpha = \{(x, y) \mid (x - 1)(y - 1) = \alpha\}$ dans le plan de Tutte. Par exemple le long de l'hyperbole H_1 , le polynôme de Tutte se simplifie joliment :

Proposition 2.2.1

Soit G un graphe connexe. Le long de l'hyperbole H_1 , nous avons la relation :

$$T(G, x, y) = x^{|\mathbb{E}|} (x - 1)^{r(\mathbb{E}) - |\mathbb{E}|}.$$

PREUVE. Nous nous plaçons sur H_1 , alors la proposition précédente nous donne que

$$T(G, x, y) = \frac{1}{(y - 1)^{|\mathbb{V}|} (x - 1)} \cdot B(G, 1, y).$$

Si nous considérons le polynôme monochromatique $B(G, 1, y) = \sum_{i=0}^{|\mathbb{E}|} b_i(G, 1) y^i$.

Autrement dit on cherche à colorier le graphe G avec une seule couleur en admettant certains défauts de colorations. Supposons dans un premier temps que G est connexe. Alors la seule manière de colorier le graphe G dans ces conditions est d'admettre $|\mathbb{E}|$ défauts de colorations. Autrement pour tout i plus petit que $|\mathbb{E}|$, on a que $b_i(G, 1) = 0$ et pour $i = |\mathbb{E}|$, on a que $b_{|\mathbb{E}|}(G, 1) = 1$. Finalement $B(G, 1, y) = y^{|\mathbb{E}|}$ si G est connexe. On en déduit

$$T(G, x, y) = \frac{1}{(y - 1)^{|\mathbb{V}|} (x - 1)} \cdot y^{|\mathbb{E}|}.$$

Or si l'on considère l'expression $(x - 1)(y - 1) = 1$ de l'hyperbole H_1 , on en déduit que

$$(y - 1) = \frac{1}{x - 1}$$

et donc aussi que

$$\begin{aligned} y &= \frac{1}{x - 1} + 1 \\ &= \frac{1 + x - 1}{x - 1} \\ &= \frac{x}{x - 1} \end{aligned}$$

En intégrant ces données dans l'expression de $T(G, x, y)$ précédente, on obtient

$$\begin{aligned} T(G, x, y) &= \frac{(x - 1)^{|\mathbb{V}|}}{(x - 1)} \cdot \left(\frac{x}{x - 1} \right)^{|\mathbb{E}|} \\ &= \frac{(x - 1)^{|\mathbb{V}| - 1} x^{|\mathbb{E}|}}{(x - 1)^{|\mathbb{E}|}} \\ &= (x - 1)^{|\mathbb{V}| - |\mathbb{E}| - 1} x^{|\mathbb{E}|} \\ &= x^{|\mathbb{E}|} (x - 1)^{r(\mathbb{E}) - |\mathbb{E}|} \end{aligned}$$

car comme G est supposé connexe, $r(\mathbb{E}) = |\mathbb{V}| - \kappa(G) = |\mathbb{V}| - 1$.

2.2.3 Le polynôme de flots

Nous nous intéressons ici à la notion de k -flots partout non-nuls.

Définition 2.2.4

Soit $G = (V, E)$ un graphe orienté et A un groupe abélien fini. Un A -flot est une application $\Phi : G \rightarrow A$ telle que la loi de conservation de Kirshoff soit vérifiée :

$$\forall v \in V, \sum_{e \in \delta^+(v)} \Phi(e) = \sum_{e \in \delta^-(v)} \Phi(e).$$

Si $\text{supp}(\Phi) = E$, on dira que le flot est partout non-nul.

Exemple : La figure 2.3 donne un exemple de \mathbb{Z}_4 -flot partout non-nul sur un graphe orienté.

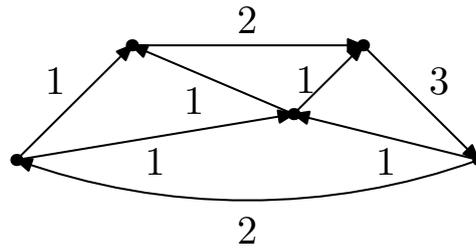


FIG. 2.3 – Exemple de \mathbb{Z}_4 -flot partout non-nul

On peut considérer que la notion de k -flots nuls nulle part est la notion duale de celle de coloration. En effet supposons que l'on ait une k -coloration propre de G , alors on peut construire une application $\phi : E(G) \rightarrow \{-(k-1), \dots, -1, 0, 1, \dots, k-1\}$ comme ceci : si les extrémités d'un arc e ont pour couleur x et y , on pose $\phi(e) = x - y$ et $\phi(e) = 0$ sinon. On montre que c'est un k -flot.

De plus comme la coloration de G est propre alors ϕ n'est jamais nulle. Soit G un graphe planaire. Si G^* admet une k -coloration si et seulement si G admet un k -flot nul nulle part.

Nous nous intéressons au nombre de A -flots partout non-nuls dans le graphe.

La proposition suivante montre que le nombre de A -flots partout non-nuls est un polynôme qui ne dépend pas de la structure du groupe abélien A , et qui, de plus, est relié au polynôme de Tutte. On appelle ce polynôme, **polynôme de flot**.

Théorème 2.2.5

Pour tout graphe G , il existe un polynôme noté $F(G, \lambda)$ tel que pour tout groupe abélien fini A d'ordre λ , $F(G, \lambda - 1)$ compte le nombre de A -flots partout non-nuls de G . De plus, on a la relation

$$F(G, \lambda) = (-1)^{|E| - r(E)} T(G, 0, 1 - \lambda).$$

On commence avec quelques lemmes :

Lemme 2.2.1

Soit $G = (V, E)$ un graphe orienté et $e \in E$ un arc du graphe n'étant ni un isthme ni une boucle. Si ϕ est un \mathbb{Z}_k -flot sur G , alors la restriction de ϕ à $E - \{e\}$ est :

1. un \mathbb{Z}_k -flot sur G/e ,

2. un \mathbb{Z}_k -flot sur $G - e$ si et seulement si $\phi(e) = 0$.

PREUVE. Soit $e = (u, v)$ un arc de G orienté de u vers v n'étant ni un isthme, ni une boucle. Le premier point est immédiat. En effet, si on note par i_1 et i_2 la valeur du flot entrant respectivement dans u et v et par o_1 et o_2 la valeur du flot sortant respectivement de u et v . Alors la loi de Kirshoff nous donne les relations :

$$i_1 = o_1 + \phi(e)$$

$$i_2 + \phi(e) = o_2$$

Si l'on contracte l'arête e , on identifie u et v , et par suite la valeur du flot entrant sur ce nouveau sommet est de $i_1 + i_2$ et la valeur du flot sortant est de $o_1 + o_2$. Par les relations précédentes, on a :

$$\begin{aligned} i_1 + i_2 &= o_1 + \phi(e) + o_2 - \phi(e) \\ &= o_1 + o_2 \end{aligned}$$

Par suite la loi de Kirshoff est bien vérifiée en ce point.

On montre maintenant le deuxième point : Si $\phi(e) = 0$ alors on a trivialement un \mathbb{Z}_k -flot sur $G - e$. Réciproquement, si on a un \mathbb{Z}_k -flot sur $G - e$, alors on déduit de la loi de Kirshoff en u et v que $\phi(e) = 0$. ■

Lemme 2.2.2

Soit $G = (V, E)$ un graphe orienté et e un arc de G n'étant ni un isthme, ni une boucle. On a les propriétés :

1. Étant donné un \mathbb{Z}_k -flot ϕ' sur G/e , il existe un seul \mathbb{Z}_k -flot ϕ sur G tel que $\phi|_{E-e} = \phi'$.
2. Étant donné un \mathbb{Z}_k -flot ϕ' sur $G - e$, il existe un seul \mathbb{Z}_k -flot ϕ sur G tel que $\phi|_{E-e} = \phi'$. De plus ce flot vérifie la propriété $\phi(e) = 0$.

PREUVE. Pour tout $e' \neq e$, nous avons nécessairement $\phi(e') = \phi'(e')$. On veut donc trouver une unique valeur de $\phi(e)$ qui rend le flot sur G valide. On note i_1, i_2, o_1, o_2 les valeurs des flots entrant et sortant des sommets u et v de G . Comme, par la remarque au dessus, le seul point où ϕ n'est pas encore défini est en e . Or $\phi(e)$ vérifie les équations dans G :

$$\phi(e) = i_1 - o_1$$

$$\phi(e) = o_2 - i_2$$

Dans le cas de G/e , on a l'équation $i_1 + i_2 = o_1 + o_2$ donc $i_1 - o_1 = o_2 - i_2$ et donc $\phi(e)$ est défini de manière unique. Dans le cas de $G - e$, on a que $i_1 = o_1$ et $i_2 = o_2$. Donc dans ce cas, on a une unique valeur possible : $\phi(e) = 0$ ■

On s'attaque maintenant à la preuve du théorème :

PREUVE. Les deux lemmes précédents nous fournissent une correspondance bijective entre les \mathbb{Z}_k -flots partout non-nuls de $G - e$ et les \mathbb{Z}_k -flots de G partout non-nuls sauf en e ainsi qu'une correspondance entre les \mathbb{Z}_k -flots partout non-nuls de G/e et les \mathbb{Z}_k -flots partout non-nuls sauf peut-être en e de G (avec e un arc qui n'est ni un isthme ni une boucle).

On en déduit que

$$F(G/e, \mathbb{Z}_k) = F(G - e, \mathbb{Z}_k) + F(G, \mathbb{Z}_k)$$

donc que

$$F(G, \mathbb{Z}_k) = F(G/e, \mathbb{Z}_k) - F(G - e, \mathbb{Z}_k).$$

pour tout arc e un arc qui n'est ni une boucle ni un isthme.

Sur le graphe L (graphe composé d'un sommet et d'une boucle), on a $F(L, \mathbb{Z}_k) = k - 1$ car la boucle peut prendre toutes les valeurs possibles sauf l'élément neutre 0. Sur le graphe C (graphe composé de deux sommets et d'une arête entre ces sommets), on a $F(C, \mathbb{Z}_k) = 0$ (il n'y a pas de flot valide sur ce graphe).

De plus si l'on considère un graphe $G = G_1 \oplus G_2$. Comme un \mathbb{Z}_k -flot d'un graphe est déterminé par la valeur de ses arêtes et que G_1 et G_2 n'en partagent aucune alors on a immédiatement que $F(G, \mathbb{Z}_k) = F(G_1, \mathbb{Z}_k)F(G_2, \mathbb{Z}_k)$.

Ainsi,

$$\begin{aligned} F(G, \mathbb{Z}_k) &= (-1)^{|E| - r(E)} T(G, 0, \frac{k-1}{-1}) \\ &= (-1)^{|E| - r(E)} T(G, 0, 1 - k) \end{aligned}$$

et de ce fait $F(G, \mathbb{Z}_k)$ est un polynôme en k . ■

Cette propriété a des implications importantes dans l'étude des configurations de glace dans un graphe :

Définition 2.2.5

Soit G un graphe 4-régulier. On appelle "configuration de glace" de G toute orientation des arêtes telle que pour tout sommet v du graphe, on ait $\delta^+(v) = \delta^-(v) = 2$.

Le nom de "configuration de glace" vient de la physique. En effet, certains cristaux, à la température du zéro absolu, ont une entropie non nulle (on parle d'entropie résiduelle) du fait de certaines forces conflictuelles dans le réseau cristallin qui interdisent une minimisation globale de l'entropie (on parle de frustration géométrique). En d'autres termes, la structure ne peut être "gelée" complètement. Il en est par exemple de la glace qui possède une énergie estimée de $3.4 \text{ J} / (\text{mol} \cdot \text{K})$ du fait de la structure tétraédrique des cellules du cristal.

Dans la glace, les atomes d'hydrogène sont toujours alignés sur une liaison du type oxygène-oxygène. Ainsi, chaque atome d'oxygène est entouré de 4 atomes d'hydrogène et chaque atome d'hydrogène est adjacent à deux atomes d'oxygène. Le problème étant que l'état d'énergie minimale du système n'est pas obtenu lorsque les atomes d'hydrogène sont situés au milieu de la liaison O-O. Les atomes d'hydrogène peuvent donc prendre deux positions différentes sur cette liaison : soit être plus proches de l'atome d'oxygène central, soit être plus proches des atomes d'oxygène adjacents. On est dans un cas classique de frustration géométrique où les cellules forment un réseau tétraédrique.

La figure 2.4 montre cette situation où les points noirs sont les atomes d'hydrogène, les cercles sont les atomes d'oxygène et les flèches noires sont les spins associés à chacun des atomes d'hydrogène.

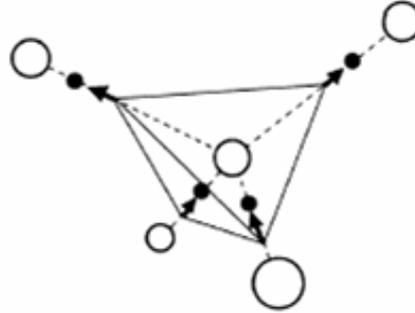


FIG. 2.4 – Frustration géométrique dans un cristal tétraédrique de molécules d'eau

Pour revenir à la notion de "configuration de glace" en théorie des graphes, on voit que l'on peut associer à chaque atome d'oxygène un sommet du graphe et à chaque atome d'hydrogène un arc entre les deux sommets représentant les atomes d'oxygène qui lui sont adjacents. En ajoutant des orientations à ces arcs, on peut représenter l'état de l'atome d'hydrogène : un arc entrant à v si l'atome H est proche du sommet v et sortant s'il lui est plus éloigné.

La propriété suivante fait intervenir le polynôme de Tutte dans le comptage des "configurations de glace" d'un graphe 4-régulier.

Corollaire 2.2.1

$T(G, 0, -2)$ compte le nombre de "configurations de glace" de G .

Remarque 2.2.1

On peut en effet construire une bijection entre les \mathbb{Z}_3 -flots partout non-nuls comptés par $T(G, 0, -2)$ et les configurations de glaces de G .

La notion de k -flots partout non-nuls est la notion duale de coloration propre. On a la propriété

Proposition 2.2.2

Soit G un graphe planaire connexe. Alors on a

$$\chi(G, \lambda) = \lambda F(G^*, \lambda).$$

PREUVE. C'est immédiat en utilisant la formule de dualité du polynôme de Tutte :

$$T(G, x, y) = T(G^*, y, x).$$

On a donc comme G est supposé connexe :

$$\begin{aligned} \chi(G, \lambda - 1, 0) &= (-1)^{|E| - r(E)} \lambda T(G, \lambda - 1, 0) \\ &= (-1)^{|E| - r(E)} \lambda T(G^*, 0, \lambda - 1) \\ &= \lambda F(G^*, \lambda) \end{aligned}$$

■

2.2.4 Le polynôme de connectivité

Nous nous intéressons maintenant à un autre polynôme connu sous le nom de polynôme de connectivité (ou polynôme de fiabilité). Ce polynôme est très intéressant car il s'exprime en terme de probabilité.

La connectivité d'un graphe exprime le fait que l'on puisse supprimer un certain nombre d'arcs tout en conservant la connexité du graphe :

Définition 2.2.6

On dit qu'un graphe connexe G a une connectivité de k si en supprimant k éléments de G , G reste connexe.

On se demande maintenant ce qui arrive si l'on supprime des arcs de graphe indépendamment avec une probabilité p . L'une des applications naturelles de ce sujet est par exemple l'étude de la fiabilité des réseaux informatiques. Les liens dans le graphe représentent les connexions entre les machines. Ces liens peuvent tomber en panne et on se demande alors si toutes les machines vont rester accessibles par toutes les autres.

En fait, cette propriété de connectivité est un polynôme en la probabilité p :

Définition 2.2.7

Soit G un graphe connexe. La probabilité que le graphe reste connexe après suppression de chacune des arêtes indépendamment avec une probabilité p est donnée par le polynôme :

$$\begin{aligned} R(G, p) &= \sum_{A \text{ connexe couvrant}} p^{|A|} (1-p)^{|E-A|} \\ &= \sum_{k=0}^{m-n+1} g_k p^{k+n-1} (1-p)^{m-k-n+1} \end{aligned}$$

avec n le nombre de sommets de G , m le nombre d'arêtes et g_k le nombre de sous-graphes connexes couvrant de $k+n-1$ arcs.

Le point important est que c'est aussi un invariant de Tutte-Grothendieck :

Théorème 2.2.6

Soit G un graphe connexe alors $R(G, p)$ est un invariant de Tutte-Grothendieck et

$$R(G, p) = p^{|E|-r(E)} (1-p)^{r(E)} T(G, 1, 1/p).$$

PREUVE. On va montrer que :

$$R(G, p) = pR(G-e, p) + (1-p)R(G/e, p)$$

si e n'est ni une boucle ni un isthme et que

$$R(H_1 \oplus H_2, p) = R(H_1, p)R(H_2, p)$$

Soit e un arc de G qui n'est ni une boucle ni un isthme.

On considère les cas :

- si e est supprimé, alors G reste connexe si et seulement si $G - e$ reste connexe, ce qui arrive avec la probabilité $R(G - e, p)$ or la probabilité que e soit supprimé est de p donc la probabilité que e soit supprimé mais que G reste connexe est donné par $pR(G - e, p)$.
- si e n'est pas supprimé, alors G reste connexe si et seulement si G/e reste connexe ce qui arrive avec la probabilité $R(G/e, p)$ donc la probabilité que e ne soit pas supprimé et que G reste connexe est donnée par $(1 - p)R(G/e, p)$

On somme les probabilités sur ces deux cas séparés pour obtenir la première relation :

$$R(G, p) = pR(G - e, p) + (1 - p)R(G/e, p).$$

De plus, on a clairement que si $G = H_1 \oplus H_2$ alors G reste connexe si et seulement si H_1 reste connexe et H_2 reste connexe donc on a bien :

$$R(G, p) = R(H_1, p)R(H_2, p).$$

Donc le polynôme $R(G, p)$ est un invariant de Tutte-Grothendieck, donc peut s'obtenir comme une évaluation du polynôme de Tutte :

On a que :

- Si $G = L$ alors e est une boucle et clairement sa suppression ne change pas le nombre de composantes connexes de G donc $R(G, p) = 1$.
- Si $G = C$ alors e est un isthme et donc le nombre de composantes connexes de G n'est pas modifié si et seulement si e n'est pas supprimé $R(G, p) = p$.

donc on a bien la relation :

$$R(G, p) = p^{|\mathbb{E}| - r(\mathbb{E})} (1 - p)^{r(\mathbb{E})} T(G, 1, 1/p).$$

■

Remarque 2.2.2

On peut étendre la propriété précédente au cas des graphes à plusieurs composantes connexes en posant :

$$R(G \sqcup H, p) = R(G, p)R(H, p)$$

et au lieu d'avoir un graphe restant connexe, on a un graphe dont le nombre de composantes connexes n'augmente pas.

2.2.5 Orientations d'un graphe

On donne maintenant une propriété combinatoire sur les graphes assez surprenante, puisqu'elle s'exprime en comptant certaines orientations particulières du graphe.

Définition 2.2.8

Soit $G = (V, E)$ un graphe connexe. Une orientation de G correspond à donner une orientation à chacun des arcs de G . On peut la définir formellement comme une fonction $\sigma : E \rightarrow \{-1, 1\}$ telle que pour tout couple $(u, v) \in V^2$, $\sigma(u, v) = -\sigma(v, u)$.

On dit qu'une orientation est :

- acyclique si le graphe orienté n'a pas de cycles
- totalement cyclique si tout arc du graphe orienté est contenu dans un cycle

Comme nous le verrons ensuite ces deux notions sont duales. Nous montrons maintenant que c'est bien un invariant de Tutte-Grothendieck :

Théorème 2.2.7

Soit $\kappa(G)$ le nombre d'orientations acycliques de G . $\kappa(G)$ est un invariant de Tutte-Grothendieck :

$$\kappa(G) = \kappa(G - e) + \kappa(G/e) \text{ si } e \text{ n'est ni une boucle ni un isthme}$$

$$\kappa(H_1 \oplus H_2) = \kappa(H_1)\kappa(H_2).$$

et on a la relation :

$$\kappa(G) = T(G, 2, 0)$$

PREUVE. Soit $G = (V, E)$ un graphe.

La seconde relation est évidente. On montre la première. Soit donc $e = (u, v)$ une arête de G qui ne soit ni un arc ni une boucle. Si σ est une orientation acyclique de G alors on a immédiatement que $\tau = \sigma|_{V-e}$ est une orientation acyclique de $G - e$. De plus, τ est une orientation acyclique de G/e si et seulement si il n'existe pas de chemins orientés joignant u à v ou v à u dans $G - e$. Il y a exactement $\kappa(G/e)$ orientations acycliques de ce type et chaque orientation acyclique de G/e permet de construire deux orientations acycliques de G (en orientant l'arc dans les deux sens). Maintenant il reste $\kappa(G - e) - \kappa(G/e)$ orientations acycliques qui n'ont pas cette propriété, donc on en déduit :

$$\begin{aligned} \kappa(G) &= 2\kappa(G/e) + (\kappa(G - e) - \kappa(G/e)) \\ &= \kappa(G - e) + \kappa(G/e) \end{aligned}$$

Ce qui montre que $\kappa(G)$ est un invariant de Tutte-Grothendieck. Or si G contient une boucle, il ne peut y avoir d'orientations acycliques de G donc $\kappa(L) = 0$ et si $G = C$ alors il y a deux orientations acycliques donc $\kappa(C) = 2$. On en déduit que :

$$\kappa(G) = T(G, 2, 0).$$

■

De même pour la propriété duale :

Théorème 2.2.8

Soit $\kappa^*(G)$ le nombre d'orientations totalement cycliques de G . $\kappa^*(G)$ est un invariant de Tutte-Grothendieck :

$$\kappa^*(G) = \kappa^*(G - e) + \kappa^*(G/e) \text{ si } e \text{ n'est ni une boucle ni un isthme}$$

$$\kappa^*(H_1 \oplus H_2) = \kappa^*(H_1)\kappa^*(H_2).$$

et on a la relation :

$$\kappa^*(G) = T(G, 0, 2)$$

PREUVE. La démonstration se fait exactement de la même manière que la précédente. ■

On considère maintenant les orientations acycliques avec une seule source. Il est loin d'être évident que le nombre d'orientation de ce type soit indépendant du sommet choisi, pourtant on a la propriété :

Proposition 2.2.3

Soit $\kappa(G, v)$ le nombre d'orientation avec pour seule source $v \in V$. Alors $\kappa(G, v)$ est un invariant de Tutte-Grothendieck et $\kappa(G, v) = T(G, 1, 0)$.

La propriété duale est loin d'être aussi naturelle que la précédente :

Proposition 2.2.4

Soit G un graphe muni d'un ordre sur ses arêtes. Alors $T(G, 0, 1)$ compte le nombre de réorientation totalement cyclique τ de G telles que pour chaque cycle de τ la plus petite arête du cycle n'est pas réorientée.

Stanley a donné dans (Stao6), une interprétation plus générale recouvrant les deux précédentes. Nous énonçons la propriété ici, elle est la suite de la remarque que nous avons faite dans le chapitre sur le polynôme chromatique concernant l'interprétation en terme d'orientations.

Définition 2.2.9

On note par $\bar{\chi}(G, \lambda)$ le nombre de couples (f, σ) avec f une fonction $f : V \rightarrow \{1, 2, \dots, \lambda\}$ et σ une orientation acyclique de G telle que :

$$\text{Si } u \rightarrow v \text{ alors } f(u) \geq f(v).$$

On peut montrer la propriété suivante :

Proposition 2.2.5

On a pour, tout entier λ positif,

$$\bar{\chi}(G, \lambda) = (-1)^{|V|} \chi(G, -\lambda),$$

avec $\chi(G, \lambda)$ le polynôme chromatique.

De plus comme $\chi(G, \lambda) = (-1)^{r(E)} \lambda^{k(G)} T(G, 1 - \lambda, 0)$ alors

$$\bar{\chi}(G, \lambda) = -\lambda^{k(G)} T(G, 1 + \lambda, 0).$$

De plus on voit que cette interprétation recouvre bien la propriété précédente pour $\lambda = 1$. De plus elle étend la notion de polynôme chromatique aux valeurs négatives.

2.2.6 Espace des bicycles et polynôme de Tutte

Nous voyageons maintenant dans l'espace des bicycles. Pour cela nous avons besoin de quelques définitions :

Définition 2.2.10

Soient G un graphe et M sa matrice d'incidence. On appelle l'espace des cycles, l'espace vectoriel engendré par les colonnes de M et on le note \mathcal{C} . On appelle espace des co-cycles, l'espace orthogonal à \mathcal{C} : \mathcal{C}^\perp . On appelle espace des bicycles $\mathcal{B} = \mathcal{C} \cap \mathcal{C}^\perp$.

Les éléments de \mathcal{C} sont appelés les cycles, les éléments de \mathcal{C}^\perp sont appelés co-cycles et les éléments de \mathcal{B} sont appelés bicycles.

Si l'on considère l'espace des cycles comme un \mathbb{R} -espace vectoriel alors comme l'espace des co-cycles est l'orthogonal de l'espace des cycles, l'espace des bicycles est trivial donc n'est pas très intéressant. Néanmoins comme la matrice d'incidence est composée uniquement de 0 et de 1, on peut considérer le \mathbb{Z}_2 -espace vectoriel et dans ce cas l'espace des bicycles n'est plus trivial.

Avec l'espace des bicycles, nous pouvons introduire une partition naturelle des arêtes du graphe en trois classes différentes, ce qui est donné par le théorème suivant :

Théorème 2.2.9

Soit e un arc d'un graphe G . Alors exactement une des propriétés suivantes est vérifiée :

1. e appartient à un bicycle.
2. e appartient à un cycle γ tel que $\gamma - e$ soit un co-cycle.
3. e appartient à un co-cycle ω tel que $\omega - e$ soit un cycle.

Exemple : La figure 2.5 montre la tripartition des arcs d'un graphe en éléments de type 1) en **bleu**, 2) en **vert** et 3) en **rouge**.

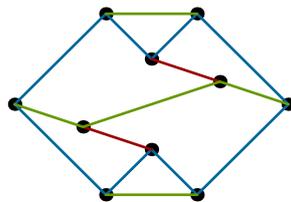


FIG. 2.5 – Tripartition des arcs d'un graphe

On pourra trouver une démonstration de ce théorème dans (PR78).

On peut relier la dimension de l'espace des bicycles de G avec celle de G/e et $G - e$ en utilisant le théorème précédent.

Proposition 2.2.6

Soit e une arête d'un graphe G qui ne soit ni une boucle ni un isthme et dont l'espace des bicycles soit de dimension $\dim_{\mathcal{B}}(G) = b$. Par le théorème précédent, e vérifie l'un des trois cas précédents. On a donc les trois relations suivantes :

- Si e est dans le cas 1) alors $\dim_{\mathcal{B}}(G - e) = b - 1$ et $\dim_{\mathcal{B}}(G/e) = b - 1$
- Si e est dans le cas 2) alors $\dim_{\mathcal{B}}(G - e) = b + 1$ et $\dim_{\mathcal{B}}(G/e) = b$
- Si e est dans le cas 3) alors $\dim_{\mathcal{B}}(G - e) = b$ et $\dim_{\mathcal{B}}(G/e) = b + 1$

PREUVE. On cherche à exprimer la dimension de l'espace des bicycles de $G - e$ en fonction de celui de G . On traitera le cas de la dimension de

l'espace des bicycles de G/e par dualité.

Soit α un cycle, cocycle ou bicycle de G . On regarde les éléments qui se transforment en bicycles de $G - e$ en supprimant l'arête e . Si α est un bicycle de G alors c'est un bicycle de G si et seulement si α ne contient pas e .

Si α n'est pas un bicycle et ne contient pas l'arête e alors ce n'est pas un bicycle de $G - e$.

Par contre si e appartient à α , alors c'est un bicycle dans $G - e$ si et seulement si en supprimant e de α on obtient un cocycle de G .

On traite maintenant les trois cas donnés par la tripartition des arêtes :

- Si on est dans le cas 1) alors e appartient à un bicycle donc tous les bicycles de G contenant e sont perdus en passant à $G - e$. Par suite la dimension de l'espace des bicycles de $G - e$ est diminué de 1 donc vaut $b - 1$. Par dualité, on en déduit aussi que la dimension de l'espace des bicycles de G/e diminue aussi de 1.
- Si on est dans le cas 2), e appartient à un cycle γ et $\gamma - e$ est un cocycle donc un bicycle dans $G - e$ donc la dimension de l'espace des bicycles de $G - e$ vaut $b + 1$.
- Si on est dans le cas 3), e appartient à un cocycle ω et $\omega - e$ est un cycle donc n'est pas un cocycle car dans ce cas ce serait un bicycle ce qui est impossible. Donc ce cas ne se produit pas.

■

A partir de ces différents cas, on peut exhiber un invariant de Tutte-Grothendieck qui correspond (au signe près) au nombre de bicycles :

$$\text{bike}(G) = (-1)^{|E|} (-2)^{\dim(\mathcal{B})}.$$

Proposition 2.2.7

bike(G) est un invariant de Tutte-Grothendieck et on a :

$$T(G, -1, -1) = (-1)^{|E|} (-2)^{\dim(\mathcal{B})}.$$

PREUVE. Soit e un arc qui ne soit ni une boucle ni un isthme. On distingue trois cas comme précédemment :

- Si e est dans le cas 1) alors on a :

$$\begin{aligned} \text{bike}(G - e) + \text{bike}(G/e) &= (-1)^{|E|-1} (-2)^{\dim(\mathcal{B})-1} + (-1)^{|E|-1} (-2)^{\dim(\mathcal{B})-1} \\ &= 2(-1)^{|E|-1} (-2)^{\dim(\mathcal{B})-1} \\ &= (-1)^{|E|} (-2)^{\dim(\mathcal{B})} \\ &= \text{bike}(G) \end{aligned}$$

- Si e est dans le cas 2) ou 3), alors on a :

$$\begin{aligned} \text{bike}(G - e) + \text{bike}(G/e) &= (-1)^{|E|-1} (-2)^{\dim(\mathcal{B})-1} + (-1)^{|E|-1} (-2)^{\dim(\mathcal{B})-1} \\ &= 2(-1)^{|E|-1} (-2)^{\dim(\mathcal{B})+1} \\ &= (-1)^{|E|} (-2)^{\dim(\mathcal{B})} \\ &= \text{bike}(G) \end{aligned}$$

On en déduit que

$$\text{bike}(G) = \text{bike}(G - e) + \text{bike}(G/e)$$

si e n'est ni une boucle ni un isthme.

De plus on a clairement que :

$$\text{bike}(H_1 \oplus H_2) = \text{bike}(H_1)\text{bike}(H_2).$$

Donc $\text{bike}(G)$ est un invariant de Tutte-Grothendieck et de plus on a que $\text{bike}(L) = -1$ et $\text{bike}(C) = -1$, donc on en déduit que

$$T(G, -1, -1) = \text{bike}(G) = (-1)^{|E|} (-2)^{\dim(B)}.$$

■

2.3 APPLICATIONS À LA PHYSIQUE STATISTIQUE

Nous avons énoncé plusieurs applications à la théorie des graphes. Nous allons maintenant voir des domaines plus variés. Nous commençons l'exploration avec certaines applications à la physique statistique.

La physique statistique s'intéresse au comportement et à l'évolution de systèmes physiques comportant un grand nombre de particules (atomes, ions, molécules). De manière plus générale, la physique statistique est un outil particulièrement puissant pour l'étude des systèmes comportant un grand nombre de variables en utilisant des méthodes statistiques.

Nous nous intéressons ici à l'étude des configurations de spins sur des graphes finis.

Nous introduisons plusieurs définitions dans un premier temps :

Définition 2.3.1

On appelle **configuration** du graphe une application de l'ensemble des sommets vers un ensemble $\{s_1, s_2, \dots, s_k\}$. Les éléments de $\{s_1, s_2, \dots, s_k\}$ sont appelés les **spins**. L'ensemble de toutes les configurations est appelé **espace des configurations**.

Les arêtes du graphe représentent des interactions entre les différents spins. Ainsi seuls deux sommets adjacents dans le graphe peuvent interagir (de manière directe). En fait nous pouvons associer une certaine **énergie d'interaction** entre les différents spins.

Nous nous posons maintenant la question de savoir comment évolue la configuration lorsque la température varie. Plus particulièrement nous nous intéressons aux configurations d'*énergie minimale*.

Différents modèles ont été développés pour répondre à cette question. Le modèle de Lenz-Ising ou modèle d'Ising est l'un des plus connus.

2.3.1 Le modèle d'Ising

Dans ce modèle, nous avons uniquement deux spins possibles que nous représenterons par +1 et -1 respectivement. Nous nous intéressons dans un premier temps au système le plus simple sans champ magnétique extérieur et où l'énergie d'interaction entre deux spins vaut une constante notée J.

A toute configuration σ du graphe, nous pouvons associer l'**énergie de la configuration** ou **hamiltonien** :

$$\mathcal{H}(\sigma) = - \sum_{(x,y) \in E} J\sigma(x)\sigma(y)$$

Lorsque $J > 0$ les spins ont tendance à s'aligner à la même valeur que celle de leurs voisins, le modèle est dit ferromagnétique :

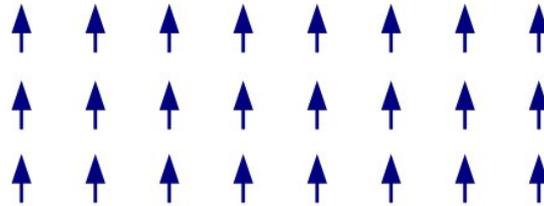


FIG. 2.6 – Alignement des spins dans le modèle ferromagnétique

Si $J < 0$ alors le modèle est dit anti-ferromagnétique et les spins ont tendance à prendre la valeur opposée à celle de leurs voisins :

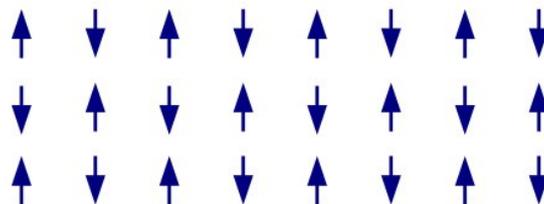


FIG. 2.7 – Alignement des spins dans le modèle anti-ferromagnétique

La probabilité de trouver le système dans une configuration σ est donnée via la mesure de Gibbs :

$$\mu_\sigma = \frac{1}{Z} e^{-\beta \mathcal{H}(\sigma)}$$

avec $\beta = \frac{1}{kT}$ la température inverse et k la constante de Boltzmann.

Dans cette équation, la constante de normalisation Z est appelée la **fonc-**

tion de partition du système et est donnée par :

$$Z = \sum_{\sigma} e^{-\beta H(\sigma)}.$$

Cette fonction joue un rôle très important en physique statistique car elle encode quasiment l'ensemble des propriétés statistiques (entropie, énergie totale, etc.) du système. Plus précisément, c'est l'énergie libre de Helmholtz A donnée par $A = -kT \log Z$ qui joue ce rôle.

Par exemple, on peut trouver l'entropie S du système en dérivant l'énergie libre à volume fixé :

$$S = - \left(\frac{\partial F}{\partial T} \right)_V$$

Nous allons voir que nous pouvons trouver une interprétation combinatoire de ce modèle. Nous aurions pu montrer que la fonction de partition est un invariant de Tutte-Grothendieck et vérifie :

$$\begin{aligned} Z(G) &= e^{\beta J} Z(G'_e) + 2 \sinh(\beta J) Z(G''_e) \\ Z(C) &= 2e^{\beta J} + 2e^{-\beta J} \\ Z(L) &= 2e^{\beta J} \end{aligned}$$

ce qui conduit à la formule suivante :

$$Z(G) = (2e^{-\beta J})^{|\mathcal{E}| - r(\mathcal{E})} (4 \sinh \beta J)^{r(\mathcal{E})} T(G, \coth \beta J, e^{2\beta J})$$

Néanmoins nous préférons introduire pour montrer cela, un autre polynôme qui nous servira à généraliser plus facilement le modèle d'Ising.

Pour cela nous avons besoin de la notion de coupe dans un graphe.

Définition 2.3.2

On appelle coupe une partition F des arêtes telle qu'il existe une partition des sommets du graphe.

A partir de là, nous considérons la taille des coupes et notons b_i le nombre de coupe avec i arcs.

Définition 2.3.3

Soit donc $G = (V, \mathcal{E})$ un graphe. On appelle **polynôme des coupes** et on note $B(G, s)$ la série génératrice

$$B(G, s) = \sum_{i=0}^{|\mathcal{E}|} b_i s^i$$

On peut exprimer la fonction de partition en fonction de ce polynôme. En effet si l'on considère une configuration σ du modèle d'Ising. Alors chaque sommet du graphe à un spin pouvant prendre deux valeurs possibles. On peut donc partitionner le graphe suivant la valeur prise par le spin,

ce qui nous donne une partition des sommets $V = (V_1, V_2)$ et on peut décomposer l'hamiltonien du système suivant cette partition :

$$\begin{aligned}
\mathcal{H}(\sigma) &= - \sum_{\{x,y\} \in V} J\sigma(x)\sigma(y) \\
&= \sum_{\{x,y\} \in V_1} -J\sigma(x)\sigma(y) + \sum_{\{x,y\} \in V_2} -J\sigma(x)\sigma(y) + \sum_{x \in V_1, y \in V_2} -J\sigma(x)\sigma(y) \\
&= \sum_{\{x,y\} \in V_1} -J + \sum_{\{x,y\} \in V_2} -J + \sum_{x \in V_1, y \in V_2} J \\
&= -mJ + J|C(V_1, V_2)|
\end{aligned}$$

avec $|C(V_1, V_2)|$ le nombre d'arêtes dont l'une des extrémités est dans V_1 et l'autre dans V_2 .

Autrement dit, lorsque l'on recherche les configurations d'énergie minimale de ce système on est rammené à trouver une coupe dans le graphe. Dans le cas ferromagnétique, le problème revient à minimiser $|C(V_1, V_2)|$, ce qui est le problème de la coupe minimale donc un problème polynomial. Par contre, dans le modèle anti-ferromagnétique, ce problème est NP-complet (et même non-approximable).

Théorème 2.3.1

MAXCUT est un problème NP-complet.

PREUVE. Le problème appartient clairement à la classe NP. On effectue une réduction depuis le problème NAE – 3 – SAT (Not All Equal 3-SAT). On considère une instance du problème NAE – 3 – SAT, c'est-à-dire un ensemble C de m clauses logiques sur un ensemble de n variables : a_1, \dots, a_n . Les clauses sont de la forme $C_i = x \wedge y \wedge z$ avec x, y, z des littéraux associés aux variables a_1, \dots, a_n .

A partir de ces clauses, on construit un graphe dont les sommets sont les littéraux donc de $2n$ sommets (les variables et leur négation). On relie ensuite les sommets correspondants aux littéraux d'une même clause. De même on relie chaque littéral avec son littéral opposé. On a donc $3m + n$ arêtes.

On vérifie que les clauses sont satisfaites si et seulement si le graphe ci-dessus admet une coupe de taille $2m + n$.

Supposons que les clauses soient NAESAT. Alors, si l'on considère l'ensemble des littéraux positifs S , $(S, V - S)$ est une coupe de taille $2m + n$.

Réciproquement, on peut supposer sans perte de généralité que les littéraux x_i et $\neg x_i$ ne sont pas dans le même ensemble. En effet dans le cas contraire on peut le changer de côté sans changer la taille de la coupe. Ainsi il y a exactement n arcs entre littéraux donc au plus $2m$ arcs introduits lorsqu'on ajoute les arcs associés aux clauses. Par suite on a l'égalité si et seulement si toutes les clauses sont NAESAT.

On a donc bien la réduction donc MAXCUT est NP-complet. ■

Ainsi le problème de trouver la fonction de partition dans le cas anti-ferromagnétique est un problème NP-difficile. Néanmoins dans le cas des

graphes planaires, la fonction de partition est calculable en temps polynomial.

On s'intéresse maintenant à la relation qu'entretient la fonction de partition avec le polynôme de Tutte. En effet le polynôme de coupe est un invariant de Tutte-Grothendieck par la proposition suivante :

Proposition 2.3.1

Soit G un graphe et e un arc qui ne soit ni une boucle ni un isthme alors on a :

$$B(G, s) = sB(G - e, s) + (1 - s)B(G/e, s)$$

et de plus

$$B(C, s) = 1 + s$$

$$B(L, s) = 1$$

PREUVE. Les deux dernières propriétés sont triviales.

Pour la première, on va montrer que la propriété est vérifiée sur les coefficients $b_i(G)$ de la série génératrice.

On pose $e = (a, b)$ un arc quelconque et on essaye de partitionner les coupes. Soit donc C une coupe quelconque :

- Si e n'appartient pas à la coupe C alors c'est une coupe de G/e .
- Si e appartient à la coupe C alors c'est une coupe de $G - e$ telle que a et b sont dans deux composantes différentes. Or une coupe de G dans laquelle a et b sont dans la même composante est aussi une coupe de G/e .

En partitionnant les coupes selon si elle contiennent e ou pas, on en déduit la relation :

$$b_i(G) = b_{i-1}(G - e) + b_i(G) - b_{i-1}(G/e)$$

ce qui conduit à la relation finale.

On peut montrer (de la même manière que pour le polynôme monochromatique) que :

$$B(G, s) = s^{m-n+1}(1 - s)^{n+1}T(G, \frac{1+s}{1-s}, \frac{1}{s})$$

et donc exprimer la fonction de partition en fonction du polynôme de Tutte :

$$Z(G, \beta) = 2\theta^{m/2-n+1}(1 - \theta)^{n-1}T(G, \frac{1+\theta}{1-\theta}, \frac{1}{\theta})$$

avec $\theta = e^{-2\beta J}$.

Il existe des généralisations de ce modèle à un cas inhomogène c'est-à-dire où les énergies d'interactions entre spins sont toutes différentes. On peut aussi ajouter un champ magnétique extérieur et dans ce cas les spins vont avoir tendance à s'aligner en fonction de ce champ.

L'hamiltonien pour ce modèle est donné par :

$$H(\sigma) = -\sum_{(ij)} J_{ij}\sigma_i\sigma_j - \sum_i M\sigma_i$$

où M est l'énergie apportée par le champ magnétique.

2.3.2 Le modèle de Potts

On considère maintenant une généralisation du modèle d'Ising au cas où le nombre de valeurs possibles prises par les spins vaut $q \geq 2$.

On suppose un modèle sans champ magnétique extérieur. L'hamiltonien du système est donné par :

$$H(\sigma) = \sum_{(ij)} K_{ij}(1 - \delta(\sigma_i \sigma_j))$$

où K_{ij} est l'énergie d'interaction associée à l'arc (ij) et δ est le symbole de Kronecker.

La fonction de partition est donc :

$$Z = \sum_{\sigma} e^{-H(\sigma)}.$$

Si l'on considère l'ensemble des arêtes E on peut partitionner naturellement les arêtes en celles dont les extrémités sont de spin différents (E^-) et celle dont le spin est identique (E^+).

Si l'on suppose que l'énergie d'interaction est constante et égale à K alors on peut réécrire la fonction de partition :

$$Z = \sum_{\sigma} e^{-K|E^-|}$$

or $E^- = E - E^+$ et E^+ représente les arcs dont les extrémités sont de même spin. Une configuration de spin peut donc se voir comme une coloration avec q couleurs et $|E^+|$ défauts. On peut donc réécrire la fonction de partition :

$$\begin{aligned} Z &= e^{-K|E|} \sum_{\sigma} e^{K|E^+|} \\ &= e^{-K|E|} \sum_{q\text{-coloration}} b_j(q) (e^K)^j \\ &= e^{-K|E|} B(G, q, e^K) \end{aligned}$$

avec $B(G, q, e^K)$ le polynôme chromatique. Or nous avons vu que le polynôme monochromatique est un invariant de Tutte-Grothendieck et

$$T(G, x, y) = \frac{1}{(y-1)^{|V|}(x-1)} B(G, (x-1)(y-1), y).$$

Ainsi l'évaluation du polynôme de Tutte sur l'hyperbole H_q fournit la fonction de partition du modèle de Potts. Le cas $q = 2$ se ramène au modèle d'Ising.

2.4 APPLICATIONS À LA THÉORIE DES NOEUDS

Nous allons voir que le polynôme de Tutte peut avoir certaines applications en théorie des noeuds.

2.4.1 Généralités

Un noeud est un plongement d'un cercle dans \mathbb{R}^3 . Par exemple, on peut considérer le noeud de trèfle est représenté par la figure 2.8. Ce noeud nous servira régulièrement d'exemple par la suite.

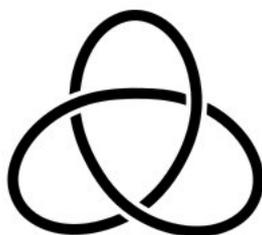


FIG. 2.8 – Le noeud de trèfle

Comme la représentation d'un noeud dans l'espace de dimension 3 n'est pas facile à se représenter, on considère la projection sur un plan. Ces projections doivent vérifier certaines conditions de régularité notamment que les tangentes en un point du noeud se projettent sur les droites du plan ou encore qu'il faut avoir un nombre fini de croisements. On appelle ces projections **diagrammes** de noeuds.

Un entrelacs est un plongement de plusieurs cercles dans \mathbb{R}^3 . L'exemple le plus connu est certainement l'entrelacs borroméen représenté par la figure 2.9.

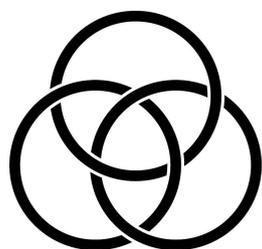


FIG. 2.9 – L'entrelacs borroméen

Formellement, on peut définir les entrelacs de la manière suivante :

Définition 2.4.1

On considère la variété différentiable obtenue en considérant l'union disjointe de n cercles S^1 . On appelle entrelacs à n composante l'image d'un plongement :

$$f : S^1 \sqcup S^1 \dots \sqcup S^1 \hookrightarrow \mathbb{R}^3$$

et on note $L = K_1 \sqcup K_2 \dots \sqcup K_n$. Les K_i représentent les composantes de l'entrelacs. Si $n = 1$, l'entrelacs est un noeud noté K .

La question naturelle qui se pose est de savoir si deux noeuds sont équivalents. On peut définir l'équivalence de deux noeuds en considérant les isotopies ambiantes entre deux noeuds, c'est-à-dire :

Définition 2.4.2

Deux entrelacs à n composantes sont isotopes s'il existe une application différentiable :

$$F : S^3 \times [0, 1] \rightarrow S^3$$
$$(x, t) \mapsto F_t(x)$$

telle que $F_0 = Id$ et $F_1(L) = L'$ et telle que F_t soit un difféomorphisme pour tout t vérifiant $F_t(K_i) = K'_i$.

C'est-à-dire que l'on a une famille de difféomorphismes préservant l'ordre des composantes de l'entrelacs.

Le théorème suivant, dû à Reidemeister, permet de caractériser facilement les entrelacs isotopes :

Théorème 2.4.1

Deux entrelacs sont isotopes si on peut transformer l'un des diagrammes en l'autre en utilisant un nombre fini de mouvements de Reidemeister (données par la figure 2.10).

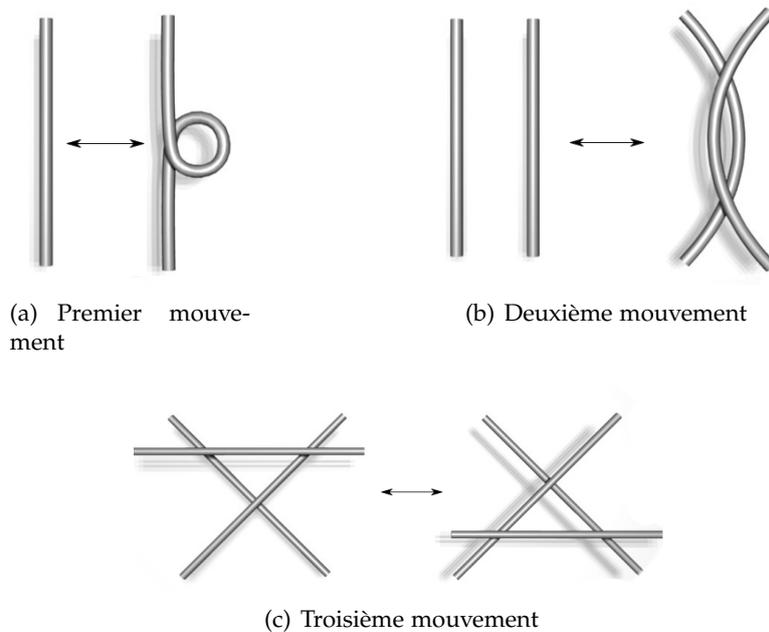


FIG. 2.10 – Mouvements de Reidemeister

Par simplicité, par la suite, on notera R_i et R'_i les diagrammes ci-dessus, correspondant aux i -ème mouvement de Reidemeister avec $i = \{1, 2, 3\}$.

2.4.2 Graphe médial et graphe signé d'un entrelacs

Graphes planaires et entrelacs entretiennent des relations très proches. Nous voyons ici comment construire un graphe à partir d'un diagramme d'entrelacs.

Par la suite, soit L un entrelacs et D son diagramme obtenu par projection régulière sur un plan. Un diagramme peut être considéré comme

un graphe planaire 4-régulier et donc ses faces sont 2-coloriables. Habituellement on utilise les couleurs noire et blanche et on colorie la face non-bornée en blanc.

Exemple : Une coloration du graphe du noeud de trèfle droit est donnée par la figure 2.11.

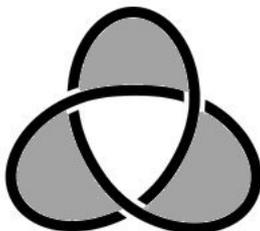


FIG. 2.11 – Coloration du diagramme du noeud de trèfle

Maintenant on considère uniquement les faces coloriées en noir. A chacune de ces faces, on associe un sommet. Deux sommets sont adjacents si et seulement si les faces noires sont adjacentes. On obtient un graphe nommé **graphe médial** associé au diagramme noté $M(L)$.

Exemple : Le graphe médial du noeud de trèfle droit est donné par la figure 2.12.

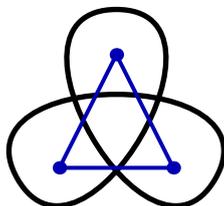


FIG. 2.12 – Graphe médial du noeud de trèfle $M(L)$

On peut maintenant associer un signe à chaque croisement selon la règle donnée par la figure 2.13.

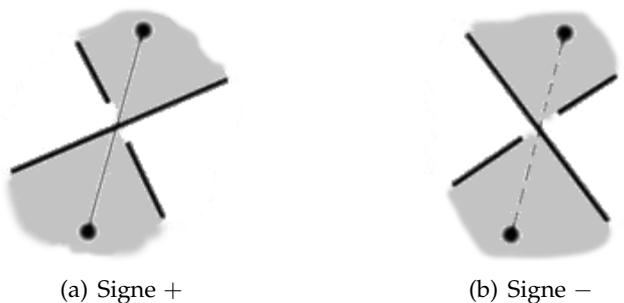


FIG. 2.13 – Signature des croisements

On obtient alors un graphe signé.

Exemple : Le graphe signé du noeud de trèfle droit est donné par la figure 2.14.

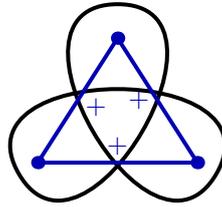


FIG. 2.14 – Graphe signé du noeud de trèfle droit

Remarque 2.4.1

Si le noeud est alterné, alors tous les arcs du graphe ont le même signe, ce qui est le cas du noeud de trèfle.

On définit maintenant un polynôme sur ces diagrammes :

Définition 2.4.3

Le crochet de Kauffman [D] d'un diagramme d'entrelacs définit par :

1. $[\bigcirc] = 1$,
2. $[D \sqcup \bigcirc] = d[D]$,
3. $[\times] = A[\nearrow] + B[\searrow]$.

Le crochet de Kauffman est clairement un polynôme en 3 variables A, B et d.

Exemple : Le crochet du noeud de trèfle droit vaut :

$$\begin{aligned} [\text{trèfle}] &= A^3 d^{(2-1)} + A^2 B d^{(1-1)} + A^2 B d^{(1-1)} + AB^2 d^{(2-1)} \\ &\quad + A^2 B d^{(1-1)} + AB^2 d^{(2-1)} + AB^2 d^{(2-1)} + B^3 d^{(3-1)} \\ &= A^3 d^1 + 3A^2 B + 3AB^2 d^1 + B^3 d^2. \end{aligned}$$

Néanmoins il est assez facile de montrer que ce n'est pas un invariant de noeud. En effet, ainsi défini, le crochet de Kauffman n'est pas invariant selon le second mouvement de Reidemeister. Une application directe de la définition du crochet à \approx montre que l'on a :

$$[\approx] = (A^2 + B^2 + ABd)[\searrow] + AB[\nearrow].$$

Or comme le second mouvement de Reidemeister impose que l'on ait $[\approx] = [\searrow]$, on pose :

$$AB = 1 \text{ et } A^2 + B^2 + ABd = 0,$$

c'est à dire :

$$B = A^{-1} \text{ et } d = -(A^2 + A^{-2}).$$

Ainsi on peut définir un nouveau crochet qui sera invariant pour le deuxième mouvement de Reidemeister.

On peut aussi montrer que le polynôme est invariant pour le troisième mouvement de Reidemeister. En effet les deux diagrammes du troisième mouvement (R_3 et R'_3) possèdent un croisement de type \times donc on peut écrire la relation 3) de la définition précédente sur ce croisement. Ensuite on applique le deuxième mouvement de Reidemeister sur la partie en A et on remarque que le développement est le même donc que les polynômes sont égaux : $[R_3] = [R'_3]$.

Malheureusement le crochet de Kauffman n'est toujours pas invariant pour le premier mouvement. Pour rendre le crochet invariant pour ce mouvement, nous avons besoin de définir une orientation sur les entrelacs. On définit donc une orientation sur chacune des composantes de l'entrelacs.

On a alors défini les diagrammes orientés selon la règle donnée par la figure 2.15.



FIG. 2.15 – Croisements dans un diagramme orienté

Ainsi on peut associer à chaque croisement d'un entrelacs orienté un signe : $+1$ si le croisement est de type L_+ et -1 s'il est de type L_- . On note $\omega(L)$ la somme des signes. La figure 2.16 donne les signes des croisements du noeud de trèfle orienté dans le sens des aiguilles d'une montre.

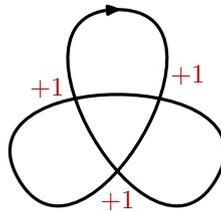


FIG. 2.16 – Noeud de trèfle droit orienté : $\omega(\text{trèfle}) = 3$

Proposition 2.4.1

$$f_D(A) = (-A^3)^{-\omega(D)} [D]$$

est invariant pour les trois mouvements de Reidemeister.

PREUVE. Comme $\omega(D)$ et $[D]$ sont invariants pour les mouvements deux et trois alors il en est de même pour $f_D(A)$.

On considère maintenant le premier mouvement de Reidemeister. Supposons que l'on ait un entrelacs L contenant un croisement de type R'_1 . On note L' l'entrelacs obtenu après avoir effectué le mouvement de Reidemeister. On note D et D' les diagrammes associés.

En écrivant la relation 3) du crochet de Kauffman sur le croisement \times de

R'_1 , on obtient :

$$\begin{aligned} [D] &= (A + A^{-1}(-A^2 - A^{-2}))[R_1] \\ &= -A^{-3}[D'] \end{aligned}$$

De plus $\omega(R'_1) = -1$ quel que soit l'orientation de R'_1 . On a que $\omega(D) = \omega(D') - 1$ et donc on a bien $f_D(A) = f_{D'}(A)$.

En fait, dans ce cas le polynôme de Kauffman s'identifie au polynôme de Jones $V_L(t)$ où $V_L(t)$ se définit de la manière suivante :

Définition 2.4.4

On appelle polynôme de Jones d'un entrelacs orienté L , le polynôme de Laurent en une variable $V_L(t)$ définie par :

1. $V_\circ(t) = 1$
2. la relation de Skein

$$\frac{1}{t}V_{L_+}(t) - tV_{L_-}(t) = \left(\sqrt{t} - \frac{1}{\sqrt{t}}\right)V_{L_0}(t).$$

Le polynôme de Jones est un invariant de noeud. On voit facilement que $f_D(t^{-1/4})$ vérifie ces conditions. De plus si l'on a un invariant défini sur une relation de type Skein et si l'on connaît sa valeur prise sur le noeud trivial alors l'invariant est uniquement déterminé, ce qui permet de relier le polynôme de Jones et le polynôme f précédent :

$$\begin{aligned} V_L(t) &= f_D(t^{-1/4}) \\ &= (-t)^{-3\omega(L)/4}[L]_{A=t^{-1/4}} \end{aligned}$$

La relation de Skein permet de calculer le polynôme de manière pratique. Par exemple le polynôme de Jones du noeud de trèfle droit est $V_{\text{trèfle}}(t) = t + t^3 - t^4$.

2.4.3 Mais où est passé le polynôme de Tutte ?

On veut maintenant interpréter la relation 3) du crochet de Kauffman en termes de graphe médial et de graphe signé. En effet le crochet de Kauffman étant bien défini sur les diagrammes, on peut alors le définir sur les graphes médiaux associés. On peut caractériser l'action de la relation 3) du crochet sur le graphe médial via la relation :

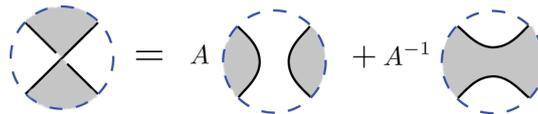


FIG. 2.17 – Relation de Kauffman et graphe médial

En notant G le graphe médial de L et e une arête de ce graphe, on peut traduire la relation suivante :

$$[G] = A[G - e] + A^{-1}[G/e]$$

lorsque le signe de e dans le graphe signé est $+$ et

$$[G] = A[G/e] + A^{-1}[G - e]$$

lorsque e est de signe $-$.

On a donc une décomposition de Tutte du graphe médial.

La décomposition en somme directe nécessaire pour introduire le polynôme, est bien moins traitée dans la littérature sur le sujet. Nous allons essayer de trouver une opération sur les noeuds qui corresponde à la somme directe des graphes médiaux.

Soit L un entrelacs On suppose que $M(L) = M(L_1) \oplus M(L_2)$ avec $M(L)$ le graphe médial associé à l'entrelacs L . On cherche à caractériser

Si $M(L_1)$ et $M(L_2)$ sont des composantes connexes différentes de $M(L)$ alors il suffit de considérer l'union disjointe des entrelacs associés à $M(L_1)$ et $M(L_2)$.

Sinon $M(L_1)$ et $M(L_2)$ partagent un point du graphe et alors on utilise la somme connexe de deux noeuds :

Définition 2.4.5

Comme en topologie algébrique, la somme connexe de deux noeuds s'obtient en considérant un ouvert sur chaque noeud et en identifiant les bords. On ajoute la condition que la somme connexe de deux noeuds ne change pas le nombre de croisements. Soient L_1 et L_2 deux noeuds. On note $L_1 \# L_2$ la somme connexe de ces deux noeuds. Si on a des entrelacs alors il faut spécifier les composantes que l'on relie.

Exemple : La somme connexe de deux noeuds (noeud de trèfle droit et noeud de huit) est donnée par la figure 2.18.

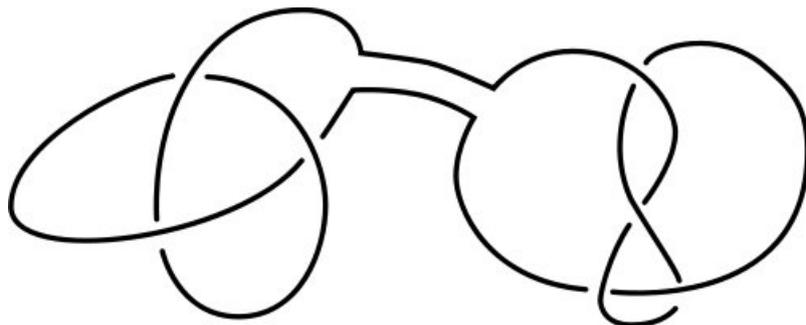


FIG. 2.18 – Somme connexe d'un noeud de trèfle et d'un noeud de huit

En terme de graphe médial, on a relié deux faces noires entre elles, c'est-à-dire que l'on a identifié deux sommets des graphes médiaux. Ainsi la décomposition en somme directe des graphes médiaux revient à décomposer un noeud en une somme de noeuds disjoints ou en somme connexe de plusieurs noeuds.

De plus, le crochet de Kauffman se comporte presque bien pour cette somme directe. On a par exemple $[\bigcirc \sqcup \bigcirc] = (-A^2 + -A^{-2})[\bigcirc] = (-A^2 + -A^{-2})$.

Cette quantité nous servira à normaliser le crochet de Kauffman des graphes médiaux à plusieurs composantes.

Plus généralement, nous avons la propriété suivante :

Proposition 2.4.2

Soit L_1 et L_2 deux entrelacs. On a

$$[L_1 \sqcup L_2] = (-A^2 + -A^{-2})[L_1] \cdot [L_2],$$

et

$$[L_1 \# L_2] = [L_1] \cdot [L_2],$$

On a par une récurrence immédiate

$$L_1 \sqcup L_2 \sqcup \dots \sqcup L_n = (-A^2 + -A^{-2})^{n-1} [L_1] \dots [L_n].$$

On peut donc normaliser le crochet de Kauffman par $(-A^2 + -A^{-2})^{n-1}$ où n représente le nombre de composantes de l'entrelacs, de manière à le rendre parfaitement compatible avec la somme directe des graphes médiaux.

Ce crochet de Kauffman normalisé est donc un invariant de Tutte-Grothendieck.

On a les relations :

$$[L^+] = -A^3 \text{ et } [L^-] = -A^{-3},$$

$$[C^+] = -A^{-3} \text{ et } [C^-] = -A^3,$$

où L^+ et L^- représentent le graphe composé d'une boucle et (respectivement) signé positivement et négativement. De même C^+ et C^- représentent les graphes signés composés d'un isthme.

On pose $|V|$ (resp. $|E|$) le nombre de sommets (resp. d'arêtes) du graphe médial $M(L)$ et $r(M)$ son rang. Si l'on se place dans un entrelacs alterné alors tous les arcs du graphe signé ont le même signe (on supposera positif dans ce cas) :

$$\begin{aligned} \frac{[L]}{(-A^2 + -A^{-2})^{n-1}} &= A^{|E|-r(M)} (A^{-1})^{r(M)} T(M(L), \frac{-A^{-3}}{-A}, \frac{-A^3}{A}) \\ &= A^{|E|-2r(M)} T(G, -A^{-4}, -A^4) \end{aligned}$$

or n est le nombre de composantes connexes de $M(G)$ donc $n = |V| - r(M)$. On en déduit que :

$$[L] = (-A^{-2} - A^2)^{|V|-r(M)-1} A^{|E|-2r(M)} T(G, -A^{-4}, -A^4)$$

Lorsque le graphe médial n'a qu'une seule composante connexe, on a $r(M) = |V| - 1$ et donc la relation :

$$[L] = A^{2|V|-|E|-2} T(M(L), -A^{-4}, -A^4).$$

On considèrera maintenant, pour simplifier, que l'on est dans le cas d'un graphe médial à une seule composante. Par suite, via le polynôme f , on peut exprimer le polynôme de Jones en fonction du polynôme de Tutte :

$$\begin{aligned} V_L(t) &= (-t)^{-3\omega(L)/4} (t^{-1/4})^{-2|V|+|E|-2} T(M(L), -t, -t^{-1}) \\ &= (-1)^{\omega(L)} (t^{-1/4})^{3\omega(L)-2|V|+|E|-2} T(M(L), -t, -t^{-1}) \end{aligned}$$

Exemple : Reprenons notre exemple du noeud de trèfle droit. C'est un noeud alterné et le polynôme de Tutte du graphe médial (Figure 2.12) est donné par $T(M(\textcircled{3}), x, y) = x^2 + x + y$ donc $T(M(\textcircled{3}), -t, -t^{-1}) = t^2 - t - t^{-1}$. On a $\omega = 3$ comme on l'a vu précédemment. On en déduit le polynôme de Jones $V_{\textcircled{3}}(t) = -1 \cdot t^2(t^2 - t - t^{-1}) = t + t^3 - t^4$.

L'évaluation du polynôme de Tutte sur l'hyperbole dégénérée $xy = 1$ se spécialise dans le polynôme de Jones. Le point $(-1, -1)$ du plan de Tutte appartient à cette hyperbole et à déjà été traité précédemment. Nous avons vu qu'il avait rapport avec la dimension de l'espace de bicycles d'un graphe. Lorsque G est planaire, on peut montrer que $T(G, -1, -1) = (-1)^{|E(G)|} (-2)^{\kappa(M(G))-1}$ avec $\kappa(M(G))$ le nombre de composantes connexes du graphe médial de G . Plus spécifiquement $V_L(1) = (-2)^{c(L)-1}$ où $c(L)$ est le nombre de composantes de L .

Au point 1, $V_L(1)$ admet une interprétation en terme d'invariant de Arf. L'invariant de Arf est un invariant de noeuds prenant les valeurs $+1$ ou -1 . En particulier l'invariant de Arf permet de distinguer le noeud trivial du noeud de trèfle et en définissant une relation d'équivalence appropriée, on peut se ramener à ces deux cas. De plus l'invariant de Arf a une interprétation en terme du polynôme de Jones :

$$Arf(L) = \frac{(V_L(-1))^2 - 1}{8} \pmod{2}$$

ou encore

$$Arf(L) = V_L(i).$$

C'est-à-dire qu'il existe une relation avec le nombre d'arbres couvrants du graphe médial donné par $T(G, 1, 1)$. En effet, en -1 , le polynôme de Jones correspond au polynôme d'Alexander-Conway : $V_L(-1) = \Delta_L(-1)$. Les relations entre les arbres couvrants et le polynôme d'Alexander-Conway sont développées dans (Mas01) et (Thi87).

Des relations entre le polynôme de Tutte et le polynôme de Homfly sont développées dans (Jae88) en utilisant une méthode similaire à celle utilisée ci-dessus pour le polynôme de Jones. Le polynôme de Homfly est un polynôme à deux variables et a des spécialisations contenant le polynôme de Jones et le polynôme d'Alexander-Conway.

2.5 ZONOTOPES ET THÉORIE D'ÉRHART

Nous nous intéressons maintenant à la théorie d'Ehrhart. Celle-ci s'intéresse à compter le nombre de points d'un réseau contenu dans un polytope.

Définition 2.5.1

Soit $V = (v_1, \dots, v_n)$ un sous-ensemble fini de l'espace euclidien \mathbb{R}^n . On appelle **polytope** l'enveloppe convexe de ce sous-espace, c'est à dire l'ensemble des combinaisons linéaires convexes :

$$\mathcal{P}(V) = \{x \in \mathbb{R}^n : x = \sum_i \lambda_i x_i, \sum_i \lambda_i = 1, \lambda_i \geq 0\}.$$

C'est un compact de \mathbb{R}^n formant le plus petit ensemble convexe de \mathbb{R}^n contenant V .

On remarque qu'il existe certains points ne pouvant s'écrire comme une combinaison linéaire stricte de points de V , c'est-à-dire s'il n'est à l'intérieur d'aucun segment strictement contenu dans \mathcal{P} . Ces points sont appelés **sommets** du polytope. On peut montrer ce résultat en utilisant le théorème de Carathéodory :

Théorème 2.5.1

Soit V un sous-ensemble de \mathbb{R}^n . Alors tout point de l'enveloppe convexe $\mathcal{P}(V)$ est dans l'enveloppe convexe d'un sous-ensemble de points affinement indépendants.

que ces points sont en nombre fini et correspondent aux points de V . Ainsi on a l'ensemble de cardinal minimal tel que l'enveloppe convexe soit \mathcal{P} .

On définit aussi les faces comme les sous-ensembles de \mathcal{P} formés par l'intersection de \mathcal{P} avec un hyperplan affine et tel que \mathcal{P} soit contenu entièrement dans l'un des deux demi-espaces formés par l'hyperplan.

On appelle **intérieur relatif** du polytope, l'intérieur du polytope dans l'espace affine qu'il engendre.

On considère le réseau $\mathbb{Z}^n \subset \mathbb{R}^n$. Étant donné un ensemble fini de points de \mathbb{Z}^n , on considère le polytope associé \mathcal{P} . On appelle un tel polytope un **polytope entier**.

Étant donné un polytope entier P , Ehrhart a étudié la fonction :

$$i_P : \mathbb{N} \rightarrow \mathbb{N}^* \\ q \mapsto |qP \cap \mathbb{Z}^n|$$

qui compte le nombre de points entiers dans le polytope dilaté d'un facteur m .

Son résultat principal est donné par le théorème suivant :

Théorème 2.5.2

i_P est une fonction polynômiale en q de degré n .

En fait seul le cas des simplexes est intéressant à étudier car il existe une décomposition d'un polytope en simplexe. Un simplexe de dimension r (ou r -simplexe) est un polytope associé à un ensemble de $r + 1$ points indépendants de \mathbb{R}^n . Un simplexe est donc un polytope avec $r + 1$ sommets. Par exemple, le simplexe de dimension 3 est le tétraèdre.

Proposition 2.5.1

Tout polytope \mathcal{P} peut se décomposer comme une réunion d'intérieurs relatifs de simplexes dont les sommets sont des points de \mathcal{P} .

Ehrhart a aussi introduit une deuxième fonction comptant le nombre de points contenu strictement à l'intérieur du polytope. Cette fonction est directement reliée au polynôme d'Ehrhart par la loi de réciprocité d'Ehrhart-MacDonald :

Proposition 2.5.2

Soit $k(P, q)$ le nombre de points du réseau contenu dans P^0 où P^0 correspond à l'intérieur de P . Alors

$$k(P, q) = (-1)^{\dim(P)} i(P, -q)$$

On restreint maintenant l'étude à des polytopes plus particuliers : les zonotopes.

Définition 2.5.2

Soient A et B deux ensembles d'un espace euclidien. On appelle somme de Minkowski de A et B et on note $A + B$:

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

Exemple : On considère la somme de Minkowski des ensembles $A = \{(0, 0), (-1, 1)\}$ et $B = \{(0, 0), (1, 1)\}$, ce qui donne l'ensemble

$$\{(0, 0), (-1, 1), (1, 1), (1, 2)\}.$$

Définition 2.5.3

Soit $V = \{v_1, \dots, v_k\}$ un ensemble fini d'éléments de \mathbb{R}^n . On appelle zonotope et on note $Z(V)$ le polytope formé par la somme de Minkowski des segments de droite fermés $L_i = \{x_i v_i \mid 0 \leq x_i \leq 1\}$:

$$Z(V) = \{\alpha_1 + \dots + \alpha_n \mid \alpha_1 \in L_1 \dots \alpha_n \in L_n\}.$$

Exemple : Si l'on considère les ensembles de l'exemple précédents qui sont deux segments de \mathbb{R}^2 , l'interprétation géométrique en terme de zonotopes donne la figure 2.20. Le quadrillage représente le réseau \mathbb{Z}^2 et dans la troisième sous-figure les points bleus représentent les points du réseau à l'intérieur de zonotope. Notons qu'il n'y a qu'un seul point strictement à l'intérieur de ce zonotope.

De la même manière que nous pouvions décomposer un polytope en simplexe, nous avons une décomposition d'un zonotope en cubes :

Définition 2.5.4

Étant donné un ensemble D de droites affines linéairements indépendantes. On appelle **cube semi-ouvert** et on note $C(D)$ la somme de Minkowski de ces demi-droites. Si on note ces droites sous la forme $\gamma_1 = \beta_1 - \alpha_1, \dots, \gamma_n = \beta_n - \alpha_n$ avec $\alpha_i, \beta_i \in \mathbb{R}^n$, alors :

$$C(D) = \{a_1 \alpha_1 + (1 - a_1) \beta_1 + \dots + a_n \alpha_n + (1 - a_n) \beta_n \mid 0 \leq a_i < 1\}.$$

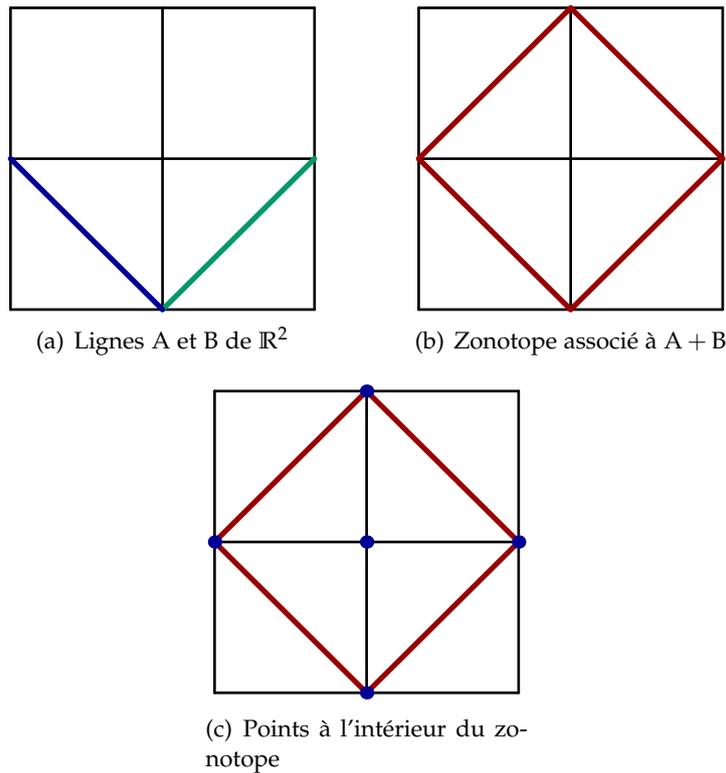


FIG. 2.19 – Exemple de zonotope dans \mathbb{R}^2

Les vecteurs γ_i sont appelés les vecteurs générateurs du cube. Si $n = 0$, l'ensemble des générateurs est vide. Notons que, quitte à traduire les vecteurs, on peut supposer que les segments de droite ont pour origine O .

Le lemme suivant donne la décomposition d'un zonotope en cubes semi-ouverts :

Proposition 2.5.3

Soit $\gamma_1, \dots, \gamma_r$ un ensemble de points de \mathbb{R}^n . On note L_i le segment de droite fermé reliant l'origine à γ_i . Alors $Z = Z(\gamma_1, \dots, \gamma_r)$ peut s'écrire comme réunion disjointe de cube semi-ouvert :

$$Z = \bigsqcup_X C_X,$$

où C_X est le cube semi-ouvert engendré par X et où X parcourt les sous-ensembles linéairement indépendants de $\{\gamma_1, \dots, \gamma_n\}$.

PREUVE. La preuve s'effectue par induction :

C'est clair lorsque $n = 0$, Z est alors réduit à un seul point (l'origine).

Supposons la propriété vraie au rang $r - 1$ alors on a une décomposition de $Z' = Z(L_1, \dots, L_{r-1})$ en cubes semi-ouverts :

$$Z' = \bigsqcup_X C_X,$$

où X parcourt les sous-ensembles linéairement indépendants de $\{\gamma_1, \dots, \gamma_{r-1}\}$.

On projette alors le zonotope Z sur un hyperplan orthogonal à L_r . On obtient alors un zonotope

$$\bar{Z} = \bigsqcup_{\bar{Y}} C_{\bar{Y}},$$

où \bar{Y} correspond aux projetés des sous-ensembles Y de $\{\gamma_1, \dots, \gamma_r\}$ tels que $Y \cup \{\gamma_r\}$ soit linéairement indépendant.

En revenant maintenant dans \mathbb{R}^n , chacun des $C_{\bar{Y}}$ s'écrit comme un produit $]0, \gamma_r] \times C_Y$. On a alors la décomposition de Z donnée par

$$Z = \left(\bigsqcup_X C_X \right) \cup \left(\bigsqcup_Y]0, \gamma_r] \times C_Y \right).$$

■

On notera que la nature inductive de cette preuve permet de trouver un algorithme de décomposition en cube semi-ouverts. On consultera (Cha92) pour plus de détails sur cette décomposition et sur la méthode.

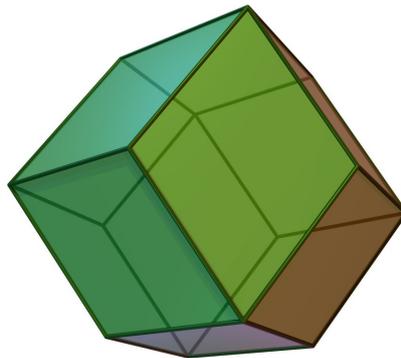


FIG. 2.20 – Exemple de zonotope dans \mathbb{R}^3

On remarque que si $\forall i, \gamma_i \in \mathbb{Z}^n$ alors les sommets de chaque C_X sont entiers. Cela va nous permettre de décomposer un zonotope en cubes entiers et de pouvoir chercher le polynôme d'Erhart uniquement sur les cubes semi-ouverts. C'est ce que fait la proposition suivante :

Théorème 2.5.3

Soit $\beta_1, \dots, \beta_r \in \mathbb{Z}^n$. On considère le zonotope entier $Z = Z(\beta_1, \dots, \beta_r)$. Alors la fonction d'Erhart s'écrit :

$$i(Z, q) = \sum_X h(X) q^{|X|},$$

où X parcourt les sous-ensembles linéairement indépendants de $\{\beta_1, \dots, \beta_r\}$ et où $h(X)$ dénote le pgcd des mineurs de taille $|X|$ de la matrice formée par les lignes β_i .

PREUVE. Par la proposition précédente, on peut décomposer notre zonotope en cubes :

$$Z = \bigsqcup_X C_X.$$

X parcourt les sous-ensembles indépendants de $\{\beta_1, \dots, \beta_r\}$. On note $X = \{\delta_1, \dots, \delta_s\}$ avec $s \leq r$. Par définition, C_X est engendré par $\pm\delta_1, \dots, \pm\delta_s$.

On considère désormais un tel cube C_Y associé à un ensemble $Y = \{\gamma_1, \dots, \gamma_s\}$. Si l'on considère l'ensemble des vecteurs entiers de l'espace vectoriel engendré par Y , ils forment un groupe abélien noté G . De plus comme les vecteurs γ_i sont aussi entiers, on peut considérer le sous-groupe de G engendré par la partie Y et noté H . Comme A est un groupe linéaire alors $h(Y) = [G : H]$ l'indice de H dans G (produit des k premiers facteurs invariants). De plus les éléments de $C \cap G$ forment une famille de représentants des classes de G (i.e. des orbites) pour l'action du sous-groupe H sur G car les générateurs de C sont entiers et linéairement indépendants, donc $|(C \cap G)|$ est égal au nombre d'orbites. Or les orbites pour l'action de H sur G forment une partition de G et les orbites sont toutes de cardinal $|H|$ (on a une bijection immédiate entre les éléments de gH avec $g \in G$ et ceux de H).

On en déduit que $|G| = |C \cap G||H|$. Par suite $i(Z, 1) = |(C \cap G)| = h(Y)$. En passant à l'échelle par un facteur q , on en déduit que

$$i(Z, q) = \sum_X i(C_X, q) = \sum_X h(X)q^{|X|}.$$

■

La matrice formée par les lignes β_i est une matrice à coefficients entiers. Maintenant si l'on se restreint à un cas bien particulier de matrice :

Définition 2.5.5

Une matrice à coefficients entiers est dite unimodulaire si son déterminant vaut ± 1 .

Définition 2.5.6

Une matrice à coefficients entiers est dite totalement unimodulaire si toute sous-matrice carrée inversible est unimodulaire.

Par exemple la matrice suivante est de ce type :

$$A = \begin{bmatrix} -1 & -1 & 0 & 0 & 0 & +1 \\ +1 & 0 & -1 & -1 & 0 & 0 \\ 0 & +1 & +1 & 0 & -1 & 0 \\ 0 & 0 & 0 & +1 & +1 & -1 \end{bmatrix}$$

Il est alors clair que tous les mineurs d'une matrice totalement unimodulaire sont 0 ou ± 1 . Dans ce cas, le coefficient du monôme q^i est égal au nombre de sous-ensembles linéairement indépendants de taille i parmi l'ensemble des générateurs. Si nous avons un matroïde \mathcal{M} représentable par une telle matrice totalement unimodulaire alors nous pouvons lui associer un zonotope formé par les lignes de la matrice. On note ce zonotope $Z(\mathcal{M})$. Ce type de matroïde est appelé **matroïde régulier**.

De plus il est immédiat de remarquer que le nombre de sous-ensembles linéairement indépendants de taille i est évaluable par le polynôme de Tutte comme nous l'avons vu précédemment.

On en déduit la proposition suivante :

Proposition 2.5.4

Soit \mathcal{M} un matroïde régulier et M sa représentation par une matrice totalement unimodulaire alors le polynôme d'Ehrhart associé au zonotope $Z(\mathcal{M})$ est donné par :

$$i(Z, q) = q^{r(\mathcal{M})} T\left(\mathcal{M}, 1 + \frac{1}{q}, 1\right).$$

On peut maintenant utiliser la loi de réciprocité d'Ehrhart-Macdonald. On suppose pour simplifier que la matrice a le même rang que l'espace \mathbb{R}^n dans lequel le zonotope vit. On a alors :

$$\begin{aligned} k(Z, q) &= (-1)^n i(Z, -q) = (-1)^n q^{r(\mathcal{M})} T\left(\mathcal{M}, 1 - \frac{1}{q}, 1\right) \\ &= (-q)^{r(\mathcal{M})} T\left(\mathcal{M}, 1 - \frac{1}{q}, 1\right) \end{aligned}$$

On a ainsi que $(-1)^{r(\mathcal{M})} T(\mathcal{M}, 0, 1)$ compte le nombre de points strictement à l'intérieur de $Z(\mathcal{M})$.

2.6 PHYSIQUE DU TAS DE SABLE ET JEUX COMBINATOIRES

Nous nous intéressons maintenant au modèle du tas de sable abélien. Ce modèle a été introduit dans les années 1980 pour introduire le concept d'états critiques auto-organisés. C'est un modèle où des perturbations locales du système peuvent engendrer une perturbation globale.

Nous allons dans un premier temps étudier un modèle combinatoire lié au tas de sable : le *chip-firing game*. Nous verrons ensuite la relation avec le modèle du tas de sable.

Dans le *chip-firing game*, on considère un graphe pointé (G, q) où q est un sommet quelconque. On définit une fonction de hauteur $\theta : V(G) \rightarrow \mathbb{Z}$ qui à chaque sommet v associe un entier $\theta(v) \geq 0$ pour tout sommet $v \neq q$ et $\theta(q) = -\sum_{v \neq q} \theta(v)$. On note $\text{indeg}(v)$ deux fois (on peut voir une boucle

comme un arc sortant et entrant) le nombre de boucles sur le sommet v et $\text{exdeg}(v)$ le nombre d'arcs incidents qui ne sont pas des boucles. On a bien $\text{deg}(v) = \text{indeg}(v) + \text{exdeg}(v)$. Le vecteur des hauteurs $\bar{\theta}$ est appelé la **configuration** du système. Ce vecteur décrit l'état global du système.

Un sommet $v \neq q$ est dit **prêt** lorsque $\theta(v) \geq \text{deg}(v)$. On dit que q est prêt uniquement dans le cas où aucun autre sommet ne l'est. Soit v un sommet prêt, on dit que le sommet v **tire** lorsque la configuration du système est réorganisée selon la règle :

$$\theta'(v) = \begin{cases} \theta(v) + v(v, w) & \text{si } v \neq w \\ \theta(v) - \text{exdeg}(v) & \text{sinon} \end{cases},$$

où $v(v, w)$ correspond au nombre d'arcs entre les sommets v et w . Autrement dit les vaisseaux se déplacent sur les sommets adjacents.

Après un tir, il peut se produire de nouveaux tirs car le mouvement des vaisseaux à pu amener de nouveaux sommets à être prêts. On considère donc une séquence de tirs successifs. Si l'on se donne une suite de sommets (v_1, \dots, v_k) . Cette suite est appelée **séquence q -valide** pour une configuration θ_1 si v_1 est prêt pour la configuration θ_1 et pour tout $2 \leq i \leq k$, v_i est prêt dans la configuration θ_i où θ_i est la configuration obtenue après le tir du sommet v dans la configuration θ_{i-1} . Intuitivement cela modélise le principe de causalité ; on a une succession de réorganisations du système dans le temps induit par les précédents.

On va maintenant caractériser les configurations :

Définition 2.6.1

Une configuration θ est dite **stable** si $\forall v \neq q, \theta(v) \leq \deg(v)$.

Certaines configurations peuvent réapparaître (considérer par exemple le graphe formé d'une seule boucle) :

Définition 2.6.2

On appelle configuration **récurrente** une configuration θ telle qu'il existe une séquence commençant et finissant par la configuration θ .

Définition 2.6.3

Une configuration stable et récurrente est dite **critique**. On définit alors son **niveau** par

$$level(\theta) = \sum_{v \neq q} \theta(v) - |E(G)| + \deg(q).$$

Les propositions suivantes sont démontrées dans (Big99), (AB91) et (Merg7), elles caractérisent les configurations critiques :

Proposition 2.6.1

Soit G un graphe connexe, $q \in V(G)$ et θ une configuration stable. Alors θ est une configuration critique si et seulement si il existe une séquence q -valide telle que chaque sommet tire exactement une fois.

De plus il est clair que si deux sommets sont prêts au même instant alors les opérations de tir commutent :

Lemme 2.6.1

Soit une séquence q -valide. Si deux éléments de cette séquence sont prêts au même instant, alors la séquence obtenue par permutation de ces deux éléments est aussi une séquence q -valide et la configuration finale est identique.

PREUVE. En effet on peut voir que si deux sommets sont prêts au même moment alors les opérations de tir commutent. Soit en effet deux sommets u et u' prêts après que q ait tiré et θ' (resp. θ'') la configuration après que u ait tiré suivi de u' (resp. u' suivi de u). Alors la configuration θ' est définie par :

$$\theta' = \begin{cases} \theta(v) + v(v, u) + v(v, u') & \text{si } v \neq u, u' \\ \theta(u) - exdeg(u) + v(u, u') & \text{si } v = u \\ \theta(u) + v(u, u') - exdeg(u') & \text{si } v = u' \end{cases}$$

On vérifie ensuite aisément que la configuration θ'' est identique. ■

On peut montrer que les niveaux des configurations critiques sont bornés par le nombre cyclotomique de G . En particulier, on a le théorème :

Théorème 2.6.1

Soit G un graphe connexe et θ une configuration critique alors

$$0 \leq \text{level}(\theta) \leq |E(G)| - |V(G)| + 1.$$

On peut donc considérer le nombre de configurations critiques de niveau i noté c_i et considérer la fonction génératrice :

$$P_q(G, y) = \sum_{i=0}^{|E(G)|-|V(G)|+1} c_i y^i.$$

On va montrer que ce polynôme est identifiable à une évaluation du polynôme de Tutte. Comme G est connexe et que l'on a affaire à des graphes pointés, nous utiliserons la définition récursive du polynôme de Tutte :

Théorème 2.6.2

Soit (G, q) un graphe pointé alors la série génératrice $P_q(G, y)$ vérifie :

$$P_q(G, y) = P_q(G - e, y) + P_q(G/e, y) \text{ si } e \text{ n'est ni une boucle ni un isthme.}$$

$$P_q(G/e, y) = P_q(G, y),$$

$$P_q(G - e, y) = yP(G - e, y).$$

De plus on a :

$$P_q(G, y) = T(G, 1, y).$$

PREUVE. Soit $e = (q, u)$ avec u un sommet adjacent à q dans G . On a trois cas possibles :

Si e est un isthme, soit θ' une configuration critique de G/e alors on définit une configuration θ de G par

$$\theta(v) = \begin{cases} \theta'(v), & \forall v \neq q, u \\ (\text{deg } u) - 1, & \text{si } v = u \\ \text{deg } q, & \text{si } v = q \end{cases}$$

Dans cette configuration, le sommet q tire en premier suivi du sommet u . De plus, comme θ' est critique dans G/e et après que q et u aient tirés on arrive dans la même configuration que celle de θ' car e est un isthme. On a donc construit une configuration critique de G à partir d'une configuration critique de G/e . Réciproquement, soit θ une configuration critique de G . On définit la configuration θ' sur G/e (le sommet u est identifié à q) par :

$$\theta'(v) = \begin{cases} \theta(v), & \forall v \neq q \\ \text{deg } q, & \text{si } v = q \end{cases}$$

Si l'on a une séquence critique de G , (q, u, v_1, \dots, v_k) alors la séquence (q, v_1, \dots, v_k) est une séquence critique de G/e . Par suite la configuration θ' est une configuration critique de G/e .

De plus, on a

$$\begin{aligned}
\text{level}(\theta') &= \left(\sum_{w \neq q, u} \theta'(w) \right) - |\mathbb{E}(G/e)| + \text{deg}_{G/e}(q) \\
&= \left(\sum_{w \neq q, u} \theta(w) \right) - (|\mathbb{E}(G)| - 1) + (\text{deg}_G(q) + \text{deg}_G(u) - 2) \\
&= \left(\sum_{w \neq q, u} \theta(w) \right) - |\mathbb{E}(G)| + \text{deg}_G(q) + \text{deg}_G(u) - 1 \\
&= \left(\sum_{w \neq q} \theta(w) \right) - |\mathbb{E}(G)| + \text{deg}_G(q) \\
&= \text{level}(\theta)
\end{aligned}$$

On a donc construit une bijection entre les configurations critiques de G et celles de G' qui préserve les niveaux des configurations. On en déduit

$$P_q(G, y) = P_q(G/e, y).$$

Si e est une boucle, alors il suffit de considérer la construction de θ' suivante :

$$\theta'(v) = \begin{cases} \theta'(v), & \forall v \neq q \\ \text{deg}_{G-e} v, & \text{si } v = q \end{cases}$$

et on a

$$\begin{aligned}
\text{level}(\theta') &= \left(\sum_{w \neq q, u} \theta'(w) \right) - |\mathbb{E}(G - e)| + \text{deg}_{G-e}(q) \\
&= \left(\sum_{w \neq q} \theta(w) \right) - (|\mathbb{E}(G)| - 1) + \text{deg}_{G-e}(q) \\
&= \left(\sum_{w \neq q} \theta(w) \right) - |\mathbb{E}(G)| + \text{deg}_G(q) - 1 \\
&= \text{level}(\theta) - 1
\end{aligned}$$

On en déduit que :

$$P_q(G, y) = yP_q(G - e, y).$$

Si e n'est une boucle ni un isthme On considère alors la partition des configurations critiques en posant \mathcal{A} l'ensemble des configurations critiques vérifiant $\theta(u) = \text{deg}(u) - 1$ et \mathcal{A}' celles ne le vérifiant pas.

On considère une configuration de \mathcal{A} . Alors on en déduit une configuration critique de G/e en posant :

$$\theta'(v) = \begin{cases} \theta'(v), & \forall v \neq q \\ \text{deg } v, & \text{si } v = q \end{cases}$$

Alors u est prêt après que q ait tiré donc quitte à permuter les sommets prêts à la seconde étape, on peut supposer que u est le deuxième élément de la séquence. Après que u ait tiré, on est dans une configuration similaire dans G et G/e . Or comme on a une configuration critique de G , on en déduit une configuration critique de G/e .

Réciproquement, étant donné une configuration critique θ' de G/e , on construit une configuration de G en posant :

$$\theta(v) = \begin{cases} \theta'(v), & \forall v \neq q, u \\ (\deg u) - 1, & \text{si } v = u \\ \deg q, & \text{si } v = q \end{cases}$$

Après que q ait tiré, $\theta(u) = \deg(u) - 1 + v(q, u)$. Ensuite, après que u ait tiré, $\theta(u) = \deg(u) - 1 + v(q, u) - \text{exdeg}(u)$. Après que les voisins de u aient tirés, on a que :

$$\begin{aligned} \theta(u) &= \deg(u) - 1 + v(q, u) - \text{exdeg}(u) + (\text{exdeg}(u) - v(q, u)) \\ &= \deg(u) - 1 \end{aligned}$$

donc la configuration est bien récurrente. De plus comme θ' est critique dans G/e , on en déduit que θ est critique dans G .

On a donc une bijection entre les configurations critiques de \mathcal{A} et celles de G/e . De plus on peut montrer (de la même manière que précédemment) que le niveau reste inchangé.

De la même manière, on établit une bijection entre les configurations de \mathcal{A}' et les configurations critiques de $G - e$ en posant :

$$\theta'(v) = \begin{cases} \theta'(v), & \forall v \neq q \end{cases}$$

Comme par hypothèse $\theta(u) < \deg(u) - 1$ toute séquence q -valide de $G - e$ est une séquence q -valide de G et réciproquement. Or comme

$$\begin{aligned} \text{level}(\theta) &= \sum_{v \neq q} \theta(v) - |\mathbb{E}(G)| + \deg_G(q) \\ &= \sum_{v \neq q} \theta'(v) - (|\mathbb{E}(G - e)| + 1) + (\deg_{G-e}(q) + 1) \\ &= \text{level}(\theta') \end{aligned}$$

On en déduit que l'on a une bijection entre les configurations de \mathcal{A}' et les configurations critiques $G - e$ conservant le niveau donc

$$P_q(G, y) = P_q(G - e, y) + P_q(G/e, y).$$

A partir de là il suffit de remarquer que $P_q(C, y) = 1$ car la seule configuration critique sur un graphe avec un seul isthme est la configuration telle que $\theta(u) = 0$, de niveau 0. De même $P_q(L, y) = y$ car la seule configuration critique est celle telle que $\theta(q) = 0$ de niveau 1. Puis comme G

est supposé connexe et $T(G, 1, y)$ et $P_q(G, y)$ suivent la même formule de récursion et prennent la même valeur sur C et L , on en déduit l'égalité :

$$T(G, 1, y) = P_q(G, y).$$

■

Ainsi le choix du sommet q est arbitraire ce qui n'était pas évident *à priori*. De plus si on considère l'interprétation du polynôme de Tutte en termes d'activité, cela signifie qu'il y a une bijection entre les configurations critiques et les bases d'activité extérieure i .

L'étude des configurations critiques révèle d'autres surprises. On peut par exemple munir l'ensemble des configurations récurrentes d'une structure de groupe abélien dont l'ordre correspond au nombre d'arbres couvrants de G . La loi de groupe est donnée en faisant la somme des fonctions de configuration et en éboulant la configuration $\theta + \theta'$. On peut, de même, munir l'ensemble des configurations critiques d'une telle loi. Ces aspects sont développés dans (Big99).

En fait le modèle du tas de sable est un modèle plus général. De la même manière que le *chip-firing game*, on considère un ensemble de sites pondérés par une fonction de hauteur. On a aussi une borne sur cette fonction de hauteur. Néanmoins la réorganisation du système lorsqu'un site est prêt suit la règle :

$$\theta'(v) = \theta(v) - \Delta_{ij},$$

où (Δ_{ij}) est une matrice à coefficients entiers satisfaisant

$$\Delta_{ii} > 0, \Delta_{ij} \leq 0, s_i = \sum_j \Delta_{ij} \geq 0$$

et où s_i est appelé la dissipation du site i . Un site i est dit non-dissipatif si $s_i = 0$.

Une succession de réarrangements est appelée un **éboulement**. Ainsi on peut voir la hauteur d'un site comme un nombre de grains de sable. Lorsque le nombre de grains sur un site est trop grand alors il se produit un éboulement. Lorsque le système est dans une configuration stable alors le nombre de grains de sable augmente.

Le modèle du *chip-firing game* se réduit à ce modèle en considérant un sommet associé à chaque site. On dispose donc d'un graphe à N sommets. Le site 0 va correspondre au sommet spécial q du modèle du *chip-firing game*. On construit les arcs du graphe en plaçant $|\Delta_{ij}|$ éléments parallèles entre les sommets i et j ($i, j \neq 0$). On relie le sommet 0 au sommet i en utilisant $|\sum_{j=1}^N \Delta_{ij}|$ arcs en parallèle. On pose aussi $\Delta_{ij} = \Delta_{ji}$, c'est-à-dire que la matrice est symétrique.

Le tir du sommet 0 correspond à ajouter des grains de sable et n'est utilisé que dans le cas d'une configuration stable.

Nous avons vu que les séquences critiques dans le *chip-firing game* étaient finies et correspondaient à une suite de tirs où chaque sommet tirait une

et une seule fois. Le problème avec le modèle du tas de sable est que les séquences peuvent être infinies. Ce problème peut être résolu en considérant que l'ajout de grain de sable au site i est égal à la dissipation du site i .

2.7 APPLICATIONS À LA THÉORIE DES CODES

Nous allons voir une dernière application du polynôme de Tutte à la théorie des codes correcteurs. Les codes correcteurs sont utilisés en informatique pour détecter et éventuellement corriger des erreurs dans une transmission d'informations.

2.7.1 Généralités

De manière très générale, pour définir un code correcteur, nous avons besoin de définir un alphabet, c'est à dire un ensemble fini A , et d'un entier n . Nous considérons alors les mots de taille n sur l'alphabet A .

Étant données deux suites $a = (a_1, \dots, a_n)$ et $b = (b_1, \dots, b_n)$ nous pouvons définir une notion de distance entre ces deux mots :

$$d(a, b) = |\{i : 1 \leq i \leq n, a_i \neq b_i\}|.$$

Cette distance est appelée **distance de Hamming** entre a et b .

Nous étudierons plus spécifiquement une catégorie bien particulière de codes correcteurs : les codes linéaires.

On se donne alors comme alphabet un corps \mathbb{F} . Les mots sont alors des éléments de \mathbb{F}^n . On appelle **code** un ensemble de mots (c'est à dire un sous-ensemble de \mathbb{F}^n) contenant au moins deux mots.

Définition 2.7.1

*Un code est dit **linéaire** sur le corps \mathbb{F} si c'est un sous-espace vectoriel de \mathbb{F}^n .*

Ainsi, de manière compacte, nous pouvons considérer un code comme une matrice G en se fixant une base. Cette matrice est dimension $k \times n$ où k est la dimension du code et n la dimension de l'espace vectoriel. Les lignes de la matrices forment donc une base du code :

$$C = \{xG \mid x \in \mathbb{F}^k\}.$$

On appelle cette matrice **matrice génératrice** du code.

Une deuxième manière de définir un code est de le faire via sa **matrice de contrôle** H . Le code étant un sous-espace vectoriel de dimension k , il existe une application linéaire surjective de \mathbb{F}^n dans un espace de dimension $n - k$ ayant pour noyau le code :

$$C = \{c \in \mathbb{F}^n \mid c^t H = 0\}.$$

On définit maintenant le code dual :

Définition 2.7.2

Soit C un code. On appelle **code dual** de C et on note C^\perp l'ensemble :

$$C^\perp = \{x \in \mathbb{F}^n \mid x \cdot c = 0 \forall c \in C\}.$$

Il est clair que ma matrice génératrice de C correspond à la matrice de contrôle de C^\perp et vice versa.

Exemple : On considère le code linéaire sur \mathbb{F}_2^3 (code binaire) donné par la matrice sous forme standard :

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Si l'on veut transmettre un mot (a, b) , on calcule : $(a, b)M = (a, b, a + b)$. Comme la matrice est sous forme standard, on remarque bien que les deux premières lettres sont le message et que la redondance est $a + b$. Les mots de ce code sont $\{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$.

Définition 2.7.3

Lorsque la matrice génératrice d'un code $C \subset \mathbb{F}^k$ est de la forme $(Id_k \ B)$ où Id_k est la matrice identité de taille $k \times k$ et B une matrice de taille $k \times (n - k)$, on dit que la matrice génératrice est sous forme **standard**.

On peut toujours se ramener à une matrice de ce type par opération sur les lignes et les colonnes quitte à considérer un code **monomialement équivalent**. En effet les opérations sur les lignes ne changent pas le code mais celles sur les colonnes changent la structure du code mais pas ses caractéristiques (dimension, polynôme énumérateur des poids, distance minimale, etc.) Cette forme est particulièrement utile car les k premiers éléments correspondent alors au message et les $n - k$ à la partie redondante du message. Dans les preuves utilisant les matrices génératrices, nous considérerons uniquement des matrices sous cette forme.

On peut trouver une relation entre la matrice génératrice du code C et la matrice génératrice de son dual :

Proposition 2.7.1

Si la matrice génératrice du code C est sous forme standard $M = (Id_k \ B)$ alors la matrice du code dual est de la forme :

$$M' = \begin{pmatrix} -{}^tB \\ I_{n-k} \end{pmatrix}.$$

PREUVE. Il est clair que $M {}^tM' = 0$ donc les colonnes de ${}^tM'$ engendrent le noyau de l'application linéaire associé à M . De plus comme G est de rang k et que ${}^tM'$ est de rang $n - k$ alors les colonnes forment une base de ce noyau. ■

Une grandeur importante est donnée par la **distance minimale** :

$$d_m = \inf_{\substack{u, v \in C \\ u \neq v}} d(u, v).$$

La distance minimale permet de caractériser les codes linéaires :

Théorème 2.7.1

Un code linéaire \mathcal{C} de distance minimale d_m peut :

- détecter au plus $d_m - 1$ erreurs
- corriger au plus $\left\lfloor \frac{d_m - 1}{2} \right\rfloor$ erreurs avec $[x]$ la partie entière de x .

La figure 2.21 illustre ce théorème. Les points noirs sont des mots du code et les points de couleur des mots reçus. La métrique de cette figure est donnée par la distance de Hamming. Lorsqu'un mot reçu appartient à l'intérieur de la boule en pointillés alors les erreurs peuvent être corrigées (points verts). S'ils se trouvent à l'extérieur de la boule en pointillés mais à l'intérieur de la boule en trait continu, ils s'est produit moins de $d_m - 1$ erreurs. Ces erreurs sont détectées mais ne peuvent être corrigées (points bleus) S'ils se trouvent à l'extérieur de toutes les boucles, on ne peut ni détecter ni corriger les erreurs (points rouges).

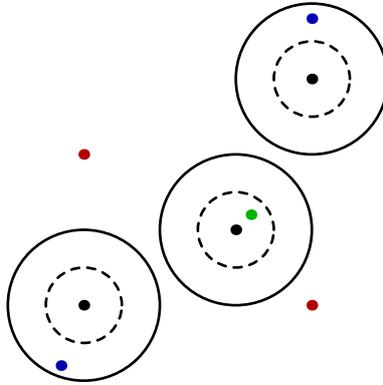


FIG. 2.21 – Distance minimale et code correcteur

Notation 2.7.1

On notera par $\mathcal{C}(n, k, d_m)$ le code linéaire sur l'espace \mathbb{F}^n de taille k et de distance minimale d_m .

Lorsque \mathbb{F} est fini alors on peut définir deux polynômes :

Définition 2.7.4

Soit \mathcal{C} un code linéaire sur un corps fini. On appelle **polynôme énumérateur des poids** le polynôme de $\mathbb{Z}[z]$ défini par

$$W_{\mathcal{C}}(z) = \sum_{c \in \mathcal{C}} z^{wt(c)} = \sum_{i=0}^n a_i z^i$$

où a_i est le nombre de mots du code \mathcal{C} de poids i et $wt(c) = d(c, 0)$ est appelé le **poids** du mot et correspond au nombre de coordonnées non-nulles du vecteur c .

Parfois on rencontrera le polynôme sous une forme à deux variables :

Définition 2.7.5

Soit \mathcal{C} un code linéaire sur un corps fini. On appelle **polynôme énumérateur des poids homogène** le polynôme de $\mathbb{Z}[x, y]$ défini par

$$W_{\mathcal{C}}(x, y) = \sum_{c \in \mathcal{C}} x^{n-wt(c)} y^{wt(c)} = \sum_{i=0}^n a_i x^{n-i} y^i$$

où a_i est le nombre de mots du code C de poids i .

En fait ces deux polynômes sont reliés simplement par la relation :

$$W_C(x, y) = x^n W_C\left(\frac{y}{x}\right).$$

Exemple : Le polynôme énumérateur des poids homogène de l'exemple donné dans le début du chapitre est :

$$W(x, y) = y^2 + 3x^2$$

2.7.2 Matroïdes et codes correcteurs

Soit C un code linéaire sur un corps \mathbb{F} et M sa matrice génératrice. On peut naturellement lui associer un matroïde engendré par les lignes de la matrice M .

On en déduit immédiatement la proposition suivante :

Proposition 2.7.2

Si le matroïde \mathcal{M} correspond à un code C alors le matroïde dual \mathcal{M}^ correspond au matroïde du code dual C^* .*

PREUVE. Si la matrice génératrice du code est de la forme $(I_k \ B)$ où I_k est la matrice identité de taille $k \times k$ alors le code dual est représenté par la matrice génératrice $\begin{pmatrix} -{}^t B \\ I_{n-k} \end{pmatrix}$ de même que pour le matroïde dual \mathcal{M}^* . ■

La proposition suivante relie le polynôme énumérateur des poids homogène au polynôme de Tutte :

Proposition 2.7.3

Soit C un code sur un corps fini à q éléments où q est une puissance d'un nombre premier et \mathcal{M} le matroïde linéaire associé au code. Alors on a

$$W_C(x, y) = y^{n-\dim(C)} (x-y)^{\dim(C)} T\left(\mathcal{M}, \frac{x+(q-1)y}{x-y}, \frac{x}{y}\right).$$

Pour pouvoir faire la preuve nous avons besoin de trouver des analogues aux boucles, co-boucles ainsi qu'aux opérations de contraction, suppression et de somme directe.

On peut construire la somme directe de matroïdes associés à des configurations de vecteurs de la manière vue au chapitre précédent. En particulier pour les codes linéaires, soient $\mathcal{C}_1 = (n_1, k_1, d_1)$ et $\mathcal{C}_2 = (n_2, k_2, d_2)$ deux codes linéaires. On peut définir la somme directe de ces deux codes comme le code $\mathcal{C} = (n_1 + n_2, k_1 \cdot k_2, \min(d_1, d_2))$. Les mots de ces codes peuvent s'écrire comme un vecteur $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ où c_1 est un vecteur correspondant à un mot du code \mathcal{C}_1 et c_2 un vecteur d'un mot du code \mathcal{C}_2 . Il est facile de voir que les matroïdes associés aux codes sont en somme directe si et seulement si les codes sont en somme directe dans le sens donné ci-dessus.

Une boucle du matroïde est décrite dans la matrice génératrice d'un code comme une coordonnée valant 0 partout. En effet un tel élément n'appartient bien à aucune base du matroïde. De même une co-boucle est un élément appartenant à toutes les bases. On peut se ramener, par opération sur les lignes, à une matrice de la forme :

$$\begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ & & & 0 & & & \\ & M_1 & & \vdots & & M_2 & \\ & & & 0 & & & \end{pmatrix}$$

Il est clair qu'un tel élément appartient à toutes les bases.

L'opération de suppression d'un élément i d'un matroïde associé à un code correspond à supprimer toutes les coordonnées en i -ème position dans ce code. L'opération de contraction consiste à considérer le sous-code engendré par les éléments dont la i -ème coordonnée est 0 et à supprimer la i -ème position de ce sous-code.

Pour l'opération de suppression la preuve que $\mathcal{M}(\mathcal{C} - e) \simeq \mathcal{M}(\mathcal{C}) - e$ est immédiate. Pour l'opération de contraction cela l'est moins. On montre la propriété suivante :

Proposition 2.7.4

Si on note \mathcal{C}/i l'opération de contraction dans un code décrite ci-dessus, alors

$$\mathcal{M}(\mathcal{C}/i) \simeq \mathcal{M}(\mathcal{C})/i.$$

PREUVE. Soit M la matrice génératrice de \mathcal{C} . Si i est une boucle alors les opérations de suppression et de contraction sont les mêmes et

$$\mathcal{M}(\mathcal{C} - i) \simeq \mathcal{M}(\mathcal{C}/i) \simeq \mathcal{M}(\mathcal{C})/i.$$

Si i n'est pas une boucle, par opérations sur les lignes, on peut supposer que la coordonnée $(1, i)$ de la première ligne et de la i -ème colonne vaut 0. et que les $k - 1$ lignes restantes forment une matrice génératrice A du code \mathcal{C}/i . Par suite le rang du matroïde $\mathcal{M}(\mathcal{C}/i)$ peut s'écrire $r(A \cup i) - 1$. Donc $A \cup i$ est un indépendant de $\mathcal{M}(\mathcal{C})$ si et seulement si c'est un indépendant de $\mathcal{M}(\mathcal{C}/i)$. Par suite

$$\mathcal{M}(\mathcal{C}/i) \simeq \mathcal{M}(\mathcal{C})/i.$$

■

On peut maintenant donner la preuve de la proposition précédente :

PREUVE. Par définition, on a :

$$W_{\mathcal{C}_1 \oplus \mathcal{C}_2}(x, y) = \sum_{i=0}^{n_1+n_2} a_i x^{n_1+n_2-i} y^i.$$

Or, au vu de la construction de la somme directe de deux codes, si on considère les mots de $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ de poids i (c'est-à-dire ceux dont le nombre de coordonnées différentes de 0 vaut i) alors ils peuvent être obtenu grâce à un mot de \mathcal{C}_1 de poids j et un mot \mathcal{C}_2 de poids k tels que

$j + k = i$. On note alors a_j (resp. a_k) le nombre de mots de poids j (resp. k) du code \mathcal{C}_1 (resp. \mathcal{C}_2). On a :

$$\begin{aligned}
W_{\mathcal{C}_1 \oplus \mathcal{C}_2}(x, y) &= \sum_{i=0}^{n_1+n_2} a_i x^{n_1+n_2-i} y^i \\
&= \sum_{i=0}^{n_1+n_2} \left(\sum_{j+k=i} a_j a_k \right) x^{n_1+n_2-j-k} y^{j+k} \\
&= \left(\sum_{j=0}^{n_1} a_j x^{n_1-j} y^j \right) \cdot \left(\sum_{k=0}^{n_2} a_k x^{n_2-k} y^k \right) \\
&= W_{\mathcal{C}_1}(x, y) W_{\mathcal{C}_2}(x, y)
\end{aligned}$$

On montre maintenant que le polynôme énumérateur des poids est un invariant pour la décomposition de Tutte. Soit e un élément qui ne soit ni une boucle ni un isthme. On partitionne le polynôme $W_{\mathcal{C}}(x, y)$ en considérant $W_1(x, y)$ (resp. $W_2(x, y)$) la somme des termes de $W_{\mathcal{C}}(x, y)$ correspondant aux mots tel que la e coordonnée vaille 0 (resp. $\neq 0$). Par construction, on a $W_{\mathcal{C}}(x, y) = W_1(x, y) + W_2(x, y)$. De plus $W_{\mathcal{C}-e}(x, y) = \frac{W_1(x, y)}{x} + \frac{W_2(x, y)}{y}$ et $W_{\mathcal{C}/e}(x, y) = \frac{W_1(x, y)}{x}$.

On en déduit

$$\begin{aligned}
W_{\mathcal{C}}(x, y) &= W_1(x, y) + W_2(x, y) \\
&= xW_{\mathcal{C}/e}(x, y) + yW_{\mathcal{C}-e}(x, y) - y \frac{W_1(x, y)}{x} \\
&= xW_{\mathcal{C}/e}(x, y) + yW_{\mathcal{C}-e}(x, y) - yW_{\mathcal{C}/e}(x, y) \\
&= yW_{\mathcal{C}-e}(x, y) + (x - y)W_{\mathcal{C}/e}(x, y)
\end{aligned}$$

On a donc un invariant de Tutte-Grothendieck.

De plus si l'on considère le code L constitué d'une seule boucle, ce code est de dimension 1 et sa matrice génératrice n'a que des zéros. Le code est alors constitué d'un unique mot de poids 0. On en déduit

$$W_L(x, y) = X.$$

De même si l'on considère le code L constitué d'un seul isthme, ce code est de dimension 1 et sa matrice génératrice comporte une seule ligne constituée de zéros sauf à la i -ème position où c'est un 1. Ce code contient $p - 1$ éléments de poids 1 et un élément de poids 0 donc

$$W_{\mathcal{C}}(x, y) = X + (q - 1)Y.$$

Comme $\dim(\mathcal{C}) = r(M)$, on a

$$W_{\mathcal{C}}(x, y) = y^{n-\dim(\mathcal{C})} (x - y)^{\dim(\mathcal{C})} \mathbb{T} \left(\mathcal{M}, \frac{x + (q - 1)y}{x - y}, \frac{x}{y} \right).$$

■

On remarque aussi qu'en posant $X = \frac{x+(q-1)y}{x-y}$ et $Y = \frac{x}{y}$, alors

$$(X - 1)(Y - 1) = q.$$

Ainsi l'évaluation du polynôme énumérateur des poids correspond à évaluer le polynôme de Tutte sur l'hyperbole H_p où q est une puissance d'un nombre premier. Nous avons déjà rencontré cette hyperbole en physique statistique avec le modèle de Potts et dans les graphes avec le polynôme monochromatique.

Ce résultat permet de donner une démonstration combinatoire du théorème de MacWilliams. Ce théorème relie le polynôme énumérateur des poids d'un code avec celui de son dual :

Théorème 2.7.2

Soit \mathcal{C} un code sur un \mathbb{F}_q -espace vectoriel de dimension n alors

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (p-1)y, x - y).$$

PREUVE. Le code dual a pour dimension $n - \dim(\mathcal{C})$ et son matroïde associé correspond à \mathcal{M}^* . On a

$$W_{\mathcal{C}^\perp}(x, y) = y^{\dim(\mathcal{C})} (x - y)^{n - \dim(\mathcal{C})} \mathbb{T} \left(\mathcal{M}, \frac{x}{y}, \frac{x + (p-1)y}{x - y} \right).$$

D'un autre coté

$$\begin{aligned} \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (p-1)y, x - y) &= \\ &= \frac{1}{p^{\dim(\mathcal{C})}} (x - y)^{n - \dim(\mathcal{C})} (py)^{\dim(\mathcal{C})} \mathbb{T} \left(\mathcal{M}, \frac{px}{py}, \frac{x + (p-1)y}{x - y} \right) \\ &= y^{\dim(\mathcal{C})} (x - y)^{n - \dim(\mathcal{C})} \mathbb{T} \left(\mathcal{M}, \frac{x}{y}, \frac{x + (p-1)y}{x - y} \right) \end{aligned}$$

On en déduit donc l'égalité. ■

Nous donnons maintenant une autre manière de démontrer le résultat sur le polynôme de Tutte, sans utiliser les invariants de Tutte-Grothendieck. La méthode a été développée dans (Ardo7) et pour un cas plus général dans (MB05).

Soit $\mathcal{C} \subset \mathbb{F}_q^n$ un code linéaire. On peut voir les colonnes de la matrice génératrice comme un arrangement de n hyperplans dans \mathbb{F}_q^n dont les vecteurs normaux sont donnés par les colonnes de la matrice génératrice. On note H_1, \dots, H_n ces hyperplans de vecteurs normaux v_1, \dots, v_n . Cet arrangement d'hyperplan est central.

On remarque que si un mot c de \mathcal{C} a sa i -ème coordonnée nulle alors $c - v_i = 0$ donc $c \in H_i$. Donc pour chaque coordonnée nulle, un mot du code appartient à un hyperplan. On en déduit une bijection entre \mathbb{F}_q^n et \mathcal{C} donnée par la fonction :

$$\begin{aligned} \phi : \mathbb{F}_q^n &\rightarrow \mathcal{C} \\ (p_1, \dots, p_n) &\mapsto p_1 v_1 + \dots + p_n v_n \end{aligned}$$

Exemple : La figure 2.22 montre la configuration d'hyperplans de l'exemple du début. Les hyperplans sont définis par les équations $x = 0$, $y = 0$ et $x + y = 0$.

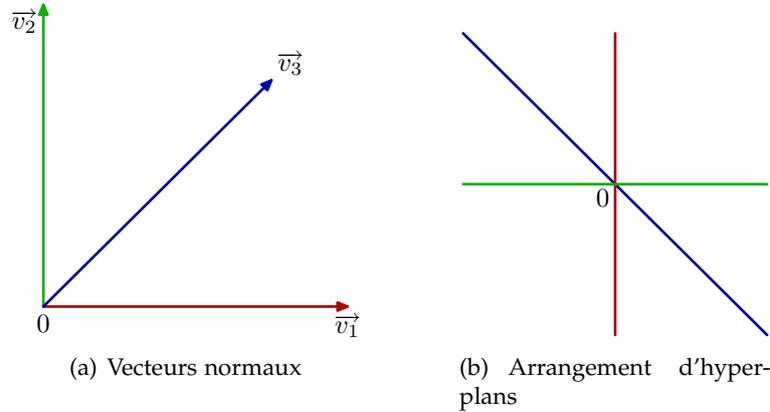


FIG. 2.22 – Arrangement d'hyperplan associé à un code

On peut ensuite réexprimer le poids d'un mot en fonction du nombre $h(c)$ d'hyperplans auquel il appartient et on en déduit :

$$\text{wt}(c) = \text{nombre de coordonnées non nulles de } c = n - h(c).$$

On en déduit :

$$\begin{aligned} W_{\mathcal{C}}(x, y) &= \sum_{c \in \mathcal{C}} x^{n-\text{wt}(c)} y^{\text{wt}(c)} \\ &= \sum_{c \in \mathbb{F}_q^n} x^{h(c)} y^{n-h(c)} \\ &= y^n \sum_{c \in \mathbb{F}_q^n} \left(\frac{x}{y} \right)^{h(c)} \end{aligned}$$

On peut maintenant utiliser la méthode du corps fini pour calculer cette fonction. La méthode du corps fini a été développée pour calculer le polynôme du cobord (*coboundary polynomial*) et le polynôme caractéristique d'un arrangement d'hyperplans de \mathbb{R}^n .

A tout arrangement d'hyperplans \mathcal{A} de \mathbb{R}^n , on peut lui associer un arrangement \mathcal{A}_q de \mathbb{F}_q^n en considérant l'arrangement induit par les équations réduites dans \mathbb{F}_q des équations définissant \mathcal{A} dans \mathbb{R}^n . On a ensuite le théorème suivant :

Théorème 2.7.3

Soit \mathcal{A} un arrangement d'hyperplans dans \mathbb{R}^n . Soit q une puissance d'un nombre premier assez grande pour que $\mathcal{A} \simeq \mathcal{A}_q$ où \mathcal{A}_q est l'arrangement induit dans \mathbb{F}_q^n . Alors

$$\bar{\chi}_{\mathcal{A}}(q, t) = \sum_{p \in \mathbb{F}_q^n} t^{h(p)},$$

où $h(p)$ correspond au nombre d'hyperplans de \mathcal{A}_q contenant p .

Ce théorème est démontré dans (Ardo7).

$\bar{\chi}_{\mathcal{A}}(q, t)$ est le polynôme du cobord défini pour un arrangement \mathcal{A} par

$$\bar{\chi}_{\mathcal{A}}(q, t) = \sum_{\substack{\mathcal{B} \subseteq \mathcal{A} \\ \text{central}}} q^{r(\mathcal{A})-r(\mathcal{B})} (t-1)^{|\mathcal{B}|},$$

où r est la fonction de rang de l'arrangement.

Dans notre cas comme l'arrangement est central, on vérifie sans effort que l'on peut exprimer le polynôme du cobord d'un arrangement central en terme de polynôme de Tutte du matroïde associé à cet arrangement :

$$\bar{\chi}_{\mathcal{A}}(q, t) = (t-1)^{r(\mathcal{M}_{\mathcal{A}})} \mathrm{T} \left(\mathcal{M}_{\mathcal{A}}, \frac{q+t-1}{t-1}, t \right)$$

et

$$\mathrm{T}(\mathcal{M}_{\mathcal{A}}, x, y) = \frac{1}{(y-1)^{r(\mathcal{M}_{\mathcal{A}})}} \bar{\chi}_{\mathcal{A}}((x-1)(y-1), y).$$

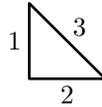
On en déduit finalement :

$$\begin{aligned} y^n \sum_{c \in \mathbb{F}_q^n} \left(\frac{x}{y} \right)^{h(c)} &= y^n \bar{\chi}_{\mathcal{A}}(q, \frac{x}{y}) \\ &= y^n \left(\frac{x}{y} - 1 \right)^{r(\mathcal{M})} \mathrm{T} \left(\mathcal{M}, \frac{q + x/y - 1}{x/y - 1}, \frac{x}{y} \right) \\ &= y^{n-r(\mathcal{M})} (x-y)^{r(\mathcal{M})} \mathrm{T} \left(\mathcal{M}, \frac{x + (q-1)y}{x-y}, \frac{x}{y} \right) \end{aligned}$$

Ce qui est le résultat attendu.

Nous pouvons aussi interpréter ce résultat dans le contexte des matroïdes graphique. On se place sur le corps \mathbb{F}_2 . Alors on peut interpréter les colonnes de la matrice génératrice comme des arcs dans un graphe.

Exemple : Le graphe associé à la matrice de notre exemple est donné par la figure suivante où les arcs 1, 2 et 3 correspondent aux colonnes respectives de la matrice $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.



Cette interprétation permet de faire le lien avec la fonction de partition du modèle de Potts et avec le polynôme monochromatique sur les hyperboles H_q .

CONCLUSION

Nous avons étudié des domaines d'applications assez variés du polynôme de Tutte. Par ce fait nous avons aperçu que la structure de matroïde pouvait être présente (de manière sous-jacente) dans des structures et des domaines très différents.

Certaines applications n'ont pas été incluses dans ce mémoire, par faute de temps pour les étudier ou les rédiger.

Il en est par exemple d'une généralisation du modèle de Potts dans le cas ferromagnétique : le modèle des amas aléatoire (*random cluster model*) dont l'étude mène à la théorie de la percolation en physique. Ou encore le nombre de pavage d'un rectangle par des *tetromino* et la couverture d'un graphe par des griffes (*claw covering*) qui s'avère être une évaluation du polynôme de Tutte au point $(3,3)$. Cela peut ensuite se généraliser aux graphes à rubans (*ribbon graph*) via le polynôme de Bollobás-Riordan qui généralise le polynôme de Tutte dans ces graphes.

En théorie des codes, l'étude des codes \mathbb{Z}_4 -linéaires peut se faire via la notion de paire de matroïdes. Le polynôme de Rutherford est une extension à trois variables du polynôme de Tutte adapté à l'étude de ces structures.

Enfin nous n'avons pas inclus l'étude des matroïdes orientés et les applications du polynôme de Tutte dans ce cadre (régions d'un arrangement d'hyperplans, etc.), ce qui aurait demandé tout un chapitre supplémentaire.

BIBLIOGRAPHIE

- [AB91] P.W. Shor A. Björner, L. Lovász. Chip-firing games on graphs. *Ann. Discrete Math.*, 12 :283–291, 1991.
- [AdMo4] M. Noy A. de Mier. On graphs determined by their tutte polynomials. *Graphs and Combinatorics*, 20 :105–119, 2004.
- [Ardo7] F. Ardila. Computing the tutte polynomial of a hyperplane arrangement. *Pacific Journal of Mathematics*, 230 :1–26, 2007.
- [Big99] N.L. Biggs. Chip firing and the critical group of a graph. *Journal of Algebraic Combinatorics*, 9 :25–45, 1999.
- [bNW] Edited by N. White. *Matroids applications*. Encyclopedia of Mathematics and its Applications.
- [Bry72a] T.H. Brylawsky. A decomposition for combinatorial geometries. *Transactions of the American Mathematical Society*, 171 :235–282, 1972.
- [Bry72b] T.H. Brylawsky. The tutte-grothendieck ring. *Algebra Universalis*, 2 :375–388, 1972.
- [Cam] P.J. Cameron. Polynomial aspects of codes, matroids and permutation groups.
- [Camo6] P.J. Cameron. Finite geometry and permutation groups : some polynomial links. *Rendiconti di Matematica*, 26 :339–350, 2006.
- [CE99] M.J. Falk C. Eschenbrenner. Orlik-solomon algebras and tutte polynomial. *Journal of Algebraic Combinatorics*, 10 :189–199, 1999.
- [C.G] G. Royle C.Godsil. *Algebraic graph theory*. Springer.
- [Cha92] C.S. Chan. *On shelling and subdivision of convex polytopes*. PhD thesis, MIT, 1992.
- [Cra69] H.H. Crapo. The tutte polynomial. 1969.
- [DWoo] C. Merino D.J.A. Welsh. The potts model and the tutte polynomial. *Journal of mathematical physics*, 41(3), 2000.
- [FB09] R. Sanyal F. Breuer. Ehrhart theory, modular flow reciprocity, and the tutte polynomial. *arXiv :math/0907.0845v1*, 2009.
- [Jae88] F. Jaeger. Tutte polynomials and link polynomials. *Proceedings of the American Mathematical Society*, 103(2) :647–654, 1988.

- [JEMo8] C. Merino J.A. Ellis-Monaghan. Graph polynomials and their applications i : The tutte polynomial. *arXiv :math/0803.3079v2*, 2008.
- [Kun08] J.P.S. Kung. Coboundaries, flows, and tutte polynomial of matrices. *Annals of Combinatorics*, 12 :183–194, 2008.
- [Mas01] G. Masbaum. Matrix-tree theorems and the alexander-conway polynomial. *Geometry & Topology Monographs*, 4 :201–214, 2001.
- [MB05] V. Reiner M. Barany. The tutte polynomial of a finite projective space. 2005.
- [Mer97] C. Merino. Chip firing and tutte polynomial. *Annals of Combinatorics*, 3 :253–259, 1997.
- [Mero1] C. Merino. The chip firing game and matroid complexes. *Discrete Mathematics and Theoretical Computer Science Proceedings*, pages 245–256, 2001.
- [Oxl] J. Oxley. *Matroids theory*. Oxford.
- [PR78] R.C. Read P. Rosenstiehl. On the principal edge tripartition of a graph. *Ann. Discrete Math.*, 3 :195–226, 1978.
- [Rei99] V. Reiner. An interpretation for the tutte polynomial. *European Journal of Combinatorics*, 20 :149–161, 1999.
- [She74] G.C. Shephard. Combinatorial properties of associated zonotopes. *Can. J. Math.*, XXVI(2) :302–321, 1974.
- [Sta80] R.P. Stanley. Decomposition of rational convex polytope. *Annals of Discrete Mathematics*, 6 :333–342, 1980.
- [Sta91] R.P. Stanley. A zonotope associated with graphical degree sequences. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 4 :555–570, 1991.
- [Stao6] R.P. Stanley. Acyclic orientations of graphs. *Discrete Mathematics*, 306 :905–909, 2006.
- [Thi87] M.B. Thistlethwaite. A spanning tree expansion of thr jones polynomial. *Topology*, 26(3) :297–309, 1987.
- [Wel] D.J.A. Welsh. *Complexity : Knots, Colourings and Counting*. Cambridge University Press.
- [Wel94] D.J.A. Welsh. The computational complexity of knot and matroid polynomials. *Discrete Mathematics*, 124 :251–269, 1994.

Ce document a été préparé à l’aide des éditeurs de texte libre Vim et Medit et du logiciel de composition typographique \LaTeX 2 ϵ sous Frugalware Linux. Les graphiques ont été produit grâce à Metapost et Gimp. Le texte est distribué sous licence Creative Common by-nc-sa. Certaines images sont sous leurs licence d’origine (Creative Common by-sa) et restent la propriété de leurs auteurs respectifs (voir les sources pour plus de détails).