Notes du cours de “Calcul Symbolique, Fonctions Symétriques et Spéciales” MMI 2006-2007. (Version provisoire)

G. H. E. DUCHAMP & CHRISTOPHE TOLLU & FRÉDÉRIC TOUMAZET *

04-06-2007 19:22

Table des matières

0 Préambule **2**

1 Introduction **3**

2 Graphes et structures de transition **3**
- 2.1 Applications . . . 7
  - 2.1.1 Chaînes de Markov à une matrice . . . 7
  - 2.1.2 Plusieurs matrices . . . 7
- 2.2 Coûts et poids . . . 7

3 Décomposition **7**
- 3.1 Cadre général . . . 7
- 3.2 Décomposition automatique de modules . . . 10
- 3.3 Calcul de l’ensemble suffixe . . . 11
- 3.4 Calcul de $\mathrm{End}_{\mathcal{A}}(M)$ et des idempotents (projecteurs) . . . 13

4 Idempotents **16**
- 4.1 Généralités . . . 16
- 4.2 Décomposition . . . 16

5 Application I : Cryptographie et fonctions booléennes **17**
- 5.1 Définition . . . 17
- 5.2 Les Diagrammes de Décision Binaire . . . 18

6 Décomposition d’une fonction booléenne **18**
- 6.1 Algèbre du groupe symétrique . . . 19
- 6.2 Exemples de décompositions . . . 20

∗ Prière de nous signaler les erreurs.

7 Application II : Module sur $\mathfrak{H}_k^n(0)$ **21**
7.1 L'algèbre de Hecke 21
7.2 Exemples de décompositions 22

8 Description du programme DEC-MOD **25**
8.1 Cas des groupes finis : Caractères 28
8.1.1 Un modèle qui contient toutes les représentations : la représentation régulière 28
8.1.2 Construction d'une FCIOM pour le groupe symétrique 30
8.1.3 Étude rapide de la complecité du calcul 34

9 Traces **36**

10 Liminaire **36**

11 Bases et algèbres de Gelfand-Tsetlin **36**

12 Description des poids **38**
12.1 Modules de l'algèbre de Hecke affine dégénérée $\mathcal{H}_2$ 38
12.2 Le graphe de Young est le graphe de branchement 39

13 Formules de Murnaghan-Nakayama **40**

14 Annexe A: Automates **41**
14.1 Description de la structure d'automate 41
14.1.1 Graphe pondéré 41
14.1.2 Structure et comportement des automates 42
14.1.3 Exemples de fonctions produites par des automates 43
14.2 Which rational calculus ? 43

0 Préambule

Ce cours est commun aux étudiants originaires des filières Informatique et Mathématique. Il est conçu de façon à permettre aux étudiants des deux sensiblilté s

– d'acquérir des élements de culture générale scientifique n'auraient pas été acquis pendant leur parcours (comme les liens entre algèbre, combinatoire, analyse et géométrie)
– d'unifier les disciplines classiques et certains thèmes innovants

Les illustrations seront faites en Maple et Mupad, mais le contenu de l'enseignement est, bien entendu, indépendant du langage.

Le poly correspond à un programme maximal. Seule une partie de celui-ci sera traitée cette année (cette partie sera délimitée pendant le Forum). Les exercices qui sont là pour aider à la compréhension du cours.
II se peut que vous ne compreniez pas certains énoncés, dans ce cas choisissez que les questions que vous êtes capables d'aborder ... et contactez-nous rapidement pour le décodage du reste.

Les parties en petits caractères sont des suppléments et ne sont pas obligatoires.

1 Introduction

Le cours qui suit est un mélange entre Mathématiques et Informatique. En particulier toutes les notions seront effectives et implémentables. Le cours débute par une description assez large et plutôt théorique, mais nous verrons très tôt

– des exemples complètement dévissés
– une implémentation et des programmes

La première partie décrit les liens entre les notions suivantes

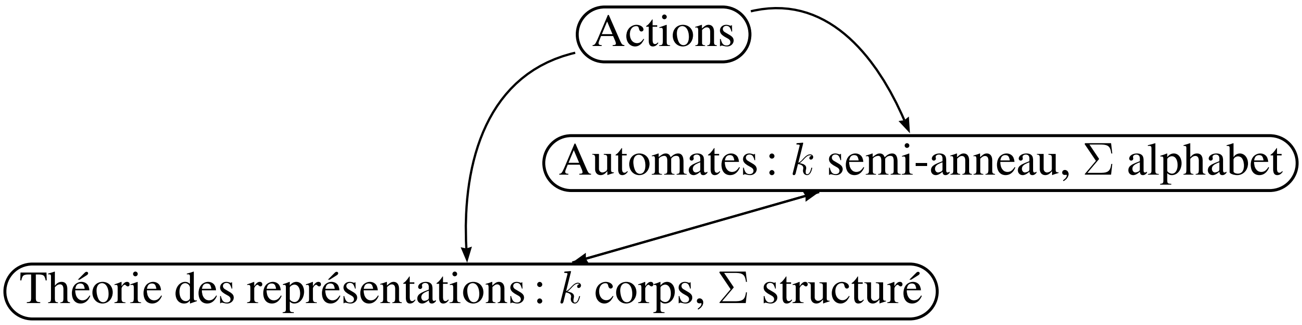


FIG. 1 – *Les différents domaines de ce cours.*

2 Graphes et structures de transition

L'élément le plus complet de ces modèles est la flêche

$$q_1 \xrightarrow{a|w} q_2$$

i) $q_1,q_2 \in Q$ Q est un ensemble (fini ou infini d'états)
ii) a est le symbole qui agit
iii) $\alpha \in k$ est un coefficient. L'ensemble (k) des coefficients est muni de deux lois $+,\times$, associatives, $+$ est commutative et $\times$ soit distributive (à droite et à gauche) sur $+$.

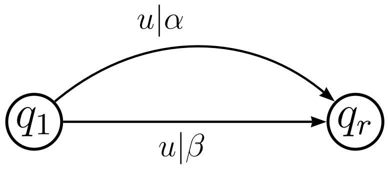
Nous verrons plus bas que ces propriétés sont nécessaires au bon fonctionnement du modèle. Si f est la flêche ci-dessus nous noterons

- $\alpha(f) = q_1$, source ou origine de f
- $\beta(f) = q_2$, but ou extrémité de f
- $\lambda(f) = a$, étiquette de f
- $weight(f)$, poids, coût ou coefficient de transition de f

On appelle <u>chemin</u> toute suite finie $c = f_1 f_2 \cdots f_n$ de flêches telle que $(\forall j < n)(\beta(f_j) = \alpha(f_{j+1}))$. On étend aussitôt les notions précédentes aux chemins par (avec $c = f_1 f_2 \cdots f_n$)

$$\left.\begin{array}{l}
\bullet\ \alpha(c) = \alpha(f_1), \text{ source ou origine de } c\\
\bullet\ \beta(c) = \beta(f_n), \text{ but ou extrémité de } c\\
\bullet\ \lambda(c) = \lambda(f_1)\lambda(f_2)\cdots\lambda(f_n) \text{ (concaténation dans } \Sigma^*\text{), étiquette de } c\\
\bullet\ weight(c) = weight(f_1)weight(f_2)\cdots weight(f_n) \text{ (produit dans } k\text{), poids de } c.
\end{array}\right\} \quad (1)$$

Lorsque l'on a deux chemins $c_1 = f_1 f_2 \cdots f_{n_1}$ et $c_2 = f_{n_1+1} f_{n_1+2} \cdots f_n$ <u>consécutifs</u> (c'est à dire que $\beta(c_1) = \alpha(c_2)$), on définit leur concaténation $c_1 c_2$ par $f_1 f_2 \cdots f_{n_1} f_{n_1+1} f_{n_1+2} \cdots f_n$.
On vérifie facilement que les formules (1) sont encore vraies pour des suites (concaténables) de chemins ce qui permet de considérer les flêches comme des chemins de longueur 1.
Le poids d'un ensemble de chemins de même source, but et étiquette est la somme des poids des chemins de cet ensemble. Ainsi, si on a deux chemins (de même étiquette) le poids de cet ensemble de chemins est $\alpha + \beta$.



On a donc que les poids se multiplient en série et s'aditionnent en parallèle. Les diagrammes suivants montrent la nécessité des propriétés exigées pour $+$ et $\times$.

Diagramme	Identité	Nom
$p \begin{array}{c}\xrightarrow{a\mid\alpha}\\ \xrightarrow{a\mid\beta}\\ \xrightarrow{a\mid\gamma}\end{array} q$	$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	Associativité de $+$
$p \begin{array}{c}\xrightarrow{a\mid\alpha}\\ \xrightarrow{a\mid\beta}\end{array} q$	$\alpha + \beta = \beta + \alpha$	Commutativité de $+$
$p \xrightarrow{a\mid\alpha} q \xrightarrow{b\mid\beta} r \xrightarrow{c\mid\gamma} s$	$\alpha(\beta\gamma) = (\alpha\beta)\gamma$	Associativité de $\times$
$p \begin{array}{c}\xrightarrow{a\mid\alpha}\\ \xrightarrow{a\mid\beta}\end{array} q \xrightarrow{b\mid\gamma} r$	$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$	Distributivité (droite) de $\times$ sur $+$
$p \xrightarrow{a\mid\alpha} q \begin{array}{c}\xrightarrow{b\mid\beta}\\ \xrightarrow{b\mid\gamma}\end{array} r$	$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$	Distributivité (gauche) de $\times$ sur $+$

Remarque 2.1 *i) La plupart du temps on a des éléments neutres pour $+$ et $\times$. S'il n'y sont pas, on peut montrer qu'il est possible de les rajouter*[1].
ii) Les règles "multiplier" en série et "ajouter" en parallèle sont - aussi - celles des probabilités.

1. en langage académique cette opértion se nomme l'"adjonction".

Exercice 2.2 *On considère l'automate probabiliste de la figure (2).*
a) Déterminer la fonction génératrice de probabilité

$$\sum_{n\geq 0} p_n z^n \tag{2}$$

où p_n est la probabilité de passer de l'entrée (avec probabilité d'entrée p_e) à la sortie (avec probabilité de sortie p_s) avec un chemin de longueur n.
des chemins réussis de l'automate probabilite de la figure (2). b) Déterminer la fonction $\{P,F\}^* \mapsto \mathbb{R}$ déterminée par l'automate ci-dessous (les charges d'entrée et de sortie sont p_e,p_s).

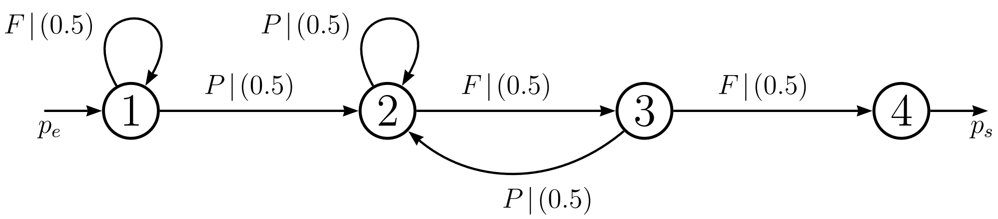


FIG. 2 – *Un automate proposé par les étudiants*

Correction de l'exercice (2.2) a) Les matrices de transition étant notées M_P,M_F, si on ne compte que la longueur des chemins, on a la matrice de transition unique $M = M_P + M_F$. Il est facile de voir (par récurrence par exemple) que $M^k[i,j]$ est la probabilité de passer de l'état i à l'état j en k coups (i.e. avec un chemin de longueur k) d'où $p_n = p_e M^n[1,4]p_s$. Par suite, la SG de probabilité est

$$\sum_{n\geq 0} p_n z^n = \sum_{n\geq 0} p_e M^n[1,4]p_s z^n = p_e p_s(\sum_{n\geq 0} M^n z^n)[1,4] = p_e p_s(1 - zM)^{-1}[1,4] \tag{3}$$

ceci se calcule avec la programme ci-dessous.

```
> with(linalg):
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

```
> Mp:=matrix(4,4,[0,1/2,0,0,0,1/2,0,0,0,1/2,0,0,0,0,0,0]);
```

$$Mp := \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

```
> Mf:=matrix(4,4,[1/2,0,0,0,0,0,1/2,0,0,0,0,1/2,0,0,0,0]);
```

$$Mf := \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

```
> M:=matadd(Mp,Mf);
```

$$M := \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

```
> I4:=matrix(4,4,(i,j)->if i=j then 1 else 0 fi);
```

$$I4 := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

```
> M2:=matadd(I4,M,1,-z);
```

$$M2 := \begin{bmatrix} 1-\frac{z}{2} & -\frac{z}{2} & 0 & 0 \\ 0 & 1-\frac{z}{2} & -\frac{z}{2} & 0 \\ 0 & -\frac{z}{2} & 1 & -\frac{z}{2} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

```
> inverse(M2)[1,4];
```

$$\frac{z^3}{(-2+z)\,(-4+2\,z+z^2)}$$

finalement, la série cherchée est

$$\frac{t^3 p_e p_s}{(2-t)(4-2t-t^2)} = p_e p_s\left(\frac{1}{8}t^3 + \frac{1}{8}t^4 + \frac{1}{8}t^5 + \frac{7}{64}t^6 + \frac{3}{32}t^7 + \frac{5}{64}t^8 + \frac{33}{512}t^9 + \cdots\right) \quad (4)$$

b) La série cherchée se calcule selon le même principe, il s'agit de remplacer $\sum_{n\geq 0} M^n z^n$ ($= (1-zM)^{-1}$), i.e. l'étoile de zM par l'étoile de $PM_P + FM_F$, ce qui se fait par les formules (73).

2.1 Applications

2.1.1 Chaînes de Markov à une matrice

2.1.2 Plusieurs matrices

2.2 Coûts et poids

3 Décomposition

3.1 Cadre général

Un graphe pondéré détermine une structure de transition qui est équivalente à la donnée d'une application $\Sigma \mapsto End(V)$.
Cela revient à se donner une famille de matrices $\{M_\alpha\}_{\alpha\in\Sigma}$ ou d'opérateurs $\{\varphi_\alpha\}_{\alpha\in\Sigma}$ qui agissent sur un espace vectoriel V, soit une application[2] $\mu \;:\; \Sigma \mapsto \mathrm{End}(V)$. Les opérateurs φ_α sont souvent appelés actions de Σ sur V.
Une telle structure est appelée représentation linéaire de l'ensemble Σ et V s'appelle alors un Σ-module. Si Σ est doué d'une structure supplémentaire (monoïde, groupe, algèbre associative, algèbre de Lie, algèbre de Hopf, de Jordan, C^*-algèbre, superalgèbre), il faut, de plus, vérifier la compatibilité de cette structure suppémentaire avec μ (on demande en général que μ soit un morphisme).

Définition 3.1 *Soit $(\mu_\alpha)_{\alpha\in\Sigma}$ une famille d'opérateurs agissant sur un espace vectoriel V.*
i) On dit que qu'un sous-espace $W \subset V$ est

- *stable si $(\forall\alpha \in \Sigma)(\mu_\alpha(W) \subset W)$*
- *irréductible si pour tout sous-espace stable $(0) \subset W_1 \subset W$, on a $W_1 = (0)$ ou $W_1 = W$.*

ii) Si $V = \oplus_{i\in I} V_i$ et que les V_i sont stables on dit que $V = \oplus_{i\in I} V_i$ est une décomposition de V.
iii) Soient deux Σ-modules U et V. On dit qu'une application linéaire $\varphi \;:\; U \mapsto V$ est Σ-linéaire si elle commute avec tous les μ_α soit

$$(\forall\alpha \in \Sigma)(\forall v \in U)(\varphi \circ \mu_\alpha(v) = \mu_\alpha \circ \varphi(v)). \tag{5}$$

On dit aussi que φ est un morphisme de Σ-modules. On note $\mathrm{Hom}_\Sigma(U,V)$ l'ensemble des applications Σ-linéaires $U \mapsto V$ (resp. $\mathrm{End}_\Sigma(U)$ si $U = V$.

Remarque 3.2 *i) On n'a pas toujours de décomposition de V en plusieurs irréductibles non nuls, comme le montre le cas d'un seul opérateur dont la matrice dans une base de V est $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.*
ii) Si V admet une décomposion en irréductibles (c'est toujours le cas, nous le verrons, pour les groupes finis) on dit que V est semi-simple ou complètement réductible.
iii) Avec la notation précédente, l'ensemble des applications (seulement !) linéaires $U \mapsto V$ se note $\mathrm{Hom}_k(U,V)$.

Exercice 3.3 *(Généralités) Soit X un ensemble. Pour $n,k \in \mathbb{N}$, la classe de Burnside $B(n,k)$ est l'ensemble des applications $f \;:\; X \mapsto X$ telles que $f^n = f^{n+k}$ où f^n est la suite d'applications définies par*

$$f^0 = Id_X \;;\; f^{n+1} = f \circ f^n \tag{6}$$

2. On rappelle que $\mathrm{End}(V)$ désigne l'espace des applications linéaires $V \mapsto V$.

Remarque. — *C'est la "puissance compositionnelle" définie, pour $n > 0$ par $f^n = \underbrace{f \circ f \cdots \circ f}_{n\ fois}$.*

Deux classes sont courantes : $B(1,1)$, les idempotents et $B(0,2)$, les involutions (resp. projecteurs ou symétries dans le cas d'applications linéaires).

1) Soit V un k-espace vectoriel et p, un projecteur de V.

a) Montrer que $V = ker(p) \oplus im(p) = V_0 \oplus V_1$

b) Ici $\Sigma = \{p\}$ Montrer que

$$\mathrm{End}_\Sigma(V) = \{f \in \mathrm{End}(V) | f(V_0) \subset V_0,\, f(V_1) \subset f(V_1)\} \tag{7}$$

2) a) On suppose que $1/2 \in k$. Soit s une symétrie de V. Montrer que

$$p_{(1)} = \frac{1}{2}(s + Id) \ \ et \ \ p_{(-1)} = \frac{1}{2}(s - Id) \tag{8}$$

sont des projecteurs.

b) On pose $\Sigma_1 = \{s\}$; $\Sigma_2 = \{p_{(-1)},p_{(1)}\}$. Montrer que $\mathrm{End}_{\Sigma_1}(V) = \mathrm{End}_{\Sigma_2}(V)$.

c) À l'aide de (1.b) et (2.b), caractériser $\mathrm{End}_{\Sigma_1}(V)$.

À ce stade, on ne peut véritablement décider si une action est "à droite" ou "à gauche" (et, à vrai dire, on peut les noter du côté que l'on veut). Si on veut garder trace de la succession des actions, c'est la structure de mot qu'il faut utiliser et étendre μ en une application

$$\bar{\mu} \ : \ \Sigma^* \mapsto \mathrm{End}(V)$$

qui transforme la concaténation en composition. Là, selon que les actions sont notées à droite ou à gauche on aura

$$\bar{\mu}(uv) = \bar{\mu}(u) \circ \bar{\mu}(v) \text{ ou bien } \bar{\mu}(uv) = \bar{\mu}(v) \circ \bar{\mu}(u). \tag{9}$$

Ceci nous amène à la structure minimale pour "préparer les actions", c'est la notion de représentation d'un semigroupe[3].

Définition 3.4 *Soit $(G,*)$ un semigroupe et $(\mu_\alpha)_{\alpha \in G}$ une représentation de G dans V. On dit que μ est une représentation "à gauche" si*

$$(\forall u,v \in G)(\mu_{\alpha * \beta} = \mu_\alpha \circ \mu_\beta) \tag{10}$$

et "à droite" si

$$(\forall u,v \in G)(\mu_{\alpha * \beta} = \mu_\beta \circ \mu_\alpha). \tag{11}$$

Note 3.5 *Cette définition est conditionnée par le déplacement des parenthèses en effet, si l'on note $q.\alpha$ (resp. $\alpha.q$) pour $\mu_\alpha(q)$ dans le cas d'une représentation à droite (resp. à gauche), on a $(q.\alpha).\beta = q.(\alpha * \beta)$ (resp. $\alpha.(\beta.q) = (\alpha * \beta).q$).*

Exemple 3.6 *Nous considérons le groupe symétrique $\mathfrak{S}_3 = \{[123],[132],[213],[231],[312],[321]\}$ agissant sur les coordonnées de l'espace (ambiant) par permutation des coordonnées des vecteurs. Nous notons $(e_i)_{i=1,2,3}$ la base canonique. Soit*

$$e_1 = (1,0,0) \ ; \ e_2 = (0,1,0) \ ; \ e_3 = (0,0,1)$$

Comme le groupe symétrique est engendré par $\sigma_1 = [213]$ et $\sigma_2 = [132]$, il suffit de coder les actions de ces générateurs sur l'espace décrit à l'aide de ses vecteurs de base.

3. Un semigroupe est un ensemble muni d'une loi associative.

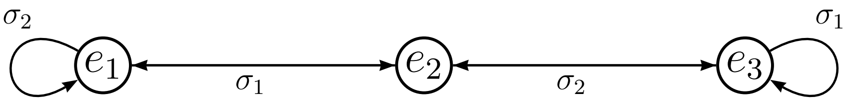


FIG. 3 – *Le $\mathfrak{S}_3$-module k^3.*

DÉCOMPOSITION EN SOUS-MODULES IRRÉDUCTIBLES. —
On remarque d'abord que le vecteur $e_{123} = e_1 + e_2 + e_3 = (1,1,1)$ est invariant par le groupe. Donc la droite $k.e_{123}$.
Le produit scalaire usuel $\langle (x,y,z)|(x',y',z')\rangle = xx' + yy' + zz'$ (ici $k = \mathbb{R}$, pour $\mathbb{C}$ prendre le premier vecteur conjugué) est invariant par $\mathfrak{S}_3$ (voir exercice (8.7)). Par suite, le plan $(e_{123})^\perp$ (d'équation $x + y + z = 0$ est invariant). Ce plan est engendré par $e_1 - e_2 = (1,-1,0)$ et $e_2 - e_3 = (0,1,-1)$. Ce module est décrit dans la figure (4).

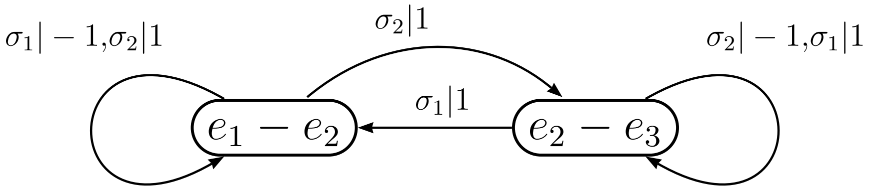


FIG. 4 – *Un sous-module du $\mathfrak{S}_3$-module k^3.*

Exercice 3.7 *Montrer que le module de la figure 4 est irréductible.*

Exercice 3.8 DÉCOMPOSITION DE LA REPÉSENTATION RÉGULIÈRE GAUCHE DE $\mathfrak{S}_3$ DANS $\mathbb{R}[\mathfrak{S}_3]$.. —
Dans tout l'exercice, $G = \mathfrak{S}_3$.
Les données sont les suivantes :

- *l'espace est celui des fonctions $G \mapsto \mathbb{R}$, notées comme des sommes $f := \sum_{h\in G} f(h)h$. Cet espace est noté $\mathbb{R}[G]$.*
- *les éléments de G sont notés comme des listes et celui qui est à gauche agit par valeurs sur celui qui est à droite.*

$$G = \mathfrak{S}_3 = \Big\{[123],[132],[213],[231],[312],[321]\Big\}$$
$$g_1.g_2 = \Big[g_1[g_2[1]],g_1[g_2[2]],g_1[g_2[3]]\Big] \tag{12}$$

- *G agit sur les fonctions par linéarité soit*

$$g.(\sum_{h\in G} f(h)h) = \sum_{h\in G} f(h)g.h \tag{13}$$

Remarque. — *On définit de même l'action à droite (mais nous n'en aurons besoin que plus tard) par*

$$(\sum_{h\in G} f(h)h).g = \sum_{h\in G} f(h)h.g \tag{14}$$

1) Montrer que, pour tout $g \in G$, l'application $\rho(g) \ : \ \mathbb{R}[G] \mapsto \mathbb{R}[G]$ est linéaire.
2) Montrer que c'est bien une représentation du groupe G au sens où

$$(\forall g_1, g_2 \in G)(\rho(g_1.g_2) = \rho(g_1) \circ \rho(g_2)) \tag{15}$$

(il suffit de montrer l'égalité des images sur une base).
3) Montrer que les droites

$$D_1 = \mathbb{R}(\sum_{g \in G} g) \ ; \ D_{-1} = \mathbb{R}(\sum_{g \in G} (-1)^{inv(g)} g) \tag{16}$$

sont invariantes par ρ.
4) Soit $w_1 = [123] - [213] + [132] - [231]$. Décrire le module W_1 engendré par w_1 sous l'action de ρ.
5) a) Calculer $w_2 = w_1.[213]$. Soit W_2 le module engendré par w_2, montrer que l'on a

$$\mathbb{R}[G] = W_1 \oplus W_2 \oplus D_1 \oplus D_{-1} = W_1 \oplus W_2 \oplus W_3 \oplus W_4 \tag{17}$$

b) Soit $1_{\mathbb{R}[G]} = e_1 + e_2 + e_3 + e_4$, la décomposition de $1_{\mathbb{R}[G]}$ selon la somme directe (17). Montrer que
i) $(\forall i, j \in [1..4])(e_i e_j = \delta_{ij} e_i) = \delta_{ij} e_j)$ *ii)* $\mathbb{R}[G]e_i = W_i$

Commentaire. — La propriété b)i) entraine que les e_i sont idempotents (i.e. vérifient $ee = e$). Si une famille d'éléments vérifie b)i), on dit que c'est une *famille d'idempotents orthogonaux*. Si, de plus, $1 = \sum_i e_i$, on dit que la famille est *complète*. Et si, de plus, tous les $W_i = \mathcal{A}e_i$ sont irréductibles, on dit que c'est une *Famille Complète d'Idempotents Orthogonaux Minimaux* (FCIOM). On verra qu'une telle famille est l'outil de décomposition de $\mathbb{C}[G]$ comme somme d'algèbres de matrices.

$\diamondsuit$

3.2 Décomposition automatique de modules

Cet algorithme est l'œuvre de Schützenberger [2, **?**, 28, 20]. En effet, il fut inventé pour l'optimisation des automates à multiplicités [2].

Un automate à multiplicités dans k est défini par la donnée d'un quintuplet (Σ, Q, I, T, F) [2] où

- Σ est l'alphabet (de commande)
- Q est l'ensemble fini des états
- $I \subset Q$ est l'ensemble des états initiaux
- $F \subset Q$ est l'ensemble des états finaux
- $T \subset Q \times A \times k \times Q$ contient les arcs orientés reliant les états entre eux.

Les actions sont notées à droite pour être compatibles avec la séquentialité des mots. Des données précédentes, on déduit la représentation linéaire (λ, μ, γ) de l'automate.

Nous ne toucherons pas dans ce cours, plus centré sur les représentations, à la très belle et très générale théorie des automates (qui appartient en propre à l'Informatique Théorique), mais verrons comment on peut appliquer quelques-uns de ses concepts au calcul dans les modules. Dans le cas (bien particulier) où l'ensemble des coefficients est un corps (ou même un anneau) ces deux théories sont équivalentes puisque, vue de la théorie des représentations, les automates sont essentiellement la donnée d'un Σ-module engendré par un seul vecteur (dit cyclique) avec une fonction d'observation (i.e. une forme linéaire) et leurs sorties sont donc déterminées par une combinaison de coefficients matriciels.

La première étape de l'algorithme de minimisation d'un k-automate (c'est à dire l'optimisation du nombre de ses états à fonctionnement équivalent), donné par sa représentation linéaire (λ,μ,γ) à multiplicités dans un corps (commutatif ou non) k (dû à Schützenberger), est la construction d'un ensemble préfixe[4] P tel que l'orbite $\lambda\mu(P)$ soit une base de $\lambda\mu(k\langle\langle A\rangle\rangle)$ [2, **?**, 28]. Ce même processus permet aussi d'obtenir un certificat $\mathrm{cert(M)}$ vérifiant si un Σ-module M engendré par une seul vecteur est décomposable ou non.

La structure de ce paragraphe est la suivante. Dans un premier temps, nous présenterons l'algorithme de décomposition d'un module. La première étape sera le calcul de l'ensemble suffixe qui correspond à la réduction à gauche de la théorie de minimisation. La deuxième étape sera le calcul des endomorphismes et des projecteurs. Puis, nous appliquerons notre algorithme pour décomposer des modules définis sur l'algèbre du groupe symétrique et aussi sur l'algèbre de Hecke à $q = 0$.

Décomposition de modules

Dans la pratique, on a besoin de passer aux combinaisons linéaires d'opérateurs et donc, par rapport à ce qui a été fait juste avant la définition (3.4), une deuxième extension aux combinaisons linéaires de mots (les polynômes non commutatifs $k\langle\Sigma\rangle$) est nécessaire.
Nous présentons l'algorithme dans le cadre général d'une algèbre d'opérateurs (associative) sur un espace vectoriel de dimension finie V. Il peut être compris avec $\mathcal{A} = k\langle\Sigma\rangle$.

Définition 3.9 *Un espace vectoriel $\mathcal{A}$ sur un corps k est muni d'une structure d'algèbre (ou k-algèbre) par la donnée d'un produit $(x,y) \to xy$, bilinéaire $\mathcal{A} \times \mathcal{A} \mapsto \mathcal{A}$. L'algèbre est dite commutative, associative, unitaire si la produit l'est. Dans la suite, une algèbre associative, avec unité (unitaire) sera désignée par AAU.*

Soit $\mathcal{A}$ une algèbre associative sur un corps (commutatif ou non) k engendrée par une ensemble S. Soit M est un $\mathcal{A}$-module à gauche. On considère le sous-module $\mathcal{A}\cdot m$, ayant pour générateur $m \in M$. La première étape dans le processus de décomposition d'un tel module est le calcul d'un ensemble suffixe. On notera par $\mathrm{ann}(m) = \{a \in \mathcal{A} : a\cdot m = 0\}$ l'ensemble des annulateurs de m. C'est un idéal à gauche de $\mathcal{A}$.

3.3 Calcul de l'ensemble suffixe

On commence par construire une partie suffixe $P \subset S^*$ tel que $P \cdot m$ soit une base de $\mathcal{A} \cdot m$.

Soit $E := \{(s_i,s) \in S \times P \mid s_i s \notin P\}$. Pour $(s_i,s) \in E$, on a :

$$s_i s.m = \sum_{s' \in P} \alpha_{s_i s, s'} s'.m \tag{18}$$

4. suffixe si le actions sont à gauche.

et les différences $R := \left\{s_i s - \sum_{s' \in P} \alpha_{s_i s, s'} s'\right\}_{(s_i,s)\in E}$ forment un ensemble complet de générateurs de ann(m). Donc, la première étape du processus de décomposition est le calcul d'un ensemble suffixe $P \subset S^*$ où on a recours à la théorie de minimisation et plus précisément la deuxième étape du processus à savoir l'algorithme de réduction à gauche qui consiste à calculer une base de $\mathcal{A} \cdot m$. On modifie cet algorithme pour qu'il puisse garder trace des relateurs qui apparaissent au cours du calcul de l'ensemble suffixe et pour obtenir ainsi un test qui permettra de choisir les idempotents de $\mathrm{End}_{\mathcal{A}}(\mathcal{A} \cdot m)$ parmi les projecteurs de $\mathrm{End}_k(\mathcal{A} \cdot m)$.

L'algorithme suivant permet donc de trouver un ensemble suffixe de S^* et l'ensemble des relateurs. Il prend en entrée l'ensemble S et un générateur $m \in M$ et retourne en sortie l'ensemble suffixe P et l'ensemble des relateurs R.

Algorithme *suffixe*

Entrée : l'ensemble S
un générateur $m \in M$
Sortie : un ensemble suffixe $P \subset S^*$
un ensemble des relateurs R
Début
1. $(P,Y,R) := (\emptyset,\{\varepsilon\},\emptyset)$
2. **Tant que** $Y \neq \emptyset$ **faire**
3. retirer un mot y de Y
4. **Si** $y \cdot m \notin$ span$(p \cdot m : p \in P)$ **alors**
5. $(P,Y) := (P \cup \{y\},(Y - \{y\}) \cup yS)$
6. **Sinon**
7. Il existe une relation $y.m = \sum_{p \in P} \alpha_p p \cdot m$
$(P,Y,R) := (P,(Y - \{y\}),R \cup \{y - \sum_{p\in P} \alpha_p p\})$
8. **Fin_si**
9. **Fin_faire**
10. **retourner** (P,R)
Fin.

L'ensemble P est un ensemble suffixe et l'algorithme se termine. En effet, l'ensemble P est un ensemble suffixe à chaque étape de l'algorithme. Ceci est évident en fait dès le début avec $P = \{\varepsilon\}$. Ensuite, si $y \in Y \subseteq S^*$ est accepté, tous les suffixes de y sont dans P. Soit $|s|$ la longueur du mot $s \in S^*$. Puisque l'espace $\mathcal{A} \cdot m$ est de dimension finie, il existe un entier positif l tel que :

$$\text{span}(s \cdot m : s \in S^*)=\text{span}(s \cdot m : s \in S^* \text{ et } |s| < l).$$

On a $P \subseteq \{s \in S^* : |s| < l\}$ et $Y \subseteq \{s \in S^* : |s| < l + 1\}$. L'ensemble devient vide durant l'algorithme et alors l'algorithme se termine.

Lemme 3.10 *L'ensemble $P \cdot m = \{s \cdot m : s \in P\}$ est une base de l'espace $\mathcal{A} \cdot m$.*

Preuve Soit $C = SP - P$ le code suffixe complet associé à l'ensemble P [2]. On a la décomposition $S^* = P \sqcup S^*CP$ du monoïde libre. Si $s_i s \in C$, il existe un relateur $s_i s -$

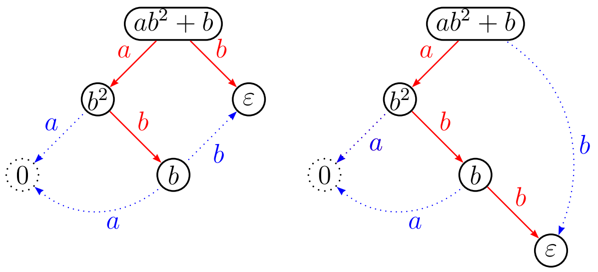


FIG. 5 – *Les ensembles suffixes pour $m = ab^2 + b$ (l'action est donnée par les quotients $(x^{-1})_{x\in\{a,b\}}$ de Eilenberg [20]).*

$\sum_{s'\in P} \alpha_{s'} s' \in R$. Soit maintenant $s_i \in S$ et $s_i s \in CS^*S$. on a alors par induction :

$$\begin{aligned} s_i s \cdot m &= \sum_{s'\in P} \alpha_{s'} s_i s' \cdot m \\ &= \sum_{s_i s' \in P} \alpha_{s'} s_i s' \cdot m + \sum_{s_i s \notin P} \sum_{s''\in P} \alpha_{s'} \beta^{s''}_{s_i s'} s'' \cdot m. \end{aligned}$$

Et donc $s_i s \cdot m \in \text{span}(s \cdot m : s \in P)$. □

D'après le lemme 3.10, l'algorithme suffixe calcule une description complète de l'espace $\mathcal{A} \cdot m$. On remarque que l'ensemble des relateurs dépend du choix du mot $y \in Y$. Soit $m = ab^2 + b \in \mathbb{Q}\langle a,b \rangle$. Les actions étant données par les formules de décalage (quotients de Eilenberg [20]). La figure 5 donne l'ensemble suffixe et l'ensemble des relateurs de $\mathcal{A}.m$. Chaque transition en trait continu représente une action qui aboutit à un nouvel élément de la base et chaque transition en trait discontinu donne un relateur. L'ensemble des relateurs peut être différent si les mots sont choisis selon l'ordre lexicographique gradué ou selon l'ordre lexicographique usuel. En effet, l'élément $b + ab^2 \in S^*$ est un relateur avec le deuxième type d'ordre (graphe à droite de la figure 5) ce qui n'est pas le cas avec le premier type (graphe à gauche de la figure 5).

3.4 Calcul de $\mathrm{End}_{\mathcal{A}}(M)$ et des idempotents (projecteurs)

D'abord un petit exercice sur les projecteurs.

Exercice 3.11 *Soit V un espace vectoriel et $f \in \mathrm{End}(V)$.*
1) Montrer que les conditions suivantes sont équivalentes
i) $f^2 =: f \circ f = f$ (on dit alors que f est idempotent)
ii) $V = Im(f) \oplus Ker(f)$ et $(\forall y \in Im(f))(f(y) = y)$
2) En indexant les propriétés comme suit :
A) $f^2 := f \circ f = f$ B) $V = Im(f) \oplus Ker(f)$ C) $(\forall y \in Im(f))(f(y) = y)$.
a) Trouver une application linéaire $V \mapsto V$ (on pourra la décrire sous forme de matrice) telle que (B) mais pas (C) ni (A).
b) Quels sont les liens logiques entre (A), (B) et (C) ?
3) On suppose maintenant que V est muni d'une structure de Σ-module.
Montrer que, si $f \in \mathrm{End}_k(V)$ est idempotent (i.e. un projecteur), les propriétés suivantes sont

équivalentes
i) f est Σ-linéaire (voir (3.1))
ii) $Im(f)$ et $Ker(f)$ sont stables par Σ (i.e. des sous-modules de V).
4) Dans cette question, on suppose que Σ engendre un groupe fini d'actions de V dans V (i.e. $\mu(\Sigma) = G \subset \mathrm{Aut}(V)$ est fini).
Soit W un sous-module de V et $p : V \mapsto V$ un projecteur sur W.
a) Montrer que

$$f(v) = \frac{1}{|G|} \sum_{g \in G} g(p(g^{-1}(v))) \tag{19}$$

définit un projecteur Σ-linéaire d'image W.
b) Déduire de ce qui précède que tout sous-module de V indécomposable est irréductible.
5) Déduire de ce qui précède que, si V est de dimension finie, il s'exprime comme somme

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r \tag{20}$$

de sous-modules indécomposables.

Commentaire. — La décomposition (21) est unique à permutation et isomophisme près. En fait, on montre que[5], dans les conditions précédentes, si

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r = W_1 \oplus W_2 \oplus \cdots \oplus W_s \tag{21}$$

sont deux décomositions en indécomposables, alors $r = s$ et il existe une permutation τ (ici renommage des indices) telle que, pour tout $1 \leq j \leq r$ $V_j \simeq W_{\tau(j)}$.

$\diamondsuit$

Nous allons voir que les projecteurs sont des outils cruciaux pour décomposer les modules. La section précédente nous a fourni un ensemble de relateurs de type particulier, ils sont de type

$$sp - \sum_{q \in P} \alpha(s,p,q)q. \text{ pour } (s,p) \in S \times P \text{ tels que } sp \notin P \tag{22}$$

La deuxième étape dans le processus de décomposition est le calcul des endomorphismes et projecteurs. On a vu dans la section précédente et d'après le lemme 3.10, qu'il est possible de déterminer algorithmiquement un endomorphisme φ dans la base $(s \cdot m)_{s \in P}$ de $\mathcal{A} \cdot m$. En effet, l'algorithme suffixe permet de calculer l'ensemble suffixe P et l'ensemble des relateurs R. À chaque élément $x = \sum_{s \in P} \alpha_s s.m$, on peut associer un unique endomorphisme $\varphi_x \in \mathrm{End}_k(\mathcal{A} \cdot m)$ tel que, pour tout

$$(\forall w \in P)(w \in P) \tag{23}$$

Pour que $\varphi_x \in \mathrm{End}_{\mathcal{A}}(\mathcal{A} \cdot m)$ il faut et il suffit que $ann(m) \subset ann(x)$.
Inversement, à chaque morphisme $\varphi \in \mathrm{End}_{\mathcal{A}}(\mathcal{A} \cdot m)$, on peut associer un élément m_φ.

L'algorithme suivant permet de construire l'endomorphisme φ. Il prend en entrée l'ensemble suffixe P, l'ensemble des relateurs R du module et l'ensemble S. L'ordre du calcul des vecteurs $\varphi(s \cdot m)$ est donné suivant le rangement de s dans l'ensemble P. Si $s = s_i s'$, alors $\varphi(s' \cdot m)$ est déjà connu.

5. Admis ici, voir le théorème de Krull-Schmidt (6.1).

Algorithme *cons_φ*

Entrée : l'ensemble des transpositions S
l'ensemble suffixe P
l'ensemble des relateurs R
Sortie : le morphisme φ
Début
1. $Y := S$
2. $\varphi(\varepsilon f) := \sum_{s\in P} \alpha_{s,\varepsilon} s \cdot m$
3. **Tant que** $Y \neq \emptyset$ **faire**
4. retirer un mot ss_i de Y
5. **Si** $ss_i \notin P$ **alors**
6. $Y := Y - \{ss_i\}$
7. **Sinon**
8. $\varphi(ss_i \cdot m) := s\varphi(s_i \cdot m)$
$Y := (Y \cup Sss_i) - \{ss_i\}$
9. **Fin_si**
10. **Fin_faire**
11. **retourner** (φ)
Fin.

L'algorithme ne considère que les éléments ss_i qui sont dans l'ensemble suffixe P, les autres éléments, qui ne sont pas dans P et qu'on retrouve forcément dans l'ensemble des relateurs R seront traités à part pour qu'on puisse les manipuler afin de vérifier le deuxième point du lemme 3.12.

Lemme 3.12 *Soit $\varphi \in \mathrm{End}_k(\mathcal{A} \cdot m)$ et $m_\varphi = \varphi(m)$. Alors la transformation linéaire φ appartient à $\mathrm{End}_{\mathcal{A}}(\mathcal{A} \cdot m)$ si et seulement si:*
i) pour tout $s \in P$, on a $\varphi(s \cdot m) = s \cdot \varphi(m)$,
ii) pour tout $(s_i,s) \in S \times P$ tel que $s_i s \notin P$, la différence $\left(s_i s - \sum_{s'\in P} \alpha_{s_i s,s'} s'\right)$ annule m_φ.

Une fois qu'on a le morphisme φ, et d'après le lemme 3.12, pour trouver l'ensemble des projecteurs, on doit étudier la relation d'idempotence

$$\varphi^2 = \varphi \tag{24}$$

et vérifier que

$$\varphi(s \cdot m) = s \cdot \varphi(m) \qquad \forall\ s \in P \tag{25}$$
$$r \cdot \varphi(m) = 0 \qquad \forall\ r \in R \tag{26}$$

De ces trois formules (24), (25) et (26), on obtient un système de $n|P|^2 + |P|$ équations en les inconnues $\alpha_{s,\varepsilon}$ pour tout $s \in P$.

Toute solution non-triviale φ donne une première décomposition $\mathcal{A} \cdot m = \mathcal{A} \cdot m_\varphi \oplus \mathcal{A} \cdot m_{1-\varphi}$. Ensuite, on réapplique l'algorithme sur $\mathcal{A} \cdot m_\varphi$ et $\mathcal{A} \cdot m_{1-\varphi}$. À l'aide de réexécutions de l'algorithme, on obtient une somme directe de sous-modules indécomposables. Sinon, s'il n'existe aucune solution non-triviale, on déduit que le module $\mathcal{A} \cdot m$ ne peut pas être une somme directe de sous-modules.

Théorème 3.13 *Soit $m \in M$. Une répétition finie de l'algorithme suffixe et $cons\_\varphi$ décide s'il existe une décomposition de $\mathcal{A} \cdot m$ en une somme directe de sous-modules indécomposables. Si aucune solution non-triviale ne peut être trouvée, le module $\mathcal{A} \cdot m$ est indécomposable.*

Dans la partie suivante, nous allons appliquer le processus de décomposition pour décomposer des modules définis sur différentes algèbres. Nous commençons par les fonctions définies sur l'algèbre du groupe symétrique. Ensuite, des modules définis sur l'algèbre de Hecke. En effet, les fonctions booléennes jouent un rôle important en cryptographie et surtout dans les systèmes de chiffrement.

Remarque 3.14 *La forme particulière des relateurs R (22) donne un quotient $(k\langle A\rangle; R)$ libre sur k même si k est un anneau.*

4 Idempotents

4.1 Généralités

Classes de Burnside, nombres idempotents, formule exponentielle.

4.2 Décomposition

Exercice 4.1 *Soit $G_n = \langle g; g^n = 1\rangle$ (le groupe cyclique d'ordre n).*
0) (Warmup) Montrer que $G_n = \{g^k\}_{0\leq k<n}$ et que

$$g^p = g^q \iff p - q \text{ est divisible par n}$$

1) Pour $0 \leq k < n$, et $\xi = e^{\frac{2i\pi}{n}}$ on pose

$$e_k = \frac{1}{n}\sum_{j=0}^{n-1} \xi^{-jk} g^j \tag{27}$$

a) Montrer que $g.e_k = \xi^k e_k$ puis que

$$e_{k_1}e_{k_2} = \delta_{k_1,k_2}e_{k_1} \tag{28}$$

b) Montrer que

$$\sum_{k=0}^{n-1} e_k = 1_{G_n} \tag{29}$$

2) (Sandwiches). —
a) Montrer que

$$dim(e_{k_1}\mathbb{C}[G_n]e_{k_2}) = 0 \text{ si } k_1 \neq k_2 \text{ et } 1 \text{ si } k_1 = k_2 \tag{30}$$

b) En déduire que si l'on pose $e_k g e_k = \mu(g)e_k$, l'application

$$g \to \begin{pmatrix} \mu_1(g) & 0 & \cdots & 0 \\ 0 & \mu_2(g) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mu_n(g) \end{pmatrix} \tag{31}$$

est une représentation injective (en théorie des représentations on dit fidèle).
4) Pour une groupe général (fini) G, on considère une FCIOM $(e_t)_{t\in T}$.
a (**) Montrer que

$$dim(e_s\mathbb{C}[G]e_t) \in \{0,1\} \tag{32}$$

b) (**) Montrer que la relation $s \sim t$ définie par $dim(e_s\mathbb{C}[G]e_t) = 1$ est une relation d'équivalence.
5) (**) Soit $B = T/\sim$ et $b \in B$. On range les éléments de b en une suite $t_1,t_2\cdots t_l$, puis on choisit $E_{i,i+1} \in e_{t_i}\mathbb{C}[G]e_{t_{i+1}}$ non nul.
a) Montrer que l'on peut choisir, pour tout $0 \le i < l$, $E_{i+1,i}$ tel que $E_{i,i+1}E_{i+1,i} = e_{t_i}$ et que cela implique que $E_{i+1,i}E_{i,i+1} = e_{t_{i+1}}$.
b) On définit $E_{i,j}$ par

$$\begin{aligned}
&E_{i,j} = E_{i,i+1}E_{i+1,i+2}\cdots E_{j-1,j} \text{ pour } i < j\\
&E_{i,j} = E_{i,i-1}E_{i-1,i-2}\cdots E_{j+1,j} \text{ pour } i > j\\
&E_{i,i} = e_{t_i}
\end{aligned} \tag{33}$$

montrer que ces éléments sont des unités matricielles i.e. $E_{i,j_1}E_{j_2,k} = \delta_{j_1,j_2}E_{i,k}$.
c) Pour $0 \le i,j \le l$ on définit $\rho_{i,j}(g)$ par $e_{t_i}ge_{t_j} = \rho_{i,j}(g)E_{i,j}$. Montrer que $\rho_b = (\rho_{i,j})_{0\le i,j\le l}$ définit une représentation matricielle de G.
6) a) (**) Montrer que la représentation par blocs $\rho = (\rho_b)_{b\in B}$; $\mathbb{C}[G] \mapsto \bigoplus_{b\in B}\mathcal{M}(l_b,\mathbb{C})$ est fidèle.
b) (***) Montrer que ρ est un isomorphisme.

5 Application I : Cryptographie et fonctions booléennes

5.1 Définition

La cryptographie est l'étude des méthodes et techniques mathématiques liées aux aspects de la sécurité de l'information tels que la confidentialité, l'intégralité des données, l'authentification d'identités et l'authentification de l'originalité des données. C'est un ensemble de techniques qui fournit la sécurité de l'information. La cryptographie permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu. Elle fait appel à l'algèbre linéaire, la théorie des groupes, la théorie combinatoire et la théorie des graphes. Différentes fonctions mathématiques de base sont importantes pour comprendre en détail les algorithmes de chiffrement. Les systèmes de chiffrement basés sur des fonctions linéaires, ou des fonctions affines, étant considérés comme faibles, la capacité à mesurer la non-linéarité est un moyen pour calculer la force d'un algorithme. La non-linéarité d'une fonction est la mesure du nombre de bits qui doivent changer dans la table de vérité d'une fonction booléenne pour s'approcher d'une fonction affine. Une fonction affine est une fonction booléenne linéaire f(x) = ax + b où l'addition peut être représentée par un OU-Exclusif et la multiplication par un ET. Les opérations OU-Exclusif et ET ensemble produisent le même résultat que les opérations somme et produit "modulo 2".
Par fonction booléenne, on entend toute fonction $\{0,1\}^n \to \{0,1\}$ ce qui, en langage informatique, est juste une fonction qui prend en argument un mot de n bits et qui retourne une valeur logique VRAI ou FAUX. À toute fonction booléenne f à n variables, on peut associer canoniquement un graphe : son diagramme de décision binaire (BDD : Binary Decision Diagram) quasi-réduit. Cette technique est utilisée depuis longtemps dans la vérification des circuits.

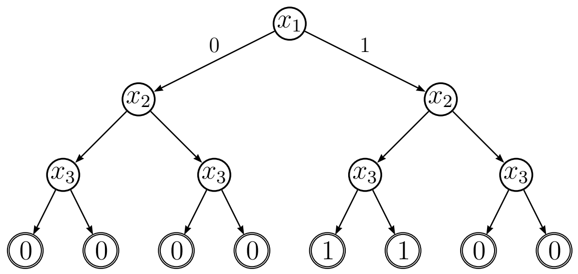


FIG. 6 – *Diagramme de Shannon de* $f = x_1x_2 + x_1$.

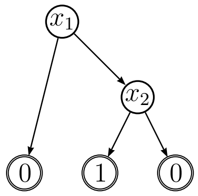


FIG. 7 – *Le BDD pour* $f = x_1x_2 + x_1$.

5.2 Les Diagrammes de Décision Binaire

Les graphes de décision binaires (BDD) sont des graphes orientés sans circuit, basés sur la décomposition de Shannon des fonctions booléennes. Ils ont été introduits en 1978 par Akers [1] pour représenter de façon compacte les fonctions booléennes. Puis en 1986, Bryant [29] propose les OBDD une représentation canonique des BDD ainsi que des algorithmes pour calculer efficament les opérations booléennes sur ces structures de données. Soit la fonction booléenne $f : \{0,1\}^3 \to \{0,1\}$ définie par $f(x_1,x_2,x_3) = x_1x_2 + x_1$. Son diagramme de Shannon est donné dans la figure 6. Après un certain nombre d'opérations de réduction sur ce diagramme, on obtient un BDD réduit. Le BDD correspondant à la fonction f est donné dans la figure 7.

6 Décomposition d'une fonction booléenne

Nous étudions ici l'orbite d'une fonction booléenne $f \in \mathbb{F}n$ sous l'action de l'algèbre $\mathcal{A}_n = \mathbb{Z}_2[\mathfrak{S}_n]$ [33] du groupe symétrique $\mathfrak{S}_n$ sur les variables dans le but de donner une décomposition de f à l'aide de la théorie de minimisation. Soit $\mathbb{F}n$ le $\mathcal{A}_n$-module à gauche des fonctions booléennes à n variables $(x_1,\ldots,x_n)$ et $f \in \mathbb{F}n$ une fonction booléenne. Considérons le sous-module $\mathcal{A}_n.f$. Il existe une décomposition du module $\mathcal{A}_n.f$ en une somme directe $\mathcal{A}_n.f = M_1 \oplus \cdots \oplus M_l$ de sous-modules indécomposables M_i. D'après le théorème de Krull-Schmidt, cette décomposition est unique à isomorphisme près.

$$
\begin{tikzcd}
 & 1 \arrow[dl, "\sigma_1"'] \arrow[dr, "\sigma_2"] \arrow[rr, dotted] & & 0 \\
\sigma_1 \arrow[d, "\sigma_2"'] & & \sigma_2 \arrow[d, "\sigma_1"] \arrow[r, dotted] & 1 \\
\sigma_2\sigma_1 \arrow[dr, "\sigma_1"] & & \sigma_1\sigma_2 \arrow[dl, "\sigma_2"'] \arrow[r, dotted] & 2 \\
 & \sigma_1\sigma_2\sigma_1 \arrow[rr, dotted] & & 3
\end{tikzcd}
$$

FIG. 8 – *Le permutoèdre pour* $n = 3$.

6.1 Algèbre du groupe symétrique

L'algèbre $\mathcal{A}_n = \mathbb{Z}_2[\mathfrak{S}_n]$ agit par permutations de variables sur l'ensemble des fonctions booléennes $\mathbb{F}n$. Elle est engendrée par les transpositions simples $S = (\sigma_1, \dots, \sigma_{n-1})$ où σ_i est la transposition de i et $i + 1$ et peut être présentée par les relations suivantes dites de Moore-Coxeter [33, 32] :

$$
\begin{cases}
{\sigma_i}^2 = 1, & \\
\sigma_i\sigma_j = \sigma_j\sigma_i & \text{si } |i-j| > 1, \\
\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}. &
\end{cases}
$$

Toute permutation $\sigma \in \mathfrak{S}_n$ est un produit de transpositions élémentaires. La longueur d'une permutation est nulle si et seulement si cette permutation est égale à 1. La longueur d'une permutation est égale à 1 si et seulement si cette permutation est une transposition élémentaire. Enfin, la longueur de l'inverse d'une permutation est égale à la longueur de la permutation (voir figure 8) [33]. L'algèbre $\mathcal{A}_n$ est une algèbre assoicative de type fini. Elle agit à gauche sur $\mathbb{Z}_2\langle x_1, \dots, x_n\rangle$ par l'action de σ_i définie sur les variables par :

$$
\begin{cases}
\sigma_i x_i = x_{i+1}, & \\
\sigma_i x_{i+1} = x_i, & \\
\sigma_i x_j = x_j & \text{si } j \neq i, i+1.
\end{cases}
$$

On rappelle que $S = \{\sigma_1, \dots, \sigma_{n-1}\}$ est l'ensemble de ces transpositions simples, $\mathbb{F}n$ un $\mathcal{A}_n$-module à gauche des fonctions booléennes à n variables. Il s'agit d'un $\mathbb{Z}_2$ espace vectoriel de dimension finie et on considère les sous-modules monogènes c'est à dire engendré par un seul élément (i.e. $\mathcal{A}_n.f$).

Théorème 6.1 (Krull-Schmidt) *Soit M un $\mathcal{A}_n$-module de dimension finie. Soient deux décompositions de M en $\mathcal{A}_n$-sous-modules indécomposables $M = M_1 \oplus \cdots \oplus M_r = N_1 \oplus \cdots N_s$ alors $r = s$ et il existe une permutation $\tau \in \mathfrak{S}_r$ telle que*

$$(\forall j \leq r)(M_j \simeq N_{\tau(j)}).$$

Il existe donc une décomposition du module $\mathcal{A}_n.f$ en une somme directe $\mathcal{A}_n.f = M_1 \oplus \cdots \oplus M_l$ de $\mathcal{A}_n$-sous-modules indécomposables, essentiellement unique d'après le théorème de Krull-Schmidt (6.1) (voir aussi [6]).

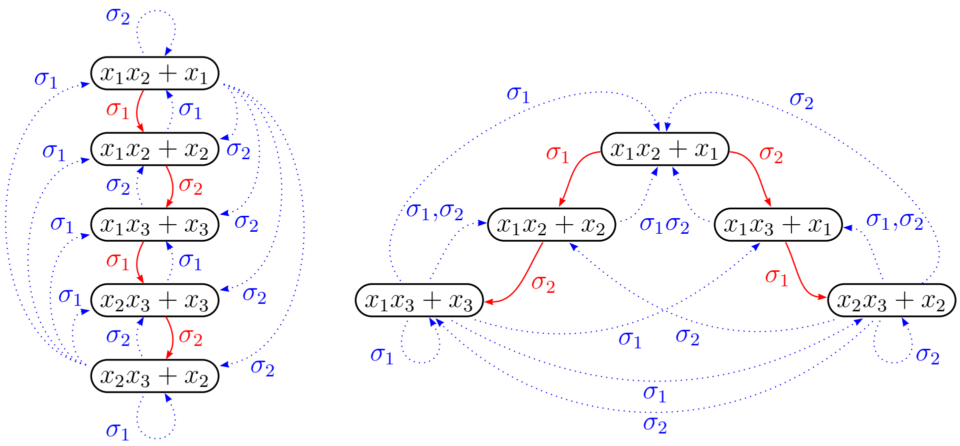


FIG. 9 – *L'ensemble suffixe et relateurs pour* $f = x_1x_2 + x_1$.

Le but de l'algorithme est donc de calculer une décomposition de $\mathcal{A}_n \cdot f$ par la connaissance de l'ensemble de projecteurs orthogonaux $\pi_i \in \mathrm{End}_{\mathcal{A}_n}(\mathcal{A}_n \cdot f)$ $(i = 1, \ldots, l)$ qui satisfont :

$$\begin{cases} \pi_i \circ \pi_i = \pi_i, \\ \pi_i \circ \pi_j = 0 \quad \text{si } i \neq j, \\ \pi_1 \oplus \cdots \oplus \pi_l = 1_{\mathrm{End}_{\mathcal{A}_n}(\mathcal{A}_n . f)}. \end{cases}$$

Ainsi, le module $\mathcal{A}_n \cdot f$ est somme directe de sous-modules $\pi_i(\mathcal{A}_n \cdot f) = \mathcal{A}_n\pi_i(f)$ qui sont engendrés par un seul élément. Si π_i est un tel projecteur, π_i doit être $\mathcal{A}_n$-linéaire.

6.2 Exemples de décompositions

On considère ici la fonction booléenne $f = x_1x_2 + x_1 \in \mathbb{F}3$. L'ensemble des relateurs dépend du choix de l'ordre du parcours de l'arbre des suffixes. En effet, la figure 9 montre bien que l'ensemble des relateurs n'est pas le même si on choisit l'ordre lexicographique gradué ou bien l'ordre lexicographique usuel. Dans notre cas, on considère l'ordre lexicographique gradué (graphe droite de la figure 9). L'ensemble suffixe est

$$P = \{\varepsilon, \sigma_1, \sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\}.$$

L'ensemble des relateurs est

$$R = \left\{ \begin{array}{l} \sigma_1\sigma_1 + \varepsilon, \\ \sigma_2\sigma_2 + \varepsilon, \sigma_1\sigma_2\sigma_2 + \sigma_1, \sigma_2\sigma_1\sigma_1 + \sigma_2, \\ \sigma_1\sigma_2\sigma_1 + (\varepsilon + \sigma_1 + \sigma_2 + \sigma_1\sigma_2 + \sigma_2\sigma_1), \\ \sigma_2\sigma_1\sigma_2 + (\varepsilon + \sigma_1 + \sigma_2 + \sigma_1\sigma_2 + \sigma_2\sigma_1). \end{array} \right\}.$$

Soit $\varphi \in \mathrm{End}_k(\mathcal{A}_3.f)$ et $f_\varphi \in \mathcal{A}_3.f$ tel que :

$$f_\varphi = \alpha_\varepsilon \varepsilon.f + \alpha_{\sigma_1}\sigma_1.f + \alpha_{\sigma_2}\sigma_2.f + \alpha_{\sigma_2\sigma_1}\sigma_2\sigma_1.f + \alpha_{\sigma_1\sigma_2}\sigma_1\sigma_2.f.$$

L'ensemble suffixe P et l'ensemble des relateurs R vont nous servir comme entrée dans l'algorithme $cons\_\varphi$ pour construire la matrice φ.

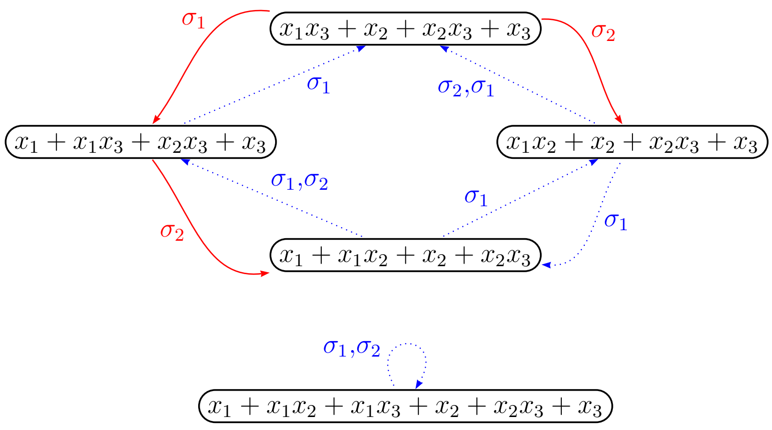


FIG. 10 – *Décomposition complète de* $\mathcal{A}_3.f$.

Selon l'algorithme $cons\_\varphi$, la matrice φ est la suivante :

$$\varphi = \begin{pmatrix} \alpha_\varepsilon & \alpha_{\sigma_1} + \alpha_{\sigma_1\sigma_2} & \alpha_{\sigma_2} + \alpha_{\sigma_2\sigma_1} & \alpha_{\sigma_2} + \alpha_{\sigma_2\sigma_1} & \alpha_{\sigma_1} + \alpha_{\sigma_1\sigma_2} \\ \alpha_{\sigma_1} & \alpha_\varepsilon + \alpha_{\sigma_1\sigma_2} & \alpha_{\sigma_1\sigma_2} + \alpha_{\sigma_2\sigma_1} & \alpha_{\sigma_2} & \alpha_{\sigma_1} + \alpha_{\sigma_2} \\ \alpha_{\sigma_2} & \alpha_{\sigma_1\sigma_2} + \alpha_{\sigma_2\sigma_1} & \alpha_\varepsilon + \alpha_{\sigma_2\sigma_1} & \alpha_{\sigma_1} + \alpha_{\sigma_2} & \alpha_{\sigma_1} \\ \alpha_{\sigma_1\sigma_2} & \alpha_{\sigma_1\sigma_2} & \alpha_{\sigma_1} + \alpha_{\sigma_2\sigma_1} & \alpha_\varepsilon + \alpha_{\sigma_2} & \alpha_{\sigma_1} + \alpha_{\sigma_2\sigma_1} \\ \alpha_{\sigma_2\sigma_1} & \alpha_{\sigma_2} + \alpha_{\sigma_1\sigma_2} & \alpha_{\sigma_2\sigma_1} & \alpha_{\sigma_2} + \alpha_{\sigma_1\sigma_2} & \alpha_\varepsilon + \alpha_{\sigma_2} \end{pmatrix}$$

Une solution non-triviale du système donné par $\varphi^2 = \varphi$, $\sigma \cdot \varphi(f) = \varphi(\sigma \cdot f)$ pour tout $\sigma \in P$ et $r \cdot \varphi(f) = 0$ pour tout $r \in R$ est :

$$f_\varphi = \sigma_2\sigma_1.f + \sigma_1\sigma_2.f$$

et

$$f_{1+\varphi} = \varepsilon.f + \sigma_2\sigma_1.f + \sigma_1\sigma_2.f$$

C'est à dire

$$f_\varphi = x_1x_3 + x_2 + x_2x_3 + x_3$$

et

$$f_{1+\varphi} = x_1 + x_1x_2 + x_1x_3 + x_2 + x_2x_3 + x_3$$

Ce qui nous donne $\mathcal{A}_3.f = \mathcal{A}_3.f_\varphi \oplus \mathcal{A}_3.f_{1+\varphi}$ et les décompositions complètes des modules $\mathcal{A}_3.f_\varphi$ et $\mathcal{A}_3.f_{1+\varphi}$ sont données dans la figure 10.

7 Application II : Module sur $\mathfrak{H}_k^n(0)$

7.1 L'algèbre de Hecke

L'algèbre de Hecke générique notée $\mathfrak{H}_k^n(q_1,q_2)$, qui peut être considérée comme une déformation à deux paramètres de l'algèbre du groupe symétrique, est l'algèbre sur l'anneau commutatif k présentée par les générateurs $(T_i)_{1\leq i<n}$ et les relations

$$\begin{cases} T_iT_j = T_jT_i & \text{si } |i-j| > 1, \\ T_iT_{i+1}T_i = T_{i+1}T_iT_{i+1}, & \\ (T_i - q_1)(T_i - q_2) = 0. & \end{cases}$$

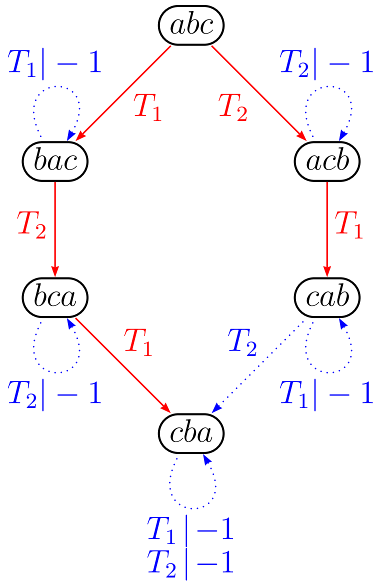


FIG. 11 – *Description de* $\mathfrak{H}_k^n(0) \cdot abc$

Les scalaires q_1 et q_2 sont les paramètres de l'algèbre. L'entier strictement positif n est son degré. L'algèbre $\mathfrak{H}_k^n(q_1,q_2)$ est de dimension $n!$ en tant que module sur k. Dans ce qui suit, on va s'intéresser à l'algèbre de Hecke à $q = 0$ sur $\mathbb{Q}$ que l'on notera $\mathfrak{H}_k^n(0)$.
Elle est engendrée par la famille $(T_i)_{1\leq i<n}$ et les relations

$$\begin{cases} T_iT_j = T_jT_i & \text{si } |i-j| > 1, \\ T_iT_{i+1}T_i = T_{i+1}T_iT_{i+1}, & \\ T_i(T_i+1) = 0. & \end{cases}$$

L'algèbre de Hecke $\mathfrak{H}_k^n(0)$ agit à gauche sur $\mathbb{Q}\langle a_1, \cdots, a_n\rangle$ comme suit :

$$\begin{cases} T_i(\dots a(i)a(i+1)\dots) = \dots a(i+1)a(i)\dots & \text{si } a(i) < a(i+1). \\ T_i(\dots a(i)a(i+1)\dots) = 0, & \text{si } a(i) = a(i+1). \\ T_i(\dots a(i)a(i+1)\dots) = -\dots a(i)a(i+1)\dots & \text{si } a(i) > a(i+1). \end{cases}$$

Où $a(i)$ est la lettre du mot argument à la place i.

7.2 Exemples de décompositions

Soit $m = abc \in \mathbb{Q}\langle a,b,c\rangle$. Une description complète de l'action de T_i sur $\mathfrak{H}_k^3(0) \cdot m$ est donnée dans la figure 11. En choisissant l'ordre lexicographique gradué pour le parcours de l'arbre des suffixes, l'ensemble suffixe est

$$P = \{\varepsilon, T_1, T_2, T_1T_2, T_2T_1, T_1T_2T_1\}.$$

L'ensemble des relateurs est ici

$$R = \left\{ \begin{array}{l} T_2^2 + T_2, T_1T_2^2 + T_1T_2, \\ T_2T_1^2 + T_2T_1, T_2T_1T_2 - T_1T_2T_1 \\ T_1T_2T_1^2 + T_1T_2T_1, T_1T_2T_1T_2 + T_1T_2T_1 \end{array} \right\}.$$

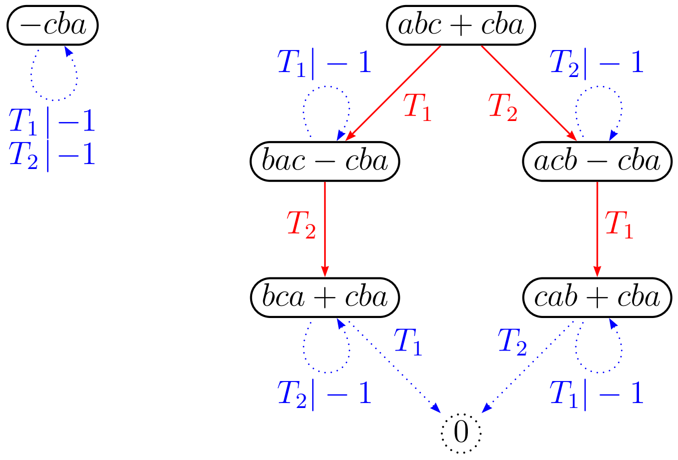


FIG. 12 – *Action de T_i sur $\mathfrak{H}_k^3(0)\cdot(-cba)$ et $\mathfrak{H}_k^3(0)\cdot(abc+cba)$.*

Soit $\varphi \in \mathrm{End}_{\mathcal{A}}(\mathcal{A}\cdot m)$ et $m_\varphi \in \mathcal{A}\cdot m$ tel que :

$$\begin{aligned} m_\varphi &= \alpha_\varepsilon \varepsilon\cdot m + \alpha_{T_1}T_1\cdot m + \alpha_{T_2}T_2\cdot m + \alpha_{T_1T_2}T_1T_2\cdot m \\ &\quad + \alpha_{T_2T_1}T_2T_1\cdot m + \alpha_{T_1T_2T_1}T_1T_2T_1\cdot m \end{aligned}$$

L'algorithme suffixe nous a retourné l'ensemble suffixe P et l'ensemble des relateurs R, on applique l'algorithme $cons\_\varphi$ qui va permettre de calculer la matrice φ et l'ensemble des projecteurs. La matrice φ est la suivante :

$$\varphi = \begin{pmatrix} \alpha T_\varepsilon & 0 & 0 & 0 & 0 & 0 \\ \alpha_{T_1} & \alpha_{T_\varepsilon}-\alpha_{T_1} & 0 & 0 & 0 & 0 \\ \alpha_{T_2} & 0 & \alpha_{T_\varepsilon}-\alpha_{T_2} & 0 & 0 & 0 \\ \alpha_{T_1T_2} & 0 & \alpha_{T_1}-\alpha_{T_1T_2} & \alpha_{T_\varepsilon}-\alpha_{T_1} & 0 & 0 \\ \alpha_{T_2T_1} & \alpha_{T_2}-\alpha_{T_2T_1} & 0 & 0 & \alpha_{T_\varepsilon}-\alpha_{T_2} & 0 \\ \alpha_{T_1T_2T_1} & \alpha_{T_1T_2}-\alpha_{T_1T_2T_1} & \alpha_{T_2T_1}-\alpha_{T_1T_2T_1} & \begin{array}{c}\alpha_{T_2}-\alpha_{T_1T_2}\\ -\alpha_{T_2T_1}\\ +\alpha_{T_1T_2T_1}\end{array} & \begin{array}{c}\alpha_{T_1}-\alpha_{T_1T_2}\\ -\alpha_{T_2T_1}\\ +\alpha_{T_1T_2T_1}\end{array} & \begin{array}{c}\alpha_{T_\varepsilon}\alpha_{T_1}-\alpha_{T_1T_2}\\ -\alpha_{T_1T_2}-\alpha_{T_2T_1}\\ +\alpha_{T_1T_2T_1}\end{array} \end{pmatrix}$$

Une solution non-triviale du système donné par $\varphi^2=\varphi$, $T\cdot\varphi(m)=\varphi(T\cdot m)$ pour tout $T\in P$ et $r\cdot\varphi(m)=0$ pour tout $r\in R$ est : $m_\varphi = -T_1T_2T_1\cdot m$ et $m_{1-\varphi}=\varepsilon\cdot m + T_1T_2T_1\cdot m$, c'est à dire $m_\varphi=-cba$ et $m_{1-\varphi}=abc+cba$. Ce qui nous donne une première décomposition $\mathfrak{H}_k^3(0)\cdot abc = -\mathfrak{H}_k^3(0)\cdot cba + \mathfrak{H}_k^3(0)\cdot(abc+cba)$ donnée dans la figure 12. On applique maintenant l'algorithme sur le sous-module $\mathfrak{H}_k^3(0)\cdot m'$ avec $m'=(abc+cba)$ pour voir s'il est décomposable ou non. L'ensemble suffixe est

$$P=\{\varepsilon, T_1, T_2, T_1T_2, T_2T_1\}.$$

L'ensemble des relateurs est

$$R=\left\{\begin{array}{l} T_1T_2T_1,\, T_2T_1T_2, \\ T_1^2+T_1,\, T_2^2+T_2, \\ T_1T_2^2+T_1T_2,\, T_2T_1^2+T_2T_1 \end{array}\right\}.$$

Soit $\varphi\in\mathrm{End}_{\mathcal{A}}(\mathcal{A}\cdot m')$ et $m'_\varphi\in\mathcal{A}\cdot m'$ tel que :

$$m'_\varphi = \alpha_\varepsilon\varepsilon\cdot m' + \alpha_{T_1}T_1\cdot m' + \alpha_{T_2}T_2\cdot m' + \alpha_{T_1T_2}T_1T_2\cdot m' + \alpha_{T_2T_1}T_2T_1\cdot m'.$$

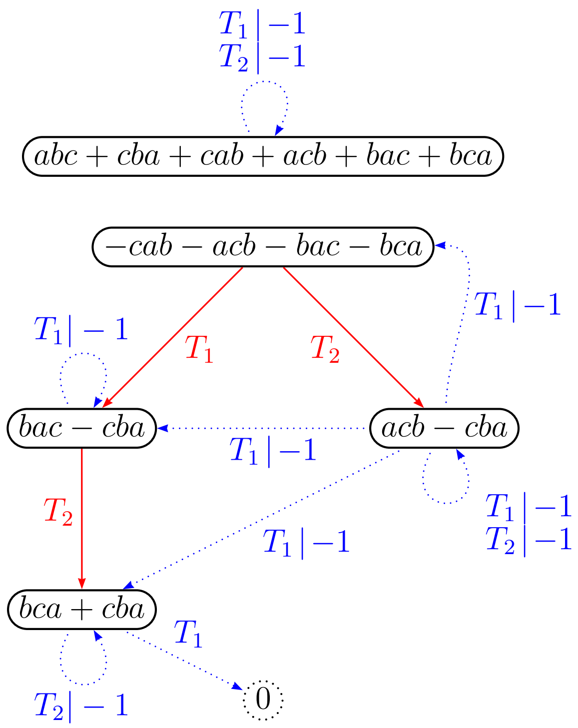


FIG. 13 – *Action de T_i sur $\mathfrak{H}_k^3(0) \cdot m'_\varphi$ et $\mathfrak{H}_k^3(0) \cdot m'_{1-\varphi}$.*

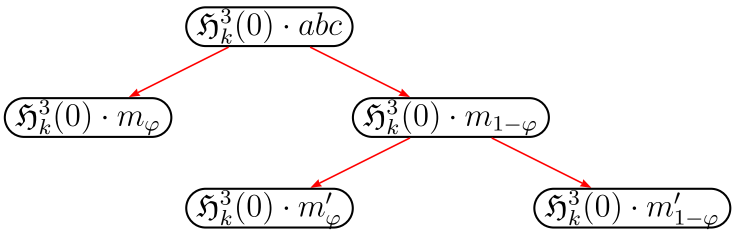


FIG. 14 – *Décomposition complète de $\mathfrak{H}_k^3(0) \cdot abc$.*

La matrice m'_φ est la suivante :

$$\varphi = \begin{pmatrix} \alpha T_\varepsilon & 0 & 0 & 0 & 0 \\ \alpha_{T_1} & \alpha_{T_\varepsilon} - \alpha_{T_1} & 0 & 0 & 0 \\ \alpha_{T_2} & 0 & \alpha_{T_\varepsilon} - \alpha_{T_2} & 0 & 0 \\ \alpha_{T_1T_2} & 0 & \alpha_{T_1} - \alpha_{T_1T_2} & \alpha_{T_\varepsilon} - \alpha_{T_1} & 0 \\ \alpha_{T_2T_1} & \alpha_{T_2} - \alpha_{T_2T_1} & 0 & 0 & \alpha_{T_\varepsilon} - \alpha_{T_2} \end{pmatrix}$$

Une solution non-triviale du système donné par $\varphi^2 = \varphi$, $T \cdot \varphi(m') = \varphi(T \cdot m')$ pour tout $T \in P$ et $r \cdot \varphi(m') = 0$ pour tout $r \in R$ est $m'_\varphi = -T_1 \cdot m' - T_2 \cdot m' - T_1T_2 \cdot m' - T_2T_1 \cdot m'$ et $m'_{1-\varphi} = \varepsilon \cdot m' + T_1 \cdot m' + T_2 \cdot m' + T_1T_2 \cdot m' + T_2T_1 \cdot m'$, c'est à dire $m'_\varphi = -cab - acb - bac - bca$ et $m'_{1-\varphi} = abc + cba + cab + acb + bac + bca$ et la description complète de $\mathfrak{H}_k^3(0) \cdot (abc + cba)$ est donnée dans la figure 13. La décomposition complète du $\mathfrak{H}_k^3(0)$-module $\mathfrak{H}_k^3(0) \cdot abc$ est donnée dans la figure 14.

8 Description du programme DEC-MOD

Nous allons manipuler maintenant notre algorithme de décomposition de module en MuPAD pour l'appliquer sur des modules sur l'algèbre du groupe symétrique ou sur l'algèbre de Hecke à $q = 0$. Nous commençons par le cas des groupes symétriques. Pour cela, on doit définir le domaine des modules sur cette algèbre.

```
>> F:=Dom::FreeModuleTable(Dom::IntegerMod(2),combinat::words)

      Dom::FreeModuleTable(Dom::IntegerMod(2), combinat::words)
```

Soit $f : \{0,1\}^3 \to \{0,1\}$ définie par $f(X_1,X_2,X_3) = X_1X_3 + X_1$. On définit maintenant le module $\mathcal{A}_3 \cdot f$ comme suit :

```
>> G:=F([1,0,1])+F([1,0,0])

                          B([1, 0, 1]) + B([1, 0, 0])
```

Une fois qu'on a le module, on peut appliquer l'algorithme :

```
>> decomposition(3,G,2)

      {[x1 = 0, x2 = 0, x3 = 0, x4 = 0, x5 = 0],

       [x1 = -1, x2 = 0, x3 = 0, x4 = 0, x5 = 0],

       [x1 = 0, x2 = 0, x3 = 0, x4 = -1, x5 = -1],

       [x1 = -1, x2 = 0, x3 = 0, x4 = -1, x5 = -1]}
```

D'après l'ensemble des projecteurs, le module $\mathcal{A}_3 \cdot f$ se décompose en $\mathcal{A}_3 \cdot (X_2X_3 + X_3)$ et $\mathcal{A}_3 \cdot (X_1X_2 + X_2)$. On applique le même algorithme sur les sous-modules $\mathcal{A}_3 \cdot (X_2X_3 + X_3)$ et $\mathcal{A}_3 \cdot (X_1X_2 + X_2)$, pour voir s'ils sont décomposables ou non :

```
>> G1:=F([0,1,1])+F([0,0,1])

                          B([0, 1, 1]) + B([0, 0, 1])

>> G2:=G+G1

   B([1, 0, 1]) + B([1, 0, 0]) + B([0, 1, 1]) + B([0, 0, 1])

>> decomposition(3,G1,2)

     {[x1 = 0, x2 = 0, x3 = 0, x4 = 0],

      [x1 = -1, x2 = 0, x3 = 0, x4 = 0]}

>> decomposition(3,G2,2)
```

```
{[x1 = 0], [x1 = -1]}
```

Les deux sous-modules ne sont donc pas décomposables et une somme directe pour le module $\mathcal{A}_3 \cdot f$ est

$$\mathcal{A}_3 \cdot f = \mathcal{A}_3 \cdot (X_2X_3 + X_3) \oplus \mathcal{A}_3 \cdot (X_1X_2 + X_2)$$

On définit maintenant le domaine des modules sur l'algèbre de Hecke à $q = 0$ $\mathfrak{H}_k^3(0)$.

```
>>F:=Dom::FreeModuleTable(Dom::Rational,combinat::integerVectors)

   Dom::FreeModuleTable(Dom::Rational, combinat::integerVectors)
```

Ensuite, le module $\mathfrak{H}_k^3(0) \cdot abc$.

```
>> G:=F([1,2,3])

                          B([1, 2, 3])
```

On applique maintenant l'algorithme pour voir si $\mathfrak{H}_k^3(0) \cdot abc$ est décomposable ou non.

```
  {[x1 = 0, x2 = 0, x3 = 0, x4 = 0, x5 = 0, x6 = 0],

   [x1 = 0, x2 = 0, x3 = 0, x4 = 0, x5 = 0, x6 = -1],

   [x1 = 1, x2 = 0, x3 = 0, x4 = 0, x5 = 0, x6 = 0],

   [x1 = 1, x2 = 0, x3 = 0, x4 = 0, x5 = 0, x6 = 1],

   [x1 = 0, x2 = -1, x3 = -1, x4 = -1, x5 = -1, x6 = 0],

   [x1 = 0, x2 = -1, x3 = -1, x4 = -1, x5 = -1, x6 = -1],

   [x1 = 1, x2 = 1, x3 = 1, x4 = 1, x5 = 1, x6 = 0],

   [x1 = 1, x2 = 1, x3 = 1, x4 = 1, x5 = 1, x6 = 1]}
```

D'après l'ensemble des projecteurs, et en choisissant le deuxième projecteur, le module se décompose en $\mathfrak{H}_k^3(0) \cdot (-cba)$ et $\mathfrak{H}_k^3(0) \cdot (abc + cba)$. On vérifie maitenant si le sous-module $\mathfrak{H}_k^3(0) \cdot (abc + cba)$ est décomposable ou non.

```
>> G1:=F([1,2,3])+F([3,2,1])

                        B([1, 2, 3]) + B([3, 2, 1])


  {[x1 = 0, x2 = 0, x3 = 0, x4 = 0, x5 = 0],
```

```
[x1 = 1, x2 = 0, x3 = 0, x4 = 0, x5 = 0],

[x1 = 0, x2 = -1, x3 = -1, x4 = -1, x5 = -1],

[x1 = 1, x2 = 1, x3 = 1, x4 = 1, x5 = 1]}
```

Si on choisit le troisième projecteur, le sous-module $\mathfrak{H}_k^3(0) \cdot (abc + cba)$ se décompose en $\mathfrak{H}_k^3(0) \cdot (-bac - acb - bca - cab)$ et $\mathfrak{H}_k^3(0) \cdot (abc + cba + bac + acb + bca + cab)$ et une somme directe du module $\mathfrak{H}_k^3(0) \cdot abc$ est

$$\begin{aligned}\mathfrak{H}_k^3(0) \cdot abc = \mathfrak{H}_k^3(0) \cdot (-cba) \\ \oplus \mathfrak{H}_k^3(0) \cdot (-bac - acb - bca - cab) \\ \oplus \mathfrak{H}_k^3(0) \cdot (abc + cba + bac + acb + bca + cab).\end{aligned}$$

On peut manipuler aussi la fonction suffixe qui calcule une base pour l'espace $\mathcal{A} \cdot m$ et un ensemble de relateurs. Nous allons l'appliquer pour le module $\mathfrak{H}_k^3(0) \cdot abc$.

```
>> suffixe(3,G,1)

 [
  [[0], B([1, 2, 3])],
  [[0, 1], B([2, 1, 3])],
  [[0, 2], B([1, 3, 2])],
  [[0, 1, 2], B([2, 3, 1])],
  [[0, 2, 1], B([3, 1, 2])],
  [[0, 1, 2, 1], B([3, 2, 1])]]


          table(
                      table(
          [0, 1, 2, 1, 2] =    [0, 1, 2, 1] = -1 ,
                           )
                      table(
          [0, 1, 2, 1, 1] =    [0, 1, 2, 1] = -1 ,
                           )
                      table(
          [0, 2, 1, 2] =    [0, 1, 2, 1] = 1 ,
                           )
                      table(
          [0, 2, 1, 1] =    [0, 2, 1] = -1 ,
                           )
                      table(
          [0, 1, 2, 2] =    [0, 1, 2] = -1 ,
                           )
                      table(
          [0, 2, 2] =    [0, 2] = -1 ,
```

```
                    )
                table(
[0, 1, 1] =       [0, 1] = -1 ,
                    )
                table(
[0] =     [0] = 1
                    )
)
```

8.1 Cas des groupes finis : Caractères

Dans ce qui suit les espace vectoriel sont supposés sur k ($= \mathbb{R}$ ou $\mathbb{C}$) et les groupes sont supposés finis.

Définition 8.1 *Soit G un groupe et V un EV. On appelle représentation de G dans V une application $\rho\ :\ G \mapsto Aut(V)$ compatible avec la multiplication, c'est à dire que*

$$(\forall g_1,g_2 \in G)(\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)) \tag{34}$$

Avec cette donnée, V est appelé G-module. L'image $\rho(g)[v]$ se note souvent $g.v$.

Exercice 8.2 *Soit G, un groupe et ρ_G une représentation de l'ensemble G dans l'espace vectoriel V.*
Montrer que les conditions suivantes sont équivalentes :
i) ρ_G est une représentation du groupe G
ii) ρ_G est une représentation du semigroupe G et $\rho_G(1_G) = Id_V$.

Selon le schema général, on dit qu'une application linéaire (k-linéaire) entre deux G-modules $\phi\ :\ V_1 \mapsto V_2$ est G-linéaire si les actions de G agissent comme des scalaires (c'est à dire permutent avec ϕ ou peuvent être "sorties" de ϕ). Si ϕ est bijective (ou inversible) on dit que V_1 et V_2 sont isomorphes (c'est à dire "ont même forme"). On dit qu'une représentation V (de G) contient une autre (disons W), s'il y a un sous-module de V qui est isomorphe à W. À cause de l'unicité des décompositions, on voit que la *signature* du G-module V est l'ensemble des "types" de modules qu'il contient (avec leur multiplicités). Il nous faut d'abord étudier une représentation modèle, c'est à dire qui contient toutes les autres.

Exercice 8.3 *Pour le module de la figure (4), écrire les matrices de transition. Montrer que ce module est irréductible.*
*Donner la fonction trace (i.e. $g \to tr(\rho(g))$ (voir le paragraphe (**??**)).*

8.1.1 Un modèle qui contient toutes les représentations : la représentation régulière

Exercice 8.4 *Soit G, un groupe fini. On considère la AAU $\mathcal{A} = \mathbb{C}[G]$ (sommes à coefficients complexes $\sum_{g\in G} \alpha_g g$) et les opérateurs $\gamma_h\ :\ \sum_{g\in G} \alpha_g g \to \sum_{g\in G} \alpha_g h.g$ ($= h.\sum_{g\in G} \alpha_g g$ dans $\mathcal{A}$).*
1) a) Montrer que $g \mapsto \gamma_g$ est une représentation de G.
2) Soit

$$\mathbb{C}[G] = \oplus_{i=1..n} V_i \tag{35}$$

une décomposition en modules (i.e. sous espace vectoriel stables pour l'action des γ_g, c'est à dire les multiplications à gauche) et $1_G = \sum_{i=1}^n e_i$ la décomposition de 1_G selon (44)[6].
a) Montrer que l'on a
i) $1_G = \sum_{i=1}^n e_i$
ii) $(\forall i \in [1..n])(e_i e_i = e_i)$
iii) $(\forall i,j \in [1..n])(i \neq j \Longrightarrow e_i e_j = e_j e_i = 0)$
b) Inversement, montrer que, si une famille d'éléments de $\mathbb{C}[G]$ vérifie (ex 8.4.2.a), on a (44) avec $V_i = \mathbb{C}[G]e_i$.

Commentaire. — Une famille $(e_i)_{i=1..n}$ d'idempotents qui vérifie les conditions de l'exercice (8.4) est appelée FCIO, *famille complète d'idempotents orthogonaux*. Si, de plus, les modules $\mathcal{A}e_i$ sont irréductibles, cette famille est appelée FCIOM, *famille complète d'idempotents orthogonaux minimaux.* $\diamondsuit$

Exercice 8.5 *Utiliser l'exercice (3.11) pour montrer que, dans $\mathcal{A} = \mathbb{C}[G]$, on peut toujours construire une FCIOM.*

Exercice 8.6 *(Cette version "effective" du théorème de Wedderburn est due à Marianne Flouret [22])*
1) a) Soient $e,f \in \mathcal{A}$ deux idempotents, montrer que la formule

$$\phi_{fae}(x) = xfae \tag{36}$$

définit un élément de $\mathrm{Hom}_G(\mathcal{A}f,\mathcal{A}e)$.
b) Montrer que la correspondance $fae \to \phi_{fae}(x)$, $f\mathcal{A}e \mapsto \mathrm{Hom}_G(\mathcal{A}f,\mathcal{A}e)$ est un isomorphisme d'espace vectoriel s.
c) En déduire que, si $\mathcal{A}e$ et $\mathcal{A}f$ sont irréductibles, $f\mathcal{A}e$ soit de dimension 0 (si $\mathcal{A}e$ et $\mathcal{A}f$ ne sont pas du même type) soit de dimension 1 (si $\mathcal{A}e$ et $\mathcal{A}f$ sont du même type).
2) Soit $(e_1^{(1)},\cdots e_{n_1}^{(1)},e_1^{(2)},\cdots e_{n_2}^{(2)},\cdots\cdots,e_1^{(k)},\cdots e_{n_k}^{(k)})$ une FCIOM rangés selon les types des $\mathcal{A}e_i^{(j)}$. Pour chaque bloc $e_1^{(j)},\cdots e_{n_j}^{(j)}$, et chaque $l \in [1..n_j-1]$ on prend un élément $e_l^{(j)}a_l^{(j)}e_{l+1}^{(j)}$ tel que $\neq 0$ (on rappelle que pour deux idempotents e,f de la liste, on a

$$dim(f\mathcal{A}e) = [e \textit{ et } f \textit{ sont de même type}])$$

on construit ensuite les éléments $E_{l,l+1}^{(j)} = e_l^{(j)}a_l^{(j)}e_{l+1}^{(j)}$ puis, pour $1 \leq l < m \leq n_j$

$$E_{l,m}^{(j)} = E_{l,l+1}^{(j)}E_{l+1,l+2}^{(j)}\cdots E_{m-1,m}^{(j)} \tag{37}$$

ensuite on choisit $a_{n_j}^{(j)}$ de façon que $E_{n_j,1}^{(j)} = e_{n_j}^{(j)}a_{n_j}^{(j)}e_1^{(j)}$ vérifie $E_{1,n_j}^{(j)}E_{n_j,1}^{(j)} = e_1^{(j)}$ puis, pour $1 \leq m \leq l \leq n_j$

$$E_{l,m}^{(j)} = E_{l,l+1}^{(j)}E_{l+1,l+2}^{(j)}\cdots E_{n_j-1,n_j}^{(j)}E_{n_j,1}^{(j)}E_{1,2}^{(j)}E_{2,3}^{(j)}\cdots E_{m-1,m}^{(j)} \tag{38}$$

6. On dit aussi résolution de l'unité.

a) Montrer que les $E^{(j)}_{l,m}$ forment un système d'unités matricielles c'est à dire que

$$E^{(j)}_{a,b}E^{(j)}_{c,d} = [b = c]E^{(j)}_{a,d} \tag{39}$$

et que $E^{(j)}_{a,a} = e_a(j)$
b) Montrer que la famille $\left(E^{(j)}_{a,b}\right)_{1\leq j\leq k \top 1\leq a,b\leq n_j}$ est une base de $\mathbb{C}[G]$.

8.1.2 Construction d'une FCIOM pour le groupe symétrique

Nous allons construire une FCIOM grâce à une algorithme extrêmement efficace donné par la définition d'un drapeau de polynômes, les GZ-polynômes[7]. Cette construction repose sur l'emboîtement des groupes symétriques

$$\mathfrak{S}_0 \subset \mathfrak{S}_1 \subset \mathfrak{S}_2 \subset \cdots \subset \mathfrak{S}_n \subset \mathfrak{S}_{n+1} \cdots \tag{40}$$

Exercice 8.7 *(Ici, $k = \mathbb{R}$ et G est un groupe fini) Soit V, un G-module de dimension finie. On dit qu'un produit scalaire $\langle .|. \rangle$ sur V est invariant par G si*

$$(\forall g \in G)(\forall u,v \in V)(\langle g.u|g.v\rangle = \langle u|v\rangle) \tag{41}$$

1) Montrer que si $W \subset V$ est stable, il en est de même de $W^\perp$.
2) Reprendre l'exercice précédent avec $k = \mathbb{C}$ et un produit scalaire hermitien.
3) Montrer, d'une autre façon que dans l'exercice (8.4), que la représentation régulière contient toutes les représentations.
On munit $\mathcal{A} = \mathbb{C}[G]$ de

$$\langle \sum_{g\in G} \alpha\ g | \sum_{g\in G} \beta\ g\rangle = \sum_{g\in G} \bar{\alpha}\beta. \tag{42}$$

3) a) Vérifier que (42) définit bien un produit scalaire (hermitien) pour lequel les points de G (i.e. les fonctions caractéristiques) forment une base orthogonale.
b) Montrer que

$$(\forall g \in G)(\forall\ u,v \in \mathcal{A})(\langle u|v\rangle = \langle \gamma_g(u)|\gamma_g(v)\rangle) \tag{43}$$

(c'est à dire que ce produit scalaire est invariant, voir l'exercice (8.7)).
c) En déduire qu'il existe une décomposition de type (44) en sous-modules irréductibles (les idempotents correspondants seront dits minimaux).
4) a) Soit U un G-module irréductible et x une de ses vecteurs non nuls. Soit

$$ann(x) = \{h \in \mathbb{C}[G] \mid h.x = 0\}.$$

Montrer que $ann(x)^\perp$ est un sous module de $\mathbb{C}[G]$ (en tant que G-module à gauche) et que $U \simeq ann(x)^\perp$.
b) Soit $\mathbb{C}[G] = \oplus_{i=1}^n V_i$ une décomposition en sous-modules irréductibles. Montrer qu'il existe un indice $j \in [1..n]$ (et un seul) tel que

$$\mathbb{C}[G] = (\oplus_{i=1..j-1}V_i) \oplus (ann(x)^\perp) \oplus (\oplus_{i=j+1..n}V_i) \tag{44}$$

c) En déduire que $\mathbb{C}[G]$ contient (au moins) une copie de chaque représentation irréductible de G.
5) Ici $G = \mathfrak{S}_n$. On considère, dans $\mathbb{C}[G]$, les éléments de Jucys-Murphy $(x_m)_{2\leq m\leq n}$ (voir [35] et [36]) définis par

---

7. Version simplifiée de la construction que l'on peut trouver dans la thèse d'Éric Laugerotte[21].

$$x_m \;=\; \sum_{i=1}^{m-1} \sigma_{(i,m)} \textit{ où } \sigma_{(i,m)} \textit{ est la transposition de } i \textit{ et de } m. \tag{45}$$

a) Montrer les relations suivantes. a1) Si $i,j \in [2..n]$ *tels que* $i < j-1$*,*

$$[\sigma_i, x_j] \;=\; 0. \tag{46}$$

a2) Si $i = j-1$*,*

$$\sigma_{j-1} x_j \;=\; 1 + x_{j-1}\sigma_{j-1} \tag{47}$$

a3)

$$x_j \sigma_{j-1} \;=\; 1 + \sigma_{j-1} x_{j-1}. \tag{48}$$

b) Déduire des relations 46, 47 et 48, la relation de commutation

$$[x_i, x_j] = 0. \tag{49}$$

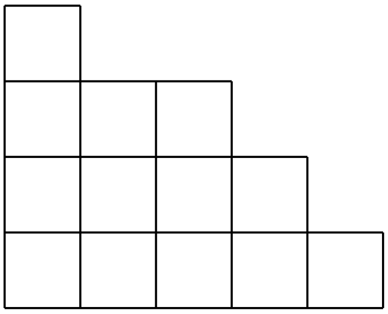


FIG. 15 – *Le diagramme de Ferrers de* $(5,4,3,1)$.

Les modules irréductibles sur $\mathfrak{S}_n$ sont indexés par des diagrammes de Ferrers à n cases.
Les polynômes qui servent à la construction d'une FCIOM sont calculés par rapport à un objet combinatoire que l'on nomme *tableau de Young*.

On désigne par t un *tableau* de Young (voir [12], [39] ou [40]) de forme λ, un remplissage du diagramme de Ferrers de forme λ par des lettres appartenant à un alphabet $\{a_1, a_2 \ldots\}$, ordonné par $(a_1 < a_2 < \cdots)$, tel que les mots lus de la gauche vers la droite sur les lignes soient croissants et les mots lus sur les colonnes de bas en haut soient strictement croissants.
Un tableau de Young est dit standard lorsqu'il ne comporte aucune répétition. Il est utile pour la suite, sans perte de généralité, de prendre comme alphabet l'ensemble $[1..n]$ muni de l'ordre usuel sur les entiers.
Précisons l'action des x_m sur $\mathcal{H}^n_{\mathbb{Q}(q)}(q)$.
Les *GZ-polynômes*, indexés par les tableaux de Young et notés GZ_t, seront définis récursivement comme suit,

$$GZ_t = \begin{cases} 1 & \text{si } t \text{ est de poids } 1, \\ GZ_{t-n} \times \displaystyle\prod_{\substack{t'-n=t-n \\ t' \neq t}} \frac{X_n - \chi_{t'}(n)}{\chi_t(n) - \chi_{t'}(n)} & \text{si } t \text{ est de poids } n. \end{cases}$$

Théorème 8.8 *Posons* $t \in \mathit{Tab}(n)$*,* $GZ_t\,(x_2, x_3, \ldots, x_n) = g_t$*. Alors* $(g_t)_{t \in \mathit{Tab}(n)}$ *est une FCIOM de* $\mathbb{C}[\mathfrak{S}_n]$ *(qui est d'ailleurs dans* $\mathbb{Q}[\mathfrak{S}_n]$*).*

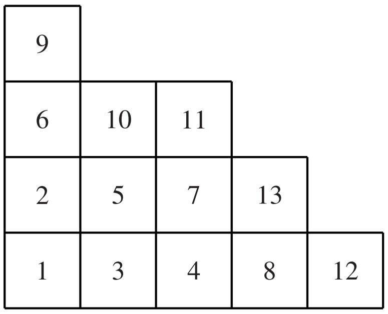


FIG. 16 – *Un tableau de Young de forme* $(5,4,3,1)$.

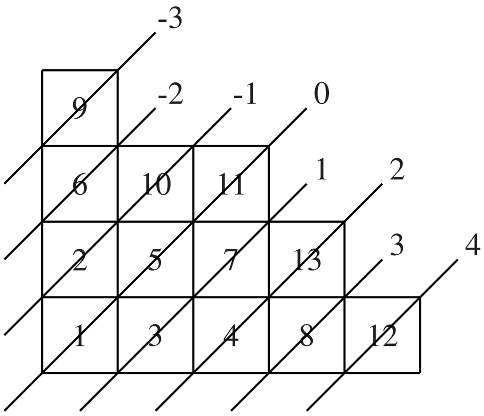


FIG. 17 – *Les diagonales d'un tableau de Young.*

Preuve Soit h_t l'évaluation du polynôme GZ_t en $(x_2,x_3,\ldots,x_n)$. Quand $n = 2$, les GZ-polynômes sont les suivants,

$$\begin{aligned} GZ_{(1,1)^c} &= \frac{-1}{2}\left(X_2 - 1\right), \\ GZ_{(2)^c} &= \frac{1}{2}\left(X_2 + 1\right). \end{aligned}$$

À l'aide de quelques calculs simples, on montre que

$$\begin{aligned} \chi_{(1,1)^c}\left(h_{(1,1)^c}\right) &= 1, \\ \chi_{(2)^c}\left(h_{(1,1)^c}\right) &= 0, \\ \chi_{(1,1)^c}\left(h_{(2)^c}\right) &= 0, \\ \chi_{(2)^c}\left(h_{(2)^c}\right) &= 1. \end{aligned}$$

On suppose maintenant $n > 2$. Pour tout tableau de Young $t \in \text{Tab}(n)$, on déduit de la formule du polynôme GZ_t que, si $t_0 \in \text{Tab}(n)$,

$$\chi_{t_0}\left(h_t\right) = \chi_{t_0}\left(h_{t-n}\right)\chi_{t_0}\left(\prod_{\substack{t'-n=t-n \\ t'\neq t}} \frac{x_n - \chi_{t'}(x_n)}{\chi_t(x_n) - \chi_{t'}(x_n)}\right).$$

Comme X_n n'intervient pas dans l'expression du polynôme GZ_{t-n}, on a

$$\chi_{t_0}\left(h_{t-n}\right) = \chi_{t_0-n}\left(h_{t-n}\right).$$

Par conséquent,

$$\chi_{t_0}(h_t) = \chi_{t_0-n}(h_{t-n}) \prod_{\substack{t'-n=t-n \\ t'\neq t}} \frac{\chi_{t_0}(x_n) - \chi_{t'}(x_n)}{\chi_t(x_n) - \chi_{t'}(x_n)}.$$

Si $t_0 = t$, $\chi_t(h_t) = \chi_{t-n}(h_{t-n}) = 1$ par induction. Si $t_0 \neq t$ et $t_0 - n = t - n$, par construction on a $\chi_{t_0}(h_t) = 0$. Si $t_0 \neq t$ et $t_0 - n \neq t - n$, $\chi_{t_0-n}(h_{t-n}) = 0$ par induction, et ainsi $\chi_{t_0}(h_t) = 0$. △

Cette famille vérifie une relation dont l'importance sera mise en évidence lorsque l'on discutera de l'efficacité du calcul.

Proposition 8.9 *Les éléments de la FCIOM $(g_t)_{t\in Tab(n)}$ vérifient*

$$g_t = \sum_{\substack{t'\in Tab(n+1) \\ t'-(n+1)=t}} g_{t'}. \tag{50}$$

Preuve Soit $s_t = \sum_{\substack{t'\in \mathrm{Tab}(n+1) \\ t'-(n+1)=t}} g_{t'}$. D'après le théorème 8.8, on a

$$\begin{aligned} g_t s_t &= g_t \sum_{\substack{t'\in \mathrm{Tab}(n+1) \\ t'-(n+1)=t}} g_t \prod_{\substack{t"-(n+1)=t'-(n+1) \\ t"\neq t'}} \frac{x_{n+1} - \chi_{t"}(x_{n+1})}{\chi_{t'}(x_{n+1}) - \chi_{t"}(x_{n+1})} \\ &= \sum_{\substack{t'\in \mathrm{Tab}(n+1) \\ t'-(n+1)=t}} g_t \prod_{\substack{t"-(n+1)=t'-(n+1) \\ t"\neq t'}} \frac{x_{n+1} - \chi_{t"}(x_{n+1})}{\chi_{t'}(x_{n+1}) - \chi_{t"}(x_{n+1})} \\ &= s_t. \end{aligned}$$

De même, $g_{t'} s_t = 0$ si t' est un tableau de poids n distinct de t. Cependant

$$\sum_{t\in \mathrm{Tab}(n)} s_t = \sum_{t\in \mathrm{Tab}(n+1)} g_t = 1 \tag{51}$$

ce qui prouve que $g_t = s_t$. △

Sans évaluer, les GZ-polynômes satisfont deux importantes relations.

Proposition 8.10 *Les GZ-polynômes vérifient*

$$GZ_t = \sum_{\substack{t'\in Tab(n+1) \\ t'-(n+1)=t}} GZ_{t'}, \tag{52}$$

$$\sum_{t\in Tab(n)} GZ_t = 1. \tag{53}$$

Preuve La relation (52) est déduite de la définition récursive des GZ-polynômes et de la relation formelle

$$\sum_{i=1}^{m} \prod_{j\neq i} \frac{X - a_j}{a_i - a_j} = 1$$

qui est vraie pour toute famille $(a_1, a_2, \ldots, a_m)$ de scalaires distincts. La relation (53) est une application directe de (52). △

8.1.3 Étude rapide de la complecité du calcul

On constate que les formules des GZ-polynômes sont moins “complexes” que les formules des polynômes DJ obtenues par l'interpolation de Lagrange. On peut fixer deux opérations élémentaires qui sont l'addition d'éléments de la forme $\sigma \in \mathfrak{S}_n$ et le produit d'un générateur σ_i et de σ. Comme $T_{(i,m)}$ (transposition de i et de m) se décompose en $\sigma_i \cdots \sigma_{m-2}\sigma_{m-1}\sigma_{m-2} \cdots \sigma_i$, le produit $x_m\sigma$ nécessite au minimum $(m-1)m$ opérations élémentaires. La proposition suivante montre que les polynômes GZ_t sont minimaux en la variable X_n qui est la plus coûteuse en calculs lors de l'évaluation en les q- analogues de Jucys-Murphy. On note $\deg_i(Q)$ le degré du polynôme Q en X_i.

Proposition 8.11 *Si $Q_t \in k[X_i]_{1<i\leq n}$ vérifie $Q_t\,(x_2,x_3,\ldots,x_n) = g_t$ alors*

$$deg_n(Q_t) \geq deg_n\,(GZ_t)\,. \tag{54}$$

De plus, si on a égalité,

$$Q_t = \prod_{\substack{t'-n=t-n \\ t'\neq t}} \frac{X_n - \chi_{t'}\,(x_n)}{\chi_t\,(x_n) - \chi_{t'}\,(x_n)} \times Q_{t-n} + R \tag{55}$$

avec $Q_{t-n} \in k[X_i]_{1<i\leq n-1}$, $deg_n(R) < deg_n(Q_t)$ et

$$R\,(x_2,x_3,\ldots,x_n)\,g_{t-n} = 0. \tag{56}$$

Preuve On peut supposer que $Q_t = \sum_{i=0}^{m} X_n^i Q_i$ où $Q_j \in k[X_i]_{1<i\leq n-1}$. Puisque l'évaluation de Q_t en les éléments de Jucys-Murphy est g_t, on a

$$\begin{aligned}
\delta_{t\,t'} &= \chi_{t'}\,(Q_t\,(x_2,x_3,\ldots,x_n)) \\
&= \sum_{i=0}^{m} \chi_{t'}^i\,(x_n)\,\chi_{t-n}\,(Q_i\,(x_2,x_3,\ldots,x_{n-1})) \\
&= \chi_{t-n}\,(Q_t\,(x_2,x_3,\ldots,x_{n-1},X_n))\,(\chi_{t'}\,(x_n))
\end{aligned}$$

ce qui prouve que le polynôme $\chi_{t-n}\,(Q_t\,(x_2,x_3,\ldots,x_{n-1},X_n))$ est un polynôme d'interpolation L correspondant aux équations

$$L\,(\chi_{t'}\,(x_n)) \;=\; \delta_{t\,t'} \tag{57}$$

dont le degré en X_n, qui est m, est par conséquent nécessairement supérieur ou égal au nombre de tableaux de Young $t' \neq t$ tel que $t'-n = t-n$ (le polynôme $\chi_{t-n}\,(GZ_t\,(x_2,x_3,\ldots,x_{n-1},X_n))$ étant le polynôme d'interpolation de Lagrange correspondant aux équations 57).

Enfin, l'égalité 55 est obtenue en effectuant la division euclidienne de Q_t par $\displaystyle\prod_{\substack{t'-n=t-n \\ t'\neq t}} \frac{X_n - \chi_{t'}\,(x_n)}{\chi_t\,(x_n) - \chi_{t'}\,(x_n)}$ avec $\deg_n(R) < \deg_n\,(Q_t)$. Le fait que $\deg_n\,(Q_t) = \deg_n\,(GZ_t)$ montre que Q_{t-n} est indépendant de X_n, ce qui entraîne, par comparaison du terme dominant avec le polynôme d'interpolation de Lagrange que

$$\chi_t\,(Q_{t-n}\,(x_2,x_3,\ldots,x_{n-1})) = 1. \tag{58}$$

En effet, si t' est un tableau de Young distinct de t mais tel que $t'-n=t-n$, on a

$$\begin{array}{rcl}\chi_{t'}\left(R\left(x_2,x_3,\ldots,x_{n-1},X_n\right)\right)\left(\chi_{t'}\left(x_n\right)\right) & = & \chi_{t'}\left(R\left(x_2,x_3,\ldots,x_{n-1},x_n\right)\right)\\ & = & \chi_{t'}\left(Q_t\left(x_2,x_3,\ldots,x_{n-1},x_n\right)\right)\\ & = & 0.\end{array}$$

Le polynôme $\chi_{t'}\left(R\left(x_2,x_3,\ldots,x_{n-1},X_n\right)\right)$ est donc divisible par le polynôme $\prod_{\substack{t'-n=t-n\\ t'\neq t}}\left(X_n-\chi_{t'}(x_n)\right)$ et ainsi

$$\chi_{t'}\left(R\left(x_2,x_3,\ldots,x_{n-1},X_n\right)\right)=0 \tag{59}$$

vu la condition sur $\deg_n(R)$. Comme (toujours pour $t-n=t'-n$) on a $\chi_t\equiv\chi_{t'}$ sur $\mathcal{JM}_k^{n-1}$, on en déduit la relation 58 mais cela montre aussi la relation 56 en vertu des propositions **??** et 8.9. $\triangle$

On attire l'attention sur l'efficacité du calcul des idempotents g_t par les GZ-polynômes. Ainsi ce calcul a une meilleure complexité, en considérant les opérations élémentaires mentionnées précédemment, que par les formules de R. DIPPER et G. JAMES. Pour tout tableau de Young t de poids $n>1$,

$$\begin{cases}\deg_i\left(DJ_t\right)\geq\deg_i\left(GZ_t\right) & \text{si } i=2,\\ \deg_i\left(DJ_t\right)>\deg_i\left(GZ_t\right) & \text{si } 2<i\leq n.\end{cases}$$

Si $i=2$,

$$\deg_2\left(DJ_t\right)=\frac{1}{2}\sum_{|\lambda|=n}n_\lambda\geq 1=\deg_2\left(GZ_t\right)$$

avec l'égalité quand $n=2$. Si $2<i\leq n$, on note t_i le tableau de Young de poids i obtenu en retirant de t les cellules numérotées par un nombre supérieur à i. On trouve $\deg_i\left(DJ_t\right)>\deg_i\left(GZ_t\right)$ car

$$\begin{array}{rcl}\deg_i\left(DJ_t\right) & = & \deg_i\left(\prod_{\substack{t'\in\mathrm{Tab}(n)\\ \chi_{t'}(i)\neq\chi_t(i)}}\frac{X_i-\chi_{t'}(x_i)}{\chi_t(x_i)-\chi_{t'}(x_i)}\right)\\ & = & \deg_i\left(\prod_{\substack{t'\in\mathrm{Tab}(i)\\ \chi_{t'}(i)\neq\chi_t(i)}}\frac{X_i-\chi_{t'}(x_i)}{\chi_t(x_i)-\chi_{t'}(x_i)}\right)\end{array}$$

et

$$\deg_i\left(GZ_t\right)=\deg_i\left(\prod_{\substack{t'-i=t_i-i\\ t'\neq t_i}}\frac{X_i-\chi_{t'}(x_i)}{\chi_t(x_i)-\chi_{t'}(x_i)}\right).$$

9 Traces

10 Liminaire

Nous utiliserons plus tard le résultat général suivant :

Proposition 10.1 *Soit $\mathcal{A}$ et $\mathcal{B}$ deux algèbres semi-simples de dimensions finies. On suppose que $\mathcal{A}$ est une sous-algèbre de $\mathcal{B}$ et on dénote par $\mathcal{C}$ le centralisateur de $\mathcal{A}$ dans $\mathcal{B}$.*
Si V est un $\mathcal{A}$-module irréductible et W un $\mathcal{B}$-module irréductible, alors $Hom_{\mathcal{A}}(V,\mathit{Res}_{\mathcal{A}}W)$ est un $\mathcal{C}$-module irréductible.

Cette proposition est valide en caractéristique quelconque, mais nous ne l'appliquerons qu'au cas de deux algèbres semi-simples sur $\mathbb{C}$.

11 Bases et algèbres de Gelfand-Tsetlin

Dans $\mathbb{C}\mathfrak{S}_n$, on définit pour $k = 1,\ldots,n$, le k^{e} élément de Young-Jucys-Murphy (YJM) par :

$$L_k := \sum_{1\le m<k} (m,k),$$

où (m,k) désigne la transposition échangeant m et k.
Exercice. Les éléments de YJM commutent.
On dénote par $\mathcal{Z}_n$ le centre de $\mathbb{C}\mathfrak{S}_n$, et par $\mathcal{Z}_{m,n}$ le commutant de $\mathbb{C}\mathfrak{S}_m$ dans $\mathbb{C}\mathfrak{S}_n$, si $m \le n$.
Exercice. Les sommes de $\mathfrak{S}_m$-classes de conjugaison dans $\mathfrak{S}_n$ forment un système générateur de $\mathcal{Z}_{m,n}$.

Proposition 11.1 $\mathcal{Z}_{m,n} = \langle S'_m,\mathcal{Z}_n,L_{m+1},\ldots,L_n\rangle$.

On est maintenant en mesure de donner la règle de branchement pour la tour d'algèbres

$$\mathbb{C}\mathfrak{S}_0 \subset \mathbb{C}\mathfrak{S}_1 \subset \cdots \subset \mathbb{C}\mathfrak{S}_n \subset \mathbb{C}\mathfrak{S}_{n+1} \subset \cdots$$

Théorème 11.2 *Soit W un $\mathbb{C}\mathfrak{S}_{n+1}$-module irréductible et V un $\mathbb{C}\mathfrak{S}_n$-module irréductible. Alors la multiplicité de V dans la décomposition de $\mathit{Res}_{\mathbb{C}\mathfrak{S}_n}W$ en somme directe de modules est 0 ou 1.*

Démonstration. Soit W un $\mathbb{C}\mathfrak{S}_n$-module irréductible. Il découle de la proposition 11.1 que le centralisateur de $\mathbb{C}\mathfrak{S}_n$ dans $\mathbb{C}\mathfrak{S}_{n+1}$ est commutatif. Tous ses modules irréductibles non triviaux sont donc de dimension 1. La proposition 10.1 entraîne donc que la dimension de $Hom_{\mathbb{C}\mathfrak{S}_m}(W,\mathrm{Res}_{\mathbb{C}\mathfrak{S}_n}V)$ est 0 ou 1. $\triangle$
Il reste maintenant à décrire le graphe de branchement, désigné (temporairement) par $\mathbb{B}$. On va démontrer qu'il s'agit en réalité du graphe de Young $\mathbb{Y}$, c'est-à-dire du diagramme de Hasse du treillis des partitions (ou diagrammes de Young) ordonnées par inclusion.

Soit V un $\mathbb{C}\mathfrak{S}_n$-module irréductible. Soit $\langle\cdot,\cdot\rangle$ le produit intérieur $\mathfrak{S}_n$-invariant sur V (ce produit est unique à un scalaire près). Le théorème 11.2 implique que la décomposition

$$\mathrm{Res}_{\mathbb{C}\mathfrak{S}_{n-1}}V = \bigoplus_{W\to V} W$$

(on somme sur tous les $\mathbb{C}\mathfrak{S}_n$-modules pour lesquels il existe un arc de W vers V dans le graphe de branchement) est canonique. En itérant le processus jusqu'à $\mathfrak{S}_0$, on obtient une décomposition canonique

$$\mathrm{Res}_{\mathbb{C}S_0} V = \bigoplus_T V_T$$

en sous-espaces de dimension 1 V_T, où T décrit l'ensemble des chemins $W_0 \to \cdots \to W_n = V$ dans le graphe de branchement.

Exercice. $\mathbb{C}S_k \cdot V_T = W_k$, pour tout k, $0 \leq k \leq n$.

En choisissant un vecteur v_T dans chaque V_T, on obtient une base $\{v_T\}$ appelée *base de Gelfand-Tsetlin* (en abrégé, base de GZ). Cette base est déterminée de façon unique (à des scalaires près). En outre, si $\varphi : V \to W$ est un isomorphisme de modules irréductibles, alors φ envoie une base de GZ sur une base de GZ.

Exercice. Toute base de GZ est orthogonale pour le produit intérieur $\langle \cdot, \cdot \rangle$.

D'après le théorème de Wedderburn, $\mathbb{C}\mathfrak{S}_n$ se décompose en

$$\mathbb{C}\mathfrak{S}_n = \bigoplus_V \mathrm{End}_{\mathbb{C}}(V) \tag{60}$$

(on somme sur les classes d'équivalence de $\mathbb{C}\mathfrak{S}_n$-modules irréductibles). Cette décomposition est canonique. Si on choisit une base de GZ dans chaque V. Relativement à ces bases, on a naturellement

$$\mathbb{C}\mathfrak{S}_n = \bigoplus_V M_{\mathrm{dim} V}(\mathbb{C}). \tag{61}$$

On définit la (sous-)algèbre de Gelfand-Tsetlin $\mathcal{GZ}(n) \subset \mathbb{C}\mathfrak{S}_n$ constituée de tous les éléments de $\mathbb{C}\mathfrak{S}_n$ qui sont diagonaux pour toute base de GZ dans chaque $\mathbb{C}\mathfrak{S}_n$-module irréductible. Dans les termes de la décomposition 61, $\mathcal{GZ}(n)$ est constituée de toutes les matrices diagonales. On en déduit :

Proposition 11.3 *$\mathcal{GZ}(n)$ est une sous-algèbre commutative maximale de $\mathbb{C}\mathfrak{S}_n$. C'est également une algèbre semi-simple.*

Proposition 11.4 *(i) $\mathcal{GZ}(n) = \langle \mathcal{Z}_0, \mathcal{Z}_1, \ldots, \mathcal{Z}_n \rangle$; (ii) $\mathcal{GZ}(n) = \langle \mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n \rangle$.*

Démonstration. (i) Soit $e_V \in \mathcal{Z}_n$ l'idempotent central associé au $\mathbb{C}\mathfrak{S}_n$-module irréductible V ; il agit comme l'identité sur V, et comme 0 sur tout $\mathbb{C}\mathfrak{S}_n$-module irréductible non isomorphe à V (relativement à la décomposition 60, e_V est l'endomorphisme identité sur la composante V et l'endomorphisme nul sur les autres composantes). Si T est un chemin $W_0 \to W_1 \to \cdots \to W_n = V$ dans $\mathbb{B}$, alors

$$e_{W_0} e_{W_1} \cdots e_{W_n} \in \mathcal{Z}_0 \mathcal{Z}_1 \cdots \mathcal{Z}_n$$

agit sur V comme la projection sur V_T suivant $\bigoplus_{S \neq T}$ et sur tout $\mathbb{C}\mathfrak{S}_n$-module irréductible $V' \not\cong V$, comme 0. La sous-algèbre engendrée par les centres $\mathcal{Z}_0, \mathcal{Z}_1, \ldots, \mathcal{Z}_n$ contient donc $\mathcal{GZ}(n)$. Or $\langle \mathcal{Z}_0, \mathcal{Z}_1, \ldots, \mathcal{Z}_n \rangle$ est commutative et $\mathcal{GZ}(n)$ est une sous-algèbre commutative maximale de $\mathbb{C}\mathfrak{S}_n$, donc les deux sous-algèbres coïncident.

(ii) △

On va maintenant faire jouer à $\mathcal{GZ}(n)$ le rôle d'une sous-algèbre de Cartan. Comme $\mathcal{GZ}(n)$ est semi-simple, on peut décomposer tout $\mathbb{C}\mathfrak{S}_n$-module irréductible V en une somme directe d'espaces (simultanément) propres pour les éléments de YJM $L_1, \ldots, L_n$. Si $\lambda = (\lambda_1, \ldots, \lambda_n) \in$

$\mathbb{C}^n$ et si V_λ désigne l'espace (simultanément) propre pour les $L_1, \dots, L_n$ correspondant aux valeurs prores $\lambda_1, \dots, \lambda_n$, alors on dit que λ est un poids de V et que V_λ est l'epace de poids λ.

Les vecteurs d'une base de GZ sont des poids (par définition). D'autre part, d'après la décomposition 61, $\mathcal{GZ}(n)$ est constituée de toutes les matrices diagonales, donc les espaces de poids sont de dimension 1 ; ce sont donc exactement les droites engendrées par les éléments d'une base de GZ. On remarque aussi que si λ est un poids d'un module irréductible V, ce ne peut être le poids d'aucun module irréductible non isomorphe à V. On obtient ainsi, à travers les bases de Gelfand-Tsetlin, une bijection entre les poids (pour tous les groupes symétriques) et tous les chemins démarrant à la racine dans le graphe de branchement. On désigne par λ_T le poids associé au chemin T et par T_λ un chemin associé au poids λ ; on abrège v_{T_λ} en v_λ.
Un chemin T se termine au sommet V ssi le poids associé λ_T est un poids de V. Il est maintenant évident que pour décrire le graphe de branchement $\mathbb{B}$, il suffit de décrire les ensembles

$$W(n) = \{\lambda \in \mathbb{C}^n \mid \lambda \text{ est un poids d'un } \mathbb{C}\mathfrak{S}_n\text{-module}\} \quad (n \geq 0)$$

et la relation d'équivalence sur

$$\lambda \approx \mu \Leftrightarrow \lambda \text{ et } \mu \text{ sont des poids du même } \mathbb{C}\mathfrak{S}_n\text{-module irréductible}$$

En effet, on remarque que

$$\mathbb{B} = \bigcup_{n \geq 0} (W(n)/\approx)$$

et que, pour toutes toutes $[\lambda]$ et $[\mu]$, respectivement classes d'équivalence de $\lambda \in W(n-1)$ et de $\mu \in W(n)$, on a $[\lambda] \to [\mu]$ dans $\mathbb{B}$ ssi il existe un poids $\nu = (nu_1, \dots, nu_n)$ tel que $\nu \approx \mu$ et $\lambda = (\lambda_1, \dots, \lambda_{n-1})$.
Anticipons un peu sur la suite : les éléments de $W(n)/\approx)$ seront étiquetés par les partitions $\alpha \vdash n$ et ceux de $W(n)$ par les tableaux standard de forme α ; deux tableaux seront équivalents ssi ils ont la même forme. Plus précisément, si T est un tableau standard de forme α, le poids associé λ peut être reconstruit de la façon suivante : λ_i est le *contenu* de la case de α où apparaît i.

12 Description des poids

12.1 Modules de l'algèbre de Hecke affine dégénérée $\mathcal{H}_2$

En notant s_i la transposition élémentaire échangeant i et $i+1$, on a les relations :

$$s_i L i_i = L_{i+1} s_i - 1, \ \ s_i L_j = L_j s_i \ (j \neq i, i+1)$$

De la deuxième relation, on tire
Proposition 12.1 *Soit $\lambda = (\lambda_1, \dots, \lambda_n) \in W(n)$, et $1 \leq k < n$. Alors $s_k v_\lambda$ est une combinaison linéaire de vecteurs v_μ tels que $\mu_i = \lambda_i$ pour $i \neq k, k+1$.*
Le rôle de sl_2 est joué par les $\mathcal{B}_i := \langle L_i, L_{i+1}, s_i \rangle$. Chaque $\mathcal{B}_i$ est un quotient de l'algèbre

$$\langle_2 = \langle s, x, y \mid xy = yx, s^2 = 1, sx = ys - 1 \rangle.$$

Proposition 12.2 (... description des irreps de $\langle_2$ ...) .

Corollaire 12.3 *Soit*

De ce qui précèdeon tire :

Proposition 12.4 *Soit $\lambda \in W(n)$. Alors :*
(i) $\lambda_1 = 0$;
(ii) $\{lambda_i - 1, \lambda_i + 1\} \cap \{\lambda_1, \ldots, \lambda_{i-1}\} \neq \emptyset$ pour tout i, $2 \leq i \leq n$;
(iii) Si $\lambda_i = \lambda_j = a$ pour un certain couple $i < j$, alors

$$\{a_1, a + 1\} \subset \{\lambda_{i+1}, \ldots, \lambda_{j-1}\}.$$

12.2 Le graphe de Young est le graphe de branchement

On rappelle que le graphe de Young $\mathbb{Y}$ est le graphe gradué dont l'ensemble des sommets est l'ensemble $\mathcal{P}$ des partitions (représentées par leur diagramme de Young), et dont les arcs relient tout diagramme de Young à ceux qui sont obtenus en ajoutant une case. La composante de rang n du graphe est donc l'ensemble $\mathcal{P}(n)$ des partitions de poids n (en particulier, la composante de rand 0 est constituée de l'unique diagramme vide $\emptyset$). Les chemins de $\emptyset$ à un sommet α dans $\mathbb{Y}$ sont en bijection avec les tableaux standard de forme α. À tout tableau standard T de forme $alpha$, correspondant au chemin $\emptyset = T_0, T_1, \ldots, T_n = \alpha$, on associe le vecteur de contenu cont(T), aussi noté λ_T, défini par

$$\lambda_T = (\text{cont}(T_1), \ldots, \text{cont}(T_n)) \in \mathbb{Z}^n$$

où cont(T_i) désigne le contenu (*i.e.* le n° de la diagonale) de la case ajoutée à T_{i-1} pour obtenir T_i.

On pose $W'(n) := \{\lambda_T \mid T \text{ est un tableau standard dont la forme } \in \mathcal{P}(n)\}$. Il est facile de retrouver la forme α à partir du vecteur λ_T : le nombre de cases dans la diagonale de n° a du diagramme de Young α est le nombre de composantes de λ_T égales à a. Ainsi deux n-uplets $\lambda, \mu \in W'(n)$ proviennent de tableaux de même forme ssi l'un est image de l'autre par une permutation, ce qu'on note $\lambda \sim \mu$.

Lemme 12.5 *L'ensemble $W'(n)$ est exactement l'ensemble de tous les n-uplets $\lambda \in \mathbb{C}^n$ qui satisfont les propriétés (i)–(iii) de la proposition 12.4. On en déduit $W(n) \subset W'(n)$.*

Soit $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{C}^n$. Une *transposition admissible* pour ν est une transposition élémentaire $s_i \in \mathfrak{S}_n$ correspondant à un couple ν_i, ν_{i+1} tel que $|\nu_i - \nu_{i+1}| \neq 1$. Si $\nu = \lambda_T$, une transposition admissible échange i et $i + 1$ s'ils ne se trouvent pas dans des diagonales adjacentes du tableau T. Naturellement, une transposition admissible tranforme un tableau standard en un tableau standard de même forme.

Soit $\alpha = (\alpha_1 \geq \cdots \geq \alpha_k > 0) \in \mathcal{P}(n)$. Le tableau canonique de forme α, noté $T(\alpha)$, est obtenu en remplissant chaque ligne de gauche à droite, en commençant par la première ligne.

Lemme 12.6 *Soit $\alpha \in \mathcal{P}(n)$. Si T est un tableau standard de forme α, alors il existe une suite de transpositions admissibles qui transforme T en $T(\alpha)$. En outre, on peut choisir les transpositions admissibles $s_{i_1}, \ldots, s_{i_\ell}$ de telle sorte que $\ell = \ell(s_{i_1} \cdots s_{i_\ell})$.*

Lemme 12.7 *Si $\lambda \in W'(n)$ et s'il existe $\mu \in W(n)$ tel que $\lambda \sim \mu$, alors $\lambda \in W(n)$ et $\lambda \approx \mu$.*

On touche enfin au but :

Théorème 12.8 $W(n) = W'(n)$. *En outre,* $\lambda_T \approx \lambda_S \Leftrightarrow$ *les tableaux* T *et* S *on la même forme* $\Leftrightarrow \lambda_T \sim \lambda_S$. *On en conclut que le graphe de branchement* $\mathbb{B}$ *est isomorphe au graphe de Young* $\mathbb{Y}$.

13 Formules de Murnaghan-Nakayama

14 Annexe A: Automates

14.1 Description de la structure d'automate

14.1.1 Graphe pondéré

L'élément de base de ces graphes est la flêche $A = q_1 \stackrel{a|\alpha}{\rightarrow} q_2$ avec $q_i \in Q$, $a \in \S$, $\alpha \in k$ où Q est un ensemble d'états, $\S$ un alphabet et k, un semi-anneau [8]. Pour un tel objet, on définit, selon les conventions générales de la théorie des graphes,

- $t(A) := q_1$ ("tail": queue, source, origine)
- $h(A) := q_2$ ("head" tête, but, extrémité)
- $l(A) := a$ ("label" étiquette)
- $w(A) := \alpha$ ("weight" poids).

Un *chemin* est une suite d'arêtes $c = A_1A_2 \cdots A_n$ (c'est un mot en les arêtes et sa longueur est n) telle que $h(A_k) = t(A_{k+1})$ pour $1 \leq k \leq n-1$ pour un tel chemin $t(c) = t(A_1)$, $h(c) = h(A_n)$, $l(c) = l(A_1)l(A_2)\cdots l(A_n)$ (concaténation), $w(c) = w(A_1)w(A_2)\cdots w(A_n)$ (produit dans le semi-anneau).
Par exemple pour le chemin de longueur 3 suivant ($k = \mathbb{N}$),

$$u = p \stackrel{a|2}{\rightarrow} q \stackrel{b|3}{\rightarrow} r \stackrel{c|5}{\rightarrow} s \tag{62}$$

on a $t(u) = p$, $h(u) = s$, $l(u) = abc$, $h(u) = 30$.

Le poids d'un ensemble de chemins de même source, but et étiquette est la somme des poids des chemins de cet ensemble. Ainsi, si

$$\mathbf{q}1 \quad \begin{array}{c} \stackrel{u|\alpha}{\rightarrow} \\ \stackrel{u|\beta}{\rightarrow} \end{array} \quad \mathbf{q}2 \tag{63}$$

le poids de cet ensemble de chemins est $\alpha + \beta$. On a donc que les poids se multiplient en série et s'aditionnent en parallèle. Les diagrammes suivants montrent la nécessité des axiomes de

8. Nous verrons plus bas que les axiomes de la structure de semi-anneau sont contraints par la définition même du système de transitions ainsi obtenu.

semi-anneau.

Diagramme	Identité	Nom
$p \;\substack{\xrightarrow{a\|\alpha} \\ \xrightarrow{a\|\beta} \\ \xrightarrow{a\|\gamma}}\; q$	$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	Associativité de $+$
$p \;\substack{\xrightarrow{a\|\alpha} \\ \xrightarrow{a\|\beta}}\; q$	$\alpha + \beta = \beta + \alpha$	Commutativité de $+$
$p \;\substack{\xrightarrow{a\|\alpha} \\ \xrightarrow{a\|0}}\; q$ $p \;{}^{a\|0}\; q \xrightarrow{b\|\beta} r$	$\alpha + 0 = \alpha$ $0 + \beta = \alpha$	Élément neutre (droite) de $+$ Élément neutre (gauche) de $+$
$p \xrightarrow{a\|\alpha} q \xrightarrow{b\|\beta} r \xrightarrow{c\|\gamma} s$	$\alpha(\beta\gamma) = (\alpha\beta)\gamma$	Associativité de $\times$
$p \;\substack{\xrightarrow{a\|\alpha} \\ \xrightarrow{a\|\beta}}\; q \xrightarrow{b\|\gamma} r$	$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$	Distributivité (droite) de $\times$ sur $+$
$p \xrightarrow{a\|\alpha} q \;\substack{\xrightarrow{b\|\beta} \\ \xrightarrow{b\|\gamma}}\; r$	$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$	Distributivité (gauche) de $\times$ sur $+$
$p \xrightarrow{a\|\alpha} q \xrightarrow{b\|1_k} r$ $p \xrightarrow{a\|1_k} q \xrightarrow{b\|\beta} r$	$\alpha \times 1_k = \alpha$ $1_k \times \beta = \beta$	Élément neutre (droite) de $\times$ Élément neutre (gauche) de $\times$

14.1.2 Structure et comportement des automates

Un automate à poids ou pondéré ("automaton with weights") est la donnée de trois éléments vectoriels (I,M,T):

$$\begin{cases} \bullet \quad \text{Un vecteur d'entrée } I \in k^{1\times Q} \\ \bullet \quad \text{Une famille (indexée à A) de matrices de transition } M : A \to k^{Q\times Q} \\ \bullet \quad \text{Un vecteur de sortie } T \in k^{Q\times 1} \end{cases}$$

La donnée des transitions (M) est équivalente à celle d'un graphe pondéré dont les sommets sont Q, l'alphabet A et les poids sont pris dans k. De plus celle de I (resp. T) correspond à la donnée de flêches rentrantes (resp. sortantes) marquées avec des poids. Dans tout ce processus, on peut ne pas indiquer les flêches de poids nul.
Ce type d'automates généralise les automates (booléens) de la théorie des langages (que l'on obtient alors pour $k = \mathbb{B}$) est une machine qui prend un mot en entrée et retourne un coefficient (dans k) en sortie. Son comportement est donc une fonction $\mathcal{A} : \ A^* \to k$ (que l'on peut noter, de manière équivalente, comme une série $\mathcal{A} = \sum_{w\in A^*} \mathcal{A}(w)w$).
Calcul du poids $\mathcal{A}(w)$. —
On étend d'abord la fonction de transition M à A^* par

$$M(\epsilon) = I_{Q\times Q},\, M(w) = M(a_1a_2\cdots a_n) = M(a_1)M(a_2\cdots M(a_n) \tag{64}$$

où $I_{Q\times Q}$ est la matrice identité de format $Q \times Q$. Le calcul du poids d'un mot est alors, par définition,

$$\mathcal{A}(w) := IM(w)T \tag{65}$$

d'après la règle de multiplication des matrices, on a bien que $IM(w)T$ est une matrice de format 1×1 et donc un élément de k. Le lien avec le graphe de l'automate est donné par la proposition

suivante :
Proposition 14.1 *Soit, pour deux états r,s et un mot $w \in A^*$*

$$\mathcal{A}^{r,s}(w) := I_r \left(\sum_{\frac{c,\ \text{chemin}\ l(c)=w}{t(c)=r,\ h(c)=s}} weight(c) \right) T_s \tag{66}$$

alors

$$\mathcal{A}(w) = \sum_{r,s \in Q} \mathcal{A}^{r,s}(w) \tag{67}$$

Cette proposition a le sens intuitif suivant :

1. l'équation (66) donne le poids calculé comme au paragraphe précédent
   - on fait le bilan parallèle (c'est à dire une somme) des poids des chemins qui joignent r à s
2. on multiplie (à gauche si c'est non commutatif) par le poids d'entrée en r
3. on multiplie (à droite si c'est non commutatif) par le poids de sortie en s

14.1.3 Exemples de fonctions produites par des automates

1. Longueur totale $\sum_{w \in A^*} |w|w$
2. Comptage des a, $\sum_{w \in A^*} |w|_a w$ et des b, $\sum_{w \in A^*} |w|_b w$
3. Produit des degrés partiels $\sum_{w \in A^*} |w|_a |w|_b w$
4. Autres produits $\sum_{w \in A^*} F_{|w|} |w| w$, $\sum_{w \in A^*} F_{|w|_a} |w|_b w$

14.2 Which rational calculus ?

If Q is a finite set, the space $k^{Q \times Q}$ of square matrices with indices in Q and coefficients in k has a natural semiring structure with the usual operations (sum and product). A (right) star of $M \in k^{Q \times Q}$ (when it exists) is a solution of the equation $MY + 1_{Q \times Q} = Y$ (where $1_{Q \times Q}$ is the identity matrix). Let $M \in k^{Q \times Q}$ be given by

$$M = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

where $a_{11} \in k^{Q_1 \times Q_1}$, $a_{12} \in k^{Q_1 \times Q_2}$, $a_{21} \in k^{Q_2 \times Q_1}$ and $a_{22} \in k^{Q_2 \times Q_2}$ such that $Q_1 + Q_2 = Q$. Let $N \in k^{Q \times Q}$ given by

$$N = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

with

$$A_{11} = (a_{11} + a_{12} {a_{22}}^* a_{21})^* \tag{68}$$
$$A_{12} = {a_{11}}^* a_{12} A_{22} \tag{69}$$
$$A_{21} = {a_{22}}^* a_{21} A_{11} \tag{70}$$
$$A_{22} = (a_{22} + a_{21} {a_{11}}^* a_{12})^* \tag{71}$$

Théorème 14.2 *If the right hand sides of formulas (68), (69), (70) and (71) are defined, the matrix M admits N as a right star.*

Proof. Suppose, without loss of generality, that $Q = [1,n]_{\mathbb{N}};\ n = p + q;\ Q_1 = [1,p]_{\mathbb{N}};\ Q_2 = [p+1,p+q]_{\mathbb{N}}$. We have to show that N is a solution of the equation $My + 1_{n\times n} = y$. By computation, one has

$$MN + 1 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} + \begin{pmatrix} 1_{p\times p} & 0_{p\times q} \\ 0_{q\times p} & 1_{q\times q} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}A_{11} + a_{12}A_{21} + 1_{p\times p} & a_{11}A_{12} + a_{12}A_{22} \\ a_{21}A_{11} + a_{22}A_{21} & a_{21}A_{12} + a_{22}A_{22} + 1_{q\times q} \end{pmatrix}$$

where $0_{p\times q}$ is the zero matrix in $k^{p\times q}$. We verify the relations (68), (69), (70) and (71) by:

$$\begin{aligned} a_{11}A_{11} + a_{12}A_{21} + 1_{p\times p} &= a_{11}A_{11} + a_{12}a_{22}^*a_{21}A_{11} + 1_{p\times p} = \\ A_{11}(a_{11} + a_{12}{a_{22}}^*a_{21}) + 1_{p\times p} &= A_{11} \end{aligned}$$

$$\begin{aligned} a_{11}A_{12} + a_{12}A_{22} &= a_{11}{a_{11}}^*a_{12}A_{22} + a_{12}A_{22} = \\ (a_{11}{a_{11}}^* + 1)a_{12}A_{22} &= {a_{11}}^*a_{12}A_{22} = A_{12} \end{aligned}$$

$$\begin{aligned} a_{21}A_{11} + a_{22}A_{21} &= a_{21}A_{11} + a_{22}{a_{22}}^*a_{21}A_{11} = \\ (1 + a_{22}{a_{22}}^*)a_{21}A_{11} &= {a_{22}}^*a_{21}A_{11} = A_{21} \end{aligned}$$

$$\begin{aligned} a_{21}A_{12} + a_{22}A_{22} + 1_{q\times q} &= a_{21}{a_{11}}^*a_{12}A_{22} + a_{22}A_{22} + 1_{q\times q} = \\ (a_{22}a_{21}{a_{11}}^*a12)A_{22} + 1_{q\times q} &= A_{22} \end{aligned}$$

□

Remarque 14.3 *i) In [11] and [14], similar formulas are expressed for the computation of the inverse of matrices when k is a division ring (this can be extended to the case of rings).*
It must be emphasized that the converse of Theorem (14.2), of course, does not hold as shows the example below (the coefficients are taken in a ring and here the star is unique).

$$M = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \quad M^* = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \tag{72}$$

However, if the formulas are defined at each step of the computation (see below for a formalization of this), it provides a recursive way to compute a star of a matrix.
ii) Similar formulas can be stated in the case of a left star. The matrix N is the left star of M with

$$\begin{aligned} A_{11} &= (a_{11} + a_{12}{a_{22}}^*a_{21})^* \\ A_{12} &= A_{11}a_{12}{a_{22}}^* \\ A_{21} &= A_{22}a_{21}{a_{11}}^* \\ A_{22} &= (a_{22} + a_{21}{a_{11}}^*a_{12})^* \end{aligned} \tag{73}$$

iii) When all their terms are defined, formulas above (as well as (68), (69), (70) and (71)) are valid with matrices of any size with any block partitionning. Matrices of even size are often, in practice, partitionned into square blocks but, for matrices with odd dimensions, the approach called dynamic peeling is applied. More specifically, let $M \in k^{n\times n}$ a matrix given by

$$M = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

where $n \in 2\mathbb{N}+1$. The dynamic peeling [26] consists of cutting out the matrix in the following way: a_{11} is a $(n-1)\times(n-1)$ matrix, a_{12} is a $(n-1)\times 1$ matrix, a_{21} is a $1\times(n-1)$ matrix and a_{22} is a scalar.

Références

Références générales.

[1] E. ABE Hopf algebras. Cambridge (1980).

[2] BERSTEL J. AND REUTENAUER C., *Rational series and their languages*, EATCS, 1988.

[3] BOURBAKI N., Algèbre Ch. III. Hermann (1970)

[4] COHEN H., *A Course in Computational Algebraic Number Theory*. Springer (1993)

[5] CAYLEY A., On certain results related to quaternions. Phil. Mag. **26**, 141-145 (1845).

[6] CURTIS C. W., REINER I., *Methods of representation theory.* Wiley Interscience, (1990).

[7] DAVENPORT J., SIRET Y., TOURNIER E., *Calcul formel*, Masson (1986)

[8] DEMAZURE MICHEL, Cours d'algèbre : Divisibilité, Primalité, codes. Cassini (1997).

[9] EILENBERG S., Automata, languages and machines, Acad. Press (1974).

[10] VON ZUR GATHEN J. AND GERAHRD J. Modern Computer Algebra. Cambridge (1999).

[11] HEYTING A., "Die Theorie der Linearen Gleichungen in einer Zahlenspezies mit nicht-kommutativer Multiplikation". *Math. Ann.* **98** (1927) 465-490.

[12] W. FULTON et J. HARRIS, *Representation theory: a first course*, Springer-Verlag, New-York, 1991.

[13] NAUDIN P., QUITTÉ C., *Algorithmique Algébrique* Masson (1992)

[14] RICHARDSON A. R., *Simultaneous Linear equations over a division ring*. *Proc. Lond. Math. Soc.* **28** (1928) 395-420.

[15] KNUTH D., *The art of computer programming*, Tome I & II. Addison-Wesley (1981)

[16] STANLEY R., *Enumerative Combinatorics Vol I and II*, Cambridge.

Références spécialisées.

Automates./Informatique.

[17] CHAMPARNAUD J.-M., DUCHAMP G. :*Derivatives of rational expressions and related theorems*, T.C.S. **313** 31 (2004).

[18] DUCHAMP G., REUTENAUER C., *Un critère de rationalité provenant de la géométrie noncommutative* Invent. Math. **128** 613-622. (1997).

[19] DUCHAMP G., HADJ KACEM H. AND LAUGEROTTE E., *Algebraic elimination of ϵ-transitions*, DMTCS, Volume 7 n° 1 (2005), pp. 51-70

[20] EILENBERG S., Automata, languages and machines, Acad. Press (1974).

[21] LAUGEROTTE É., *Combinatoire et Calcul symbolique en Théorie des Représentations*, Thèse de l'Université de Rouen (6 novembre 1997).

[22] FLOURET M., *Contribution à l'Algorithmique Noncommutative*, Thèse de l'Université de Rouen (19 janvier 1999).

[23] FLOURET M., LAUGEROTTE É., *Noncommutative minimization algorithms.* Information Processing Letters **64**, 123-126 (1997).

[24] HATEM HADJ-KACEM, *Contribution à la théorie et aux applications des automates à multiplicités*, Thèse de l'Université de Rouen (17/06/2005).

[25] LUQUE JEAN-GABRIEL, *Monoïdes et automates admettant un produit de mélange*, Thèse de l'Université de Rouen (09/12/1999).

[26] HUSS-LEDERMAN S., JACOBSON E.M., JOHNSON J.R., TSAO A., TURNBULL T., "Implementation of Strassen's Algorithm for Matrix Multiplication". *Proceeding of the ACM/IEEE conference on supercomputing* , Pittsburgh, Pennsylvania, USA (1996).

[27] IVERSON KENNETH E., A programming Language. Wiley, 1962.

[28] SCHÜTZENBERGER, "On the definition of a family of automata". *Inform. and Contr.* **4** (1961) 245-270.

Cryptographie/Cryptologie.

[29] BRYANT R. E., *Graph-based algorithms for boolean function manipulation*. IEEE Transactions on Computers **35**, (1986).

[30] DUCHAMP G. H. E., HADJ-KACEM H., LAUGEROTTE E., *On the decomposition of boolean functions*, BFCA05, March 7-8, 2005.

Combinatoire Algébrique

[31] FOMIN S. *Duality of graded graphs*, J. Alg. Comb. 3 (1994) 357-404 "Schensted algorithms for dual graded graphs", J. Alg. Comb. 4 (1995), 5-45.

[32] DUCHAMP G., KROB D., LASCOUX A., LECLERC B., SCHARF T., THIBON J.-Y., *Euler-Poincaré characteristic and polynomial representations of Iwahori-Hecke algebras*. Pub. of the RIMS **31**, (1995).

[33] HUMPHREYS J. E., *Reflection groups and Coxeter groups*. Cambridge University Press, (1990).

[34] JOYAL A., *Une théorie combinatoire des séries formelles*, Adv. Math.42 (1981), 1-82.

[35] JUCYS A. A., *Symmetric polynomials and the center of the symmetric group ring*, Reports on Mathematical physics, **5**, 107-112, 1974.

[36] MURPHY G. E., *A new construction of Young's seminormal representation of the symmetric groups*, Journal of Algebra, **69**, 287- 297, 1981.

[37] MURPHY G. E., *The idempotents of the symmetric group and Nakayma's conjecture*, Journal of Algebra, **81**, 258-265, 1983.

[38] OKOUNKOV A. et A. M. VERSHIK, *Inductive construction of representation theory for symmetric groups*, Russian Math. Survey, **51**, Vol 2, 1996.

[39] I. G. MACDONALD, *Symmetric functions and Hall polynomials*, Clarendon Press, Oxford, 1979.

[40] LASCOUX A. et SCHÜTZENBERGER M. -P., *Le monoïde plaxique*, Quaderni della Ricerca Scientifica del CNR, Rome, 1981.

[41] TOUCHARD J., *Sur les cycles des permutations*, Acta Math. **70** (1939), 243-297.

Combinatoire et Physique.

[42] G. H. E. DUCHAMP, P. BLASIAK, A. HORZELA, K. A. PENSON, A. I. SOLOMON, *Feynman graphs and related Hopf algebras*, Journal of Physics, Volume 30, 2006: Conference Series, SSPCM'05, Myczkowce, Poland.
arXiv: cs.SC/0510041

[43] G. Duchamp, K.A. Penson, A.I. Solomon, A. Horzela and P. Blasiak, *One-Parameter Groups and Combinatorial Physics*,Proceedings of the Third International Workshop on Contemporary Problems in Mathematical Physics (COPROMAPH3), Porto-Novo (Benin), November 2003, J. Govaerts, M. N. Hounkonnou and A. Z. Msezane Eds., p. 436, World Scientific Publishing, Singapore (2004)
arXiv : quant-ph/0401126

[44] Ridell R.J., Uhlenbeck G.E., *On the theory of the virial development of the equation of state of monomatomic gases*, J. Chem. Phys. **21** (1953), 2056-2064.