Combinatoire algébrique expérimentale

Jean Fromentin

Université du Littoral Côte d'Opale

Combinatoire algébrique expérimentale

Mémoire d'Habilitation à Diriger des Recherches
Spécialité : Mathématiques

Jean FROMENTIN

soutenu publiquement le ***4 décembre 2019***

Membres du Jury

M. Shalom Eliahou, professeur, Université du Littoral Côte d'Opale
M. Loïc Foissy, professeur, Université du Littoral Côte d'Opale
M. Eddy Godelle, professeur, Université de Caen
M. Florent Hivert, professeur, Université Paris-Sud
M. Jean-Christophe Novelli, professeur, Université Paris-Est
M. Luis Paris, professeur, Université de Bourgogne
M. Matthieu Picantin, maître de conférences (H.d.R), Université Paris Diderot
M. Jorge Ramírez Alfonsín, professeur, Université de Montpellier

Rapporteurs

M. Eddy Godelle, professeur, Université de Caen
M. Matthieu Picantin, maître de conférences (H.d.R), Université Paris Diderot
M. Jorge Ramírez Alfonsín, professeur, Université de Montpellier

Table des matières

Introduction

Dans ce mémoire d'habilitation je présente les travaux de recherche que j'ai menés depuis que j'ai été recruté comme maître de conférences à l'Université du Littoral Côte d'Opale. Mes domaines de recherche sont la théorie des tresses et des nœuds ainsi que la combinatoire additive avec un soupçon de théorie de Ramsey. Le tout peut être englobé dans ce que nous appelons la combinatoire algébrique. Le point commun à toutes mes activités de recherche est sans aucun doute la conception d'algorithmes, soit pour établir un résultat mathématique, comme lors de la détermination de la non-existence de coloriage morphique à 2 ou 3 couleurs des entiers naturels évitant les triplets pythagoriciens monochromatiques, soit pour observer certaines propriétés et ensuite les démontrer. Cette dernière façon d'utiliser les algorithmes pour la recherche mathématique est souvent invisible. En effet dès que la propriété observée est démontrée alors l'algorithme ayant permis son observation n'a plus vraiment de raison d'être utilisé, ni même d'être décrit. Tous les travaux présentés dans ce mémoire ont, à un moment donné, nécessité la conception d'algorithmes que ce soit de façon explicite ou implicite.

Il est assez courant dans un mémoire d'habilitation de présenter les activités de recherche sans trop entrer dans les détails. Ce n'est pas le choix que j'ai fait ici. Presque toutes les démonstrations des résultats présentés sont données dans ce mémoire. J'ai fait ce choix afin de simplifier le travail du lecteur non expert désirant obtenir des détails sur comment démontrer tel ou tel résultat. Les recherches présentées provenant de différents domaines, il se peut que le lecteur ne soit pas familiarisé avec certains d'entre eux.

Contextes et résultats obtenus depuis la thèse

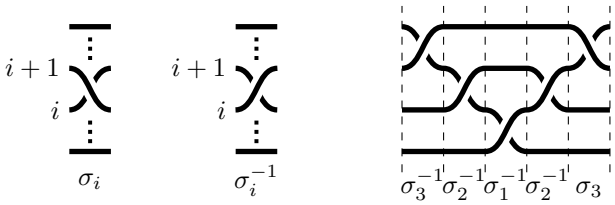
Poursuite des travaux commencés durant la thèse

Présentation des tresses

Originellement, le groupe B_n des tresses à n brins est défini comme le groupe des classes d'isotopie des tresses géométriques à n brins. La présentation algébrique suivante a été établie par E. Artin dans [3] :

$$B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\,\sigma_j = \sigma_j\,\sigma_i & \text{pour } |i-j| \geqslant 2 \\ \sigma_i\,\sigma_j\,\sigma_i = \sigma_j\,\sigma_i\,\sigma_j & \text{pour } |i-j| = 1 \end{array} \right\rangle$$

Ainsi une tresse à n brins est une classe d'équivalence (infinie) de mots de tresse en les lettres $\sigma_i^{\pm 1}$. Sur les dessins ci-dessous, on peut voir l'interprétation des lettres σ_i et σ_i^{-1} comme tresses géométriques ainsi que le codage d'une tresse géométrique à l'aide d'un mot de tresse.



Un des principaux outils en théorie algorithmique des tresses est l'utilisation de formes normales permettant, pour chaque tresse, d'isoler un mot particulier parmi tous ceux de la classe d'équivalence associée. L'une des plus connues est la forme normale de Garside introduite en 1969 par F. A. Garside [73].

Mot σ-définis

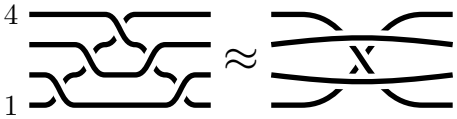
En 1992, P. Dehornoy [26] définit un ordre total $<$ sur le groupe des tresses B_n, compatible avec la multiplication à gauche. La construction de cet ordre repose essentiellement sur l'existence, pour toute tresse β de B_n, d'un mot de tresse dit σ-défini représentant la tresse β. Un mot de tresse w est dit *σ-défini* s'il est vide ou si la lettre σ_i, avec i maximal, n'apparaît que positivement ou que négativement. Par exemple le mot $\sigma_2\,\sigma_1\,\sigma_2^{-1}$ n'est pas σ-défini car l'indice maximal est 2 et ce mot contient à la fois σ_2 et σ_2^{-1}. Par contre le mot $\sigma_1^{-1}\sigma_2\sigma_1$, qui lui est équivalent, est σ-défini.

Monoïde des tresses duales

J.S. Birman, K.H. Ko et S.J. Lee ont introduit [8] et étudié en 1998 un nouveau sous-monoïde B_n^{+*} de B_n, appelé *monoïde de Birman–Ko–Lee* ou encore *monoïde des tresses duales*. Le monoïde B_n^{+*} est le sous-monoïde de B_n engendré par les tresses

$$a_{i,j} = \sigma_i \,\ldots\, \sigma_{j-2}\,\sigma_{j-1}\,\sigma_{j-2}^{-1} \,\ldots\, \sigma_i^{-1} \quad \text{avec } 1 \leqslant i < j \leqslant n.$$

Voici par exemple l'interprétation de la tresse $a_{1,4}$ comme tresse géométrique.



Forme normale tournante

Durant ma thèse j'ai construit une nouvelle forme normale [65], dite *tournante*, sur le monoïde B_n^{+*}. Cette forme normale est construite à l'aide de la structure de Garside du monoïde B_n^{+*} et l'injection naturelle de B_n^{+*} dans B_{n+1}^{+*}. Elle est particulièrement intéressante car elle a une interaction forte avec l'ordre des tresses. En particulier, j'ai pu montrer [66] que la restriction de $<$ à B_n^{+*} est un bon ordre de type $\omega^{\omega^{n-2}}$, améliorant un résultat de R. Laver [90] qui établit que la restriction $(B_n^{+*}, <)$ est un bon ordre, sans en préciser le type. À l'aide d'une analyse fine de l'interaction entre la forme normale tournante et l'ordre des tresses, j'ai pu prouver [67] que toute tresse β de B_n admet un représentant σ-défini de longueur au plus $3(n-1)||\beta||_\sigma$, où $||\beta||_\sigma$ est la longueur géodésique de β en les lettres $\sigma_i^{\pm 1}$. L'existence d'un tel représentant σ-défini quasi-géodésique était conjecturée depuis 1997.

Rationalité de la forme normale tournante [68]

Un mot en les lettres $a_{i,j}$ est dit n-tournant s'il est la forme normale tournante d'une certaine tresse de B_n^{+*}. Dans [68] je me suis intéressé à l'ensemble R_n des mots n-tournants. Grâce à une analyse fine des propriétés syntaxiques des mots tournants, j'ai pu construire explicitement un automate fini déterministe $\mathcal{A}_n$ permettant de reconnaître l'ensemble miroir R_n^* de R_n. Nous obtenons en particulier que les langages R_n^* puis R_n sont rationnels. Ces travaux sont en partie présents dans ma thèse mais les résultats obtenus dans [68] sont plus généraux que ceux que j'avais obtenus alors. Dans ce même article je montre que le langage R_n n'est pas automatique à gauche et je construis un autre langage rationnel S_n^σ, composé de mots σ-définis, en bijection avec les tresses de B_n.

Combinatoire des monoïdes d'Artin–Tits

Groupes de Coxeter

Soit $\mathscr{S}$ un ensemble. Une *matrice de Coxeter* $M_{\mathbf{\Gamma}}$ sur $\mathscr{S}$ est une matrice symétrique $M = (m_{s,t})_{(s,t)\in\mathscr{S}^2}$ à coefficients dans $\mathbb{N}\cup\{\infty\}$ telle que $m_{s,t} = 1$ si et seulement si $s = t$. Le *groupe de Coxeter* $W_{\mathbf{\Gamma}}$ associé à la matrice de Coxeter $M_{\mathbf{\Gamma}}$ est

$$W_{\mathbf{\Gamma}} = \left\langle \mathscr{S} \;\middle|\; \begin{array}{ll} s^2 = 1 & \text{pour } s \in \mathscr{S} \\ \underbrace{sts\cdots}_{m_{s,t}} = \underbrace{tst\cdots}_{m_{t,s}} & \text{pour } s,t \in \mathscr{S} \text{ et } m_{s,t} \neq \infty \end{array} \right\rangle.$$

Un groupe de Coxeter est dit *irréductible* s'il ne peut pas être exprimé comme le produit direct de groupes de Coxeter. Il y a 4 familles infinies de groupes de Coxeter irréductibles finis :

$$W_{\mathbf{A_n}}(n \geqslant 1) \quad W_{\mathbf{B_n}}(n \geqslant 2) \quad W_{\mathbf{D_n}}(n \geqslant 4) \quad \text{et} \quad W_{\mathbf{I_p}}(p \geqslant 5)$$

ainsi que 6 groupes exceptionnels $W_{\mathbf{E_6}}$, $W_{\mathbf{E_7}}$, $W_{\mathbf{E_8}}$, $W_{\mathbf{F_4}}$, $W_{\mathbf{H_3}}$ et $W_{\mathbf{H_4}}$. Dans la suite de cette section tous les groupes de Coxeter seront supposés finis.

Monoïdes d'Artin–Tits

Pour tout groupe de Coxeter $W_{\mathbf{\Gamma}}$, on définit le *monoïde d'Artin–Tits* $B_{\mathbf{\Gamma}}^+$ ou *monoïde des tresses généralisées* par

$$B_{\mathbf{\Gamma}}^+ = \left\langle S \;\middle|\; \underbrace{sts\cdots}_{m_{s,t}} = \underbrace{tst\cdots}_{m_{t,s}} \text{ pour } s,t \in \mathscr{S} \text{ et } m_{s,t} \neq +\infty \right\rangle^+.$$

Le monoïde $B_{\mathbf{\Gamma}}^+$ est muni d'une structure de Garside associant à chaque tresse β de $B_{\mathbf{\Gamma}}^+$ une suite finie $\mathrm{Gar}(\beta) = (w_1, \ldots, w_\ell)$ d'éléments de $W_{\mathbf{\Gamma}}$. Une suite appartenant à l'image de Gar est dite *normale*. Les suites normales sont ainsi en bijection avec les éléments de $B_{\mathbf{\Gamma}}^+$. On montre qu'une suite $(w_1, \ldots, w_\ell)$ d'éléments de $W_{\mathbf{\Gamma}}$ vérifiant $w_\ell \neq 1$ est normale si et seulement si les paires (w_i, w_{i+1}) sont en *position normale* pour $i = 1, \ldots, \ell - 1$.

Un peu de combinatoire

Pour un groupe de Coxeter $W_{\mathbf{\Gamma}}$, nous notons $b_{\mathbf{\Gamma},d}$ le nombre de suites normales de longueur d. Le comportement de la suite $d \mapsto b_{\mathbf{\Gamma},d}$ peut être étudié à l'aide de la matrice

d'adjacence $\mathrm{Adj}_{\mathbf{\Gamma}} = (a_{u,v})$ indexée par les éléments de $W_{\mathbf{\Gamma}}$ et définie par

$$a_{u,v} = \begin{cases} 1 & \text{si } (u,v) \text{ est en position normale,} \\ 0 & \text{sinon.} \end{cases}$$

En effet, pour $d \geqslant 1$, nous avons

$$b_{\mathbf{\Gamma},d} = {}^t X \, \mathrm{Adj}_{\mathbf{\Gamma}}^{d-1} \, X \quad \text{où} \quad X_u = \begin{cases} 0 & \text{si } u = 1_{W_{\mathbf{\Gamma}}}, \\ 1 & \text{sinon.} \end{cases}$$

Les valeurs propres de $\mathrm{Adj}_{\mathbf{\Gamma}}$ donnent alors une indication sur la croissance de $b_{\mathbf{\Gamma},d}$. Notons $\chi_{\mathbf{\Gamma}}$ le polynôme caractéristique de $\mathrm{Adj}_{\mathbf{\Gamma}}$. En 2007, P. Dehornoy conjecture [30] que, pour $n \geqslant 1$, le polynôme $\chi_{\mathbf{A_n}}$ est un diviseur de $\chi_{\mathbf{A_{n+1}}}$. Ce résultat a été démontré en 2008 par F. Hivert, J.C. Novelli et J.Y. Thibon [81] en utilisant l'algèbre de Hopf **FQSym** introduite en 1995 par C. Malvenuto et C. Reutenauer dans [93].

Un résultat de divisibilité [62]

Avec L. Foissy nous avons montré [62] que, pour $n \geqslant 2$, le polynôme $\chi_{\mathbf{B_n}}$ est un diviseur de $\chi_{\mathbf{B_{n+1}}}$. Pour cela nous avons considéré l'algèbre de Hopf graduée **BFQSym**, une version décorée de l'algèbre **FQSym**. Suivant les idées de [81] nous obtenons le résultat de divisibilité, en interprétant la matrice $\mathrm{Adj}_{\mathbf{B_n}}$ comme la matrice d'un endomorphisme $\Phi_{\mathbf{B_n}}$ de **BFQSym** et en construisant une dérivation surjective ∂ de **BFQSym** qui vérifie

$$\partial \circ \Phi_{\mathbf{B_n}} = \Phi_{\mathbf{B_{n-1}}} \circ \partial.$$

Nous montrons aussi que le polynôme $\chi_{\mathbf{D_4}}$ n'est pas un diviseur de $\chi_{\mathbf{D_5}}$ et nous calculons les polynômes $\chi_{\mathbf{\Gamma}}$ pour $\Gamma = \mathbf{I_p}$ avec $p \geqslant 5$ et les types exceptionnels sauf $\mathbf{E_8}$.

Théorie des nœuds

Polynôme de Jones

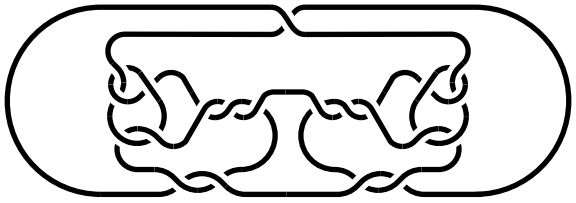
Introduit par V. Jones en 1984 [84], le polynôme de Jones est un invariant polynomial à coefficients entiers des nœuds et des entrelacs. Une question majeure en théorie des nœuds est de déterminer si le polynôme de Jones est capable de détecter les entrelacs triviaux. Plus précisément, on cherche à déterminer s'il existe un entrelacs L non trivial à k composantes tel que le polynôme de Jones de L soit le même que celui de l'entrelacs trivial à k composantes U_k.

Cas des entrelacs avec au moins 2 composantes

En 2001, M. B. Thistlethwaite exhibe [126] deux entrelacs non triviaux à deux composantes et un à trois composantes, qui admettent le même polynôme de Jones que U_2 et U_3 (respectivement). Ce sont les premiers exemples d'entrelacs non triviaux indétectables par le polynôme de Jones. En 2003, S. Eliahou, L. Kauffman et M. B. Thistlethwaite construisent [55], pour tout $k \geqslant 2$, une famille infinie d'entrelacs non triviaux à k composantes, admettant le même polynôme de Jones que l'entrelacs U_k. Cependant la question reste ouverte pour les nœuds, c.-à-d., les entrelacs à une seule composante.

Polynôme de Jones modulaire [50]

Avec S. Eliahou nous nous sommes intéressés au problème, plus faible, de trouver des nœuds non triviaux indétectables par le polynôme de Jones modulo un entier m. Dans [50], nous identifions un enchevêtrement remarquable à 20 croisements, permettant de construire explicitement une famille infinie de nœuds premiers, deux à deux distincts, à polynôme de Jones trivial modulo 2^r, pour n'importe quelle valeur r supérieure ou égale à 1 fixée. Voici par exemple le plus petit nœud possédant un polynôme de Jones trivial modulo 2 ainsi obtenu.



Semigroupes numériques

Un semigroupe numérique est un sous-ensemble S de $\mathbb{N}$ contenant 0, stable par addition et de complément fini. De manière équivalente c'est un sous-ensemble S de $\mathbb{N}$ de la forme $S = \langle a_1, \ldots, a_n \rangle = \mathbb{N}a_1 + \ldots + \mathbb{N}a_n$ pour des entiers strictement positifs $a_1, \ldots, a_n$ premiers entre eux. Le *gouffre* de S est l'ensemble $\mathbb{N} \setminus S$, son *genre* est $g(S) = \text{card}\,(\mathbb{N} \setminus S)$, sa *multiplicité* est $m(S) = \min(S \setminus \{0\})$, son *nombre de Frobenius* est $F(S) = \max(\mathbb{Z} \setminus S)$, son *conducteur* est $c(S) = F(S) + 1$. L'ensemble des *éléments primitifs* de S est le plus petit ensemble $P(S)$ de S tel que $S = \langle P(S) \rangle$.

Conjecture de Wilf

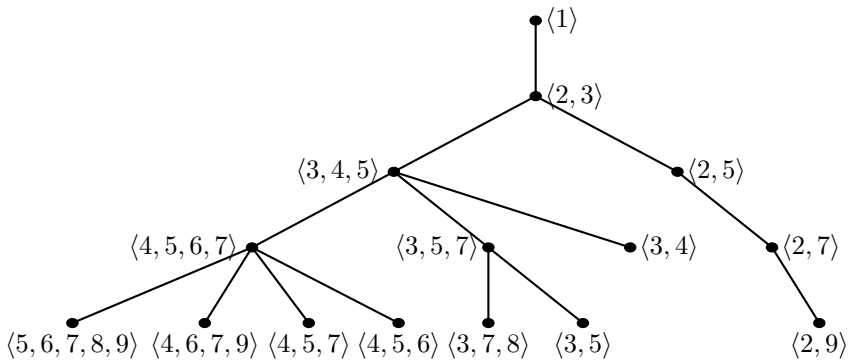
Soit S un semigroupe numérique. Notons $L(S) = S \cap [0, c(S) - 1]$ l'ensemble des éléments de S plus petits que son conducteur $c(S)$. On pose

$$W(S) = \text{card}\,(P(S)) \times \text{card}\,(L(S)) - c(S).$$

En 1978, H. Wilf conjecture [133] que quel que soit le semigroupe numérique S, la relation $W(S) \geqslant 0$ est toujours vérifiée. Bien qu'établie dans de nombreux cas particuliers, la conjecture de Wilf est à ce jour toujours ouverte.

Arbre des semigroupes numériques

En 2003, J.C. Rosales et P.A. García-Sánchez montrent [115] que tout semigroupe numérique S' peut être obtenu d'un semigroupe numérique S en posant $S' = S^x = S \setminus \{x\}$, où x est un élément primitif de S supérieur à son conducteur $c(S)$. Le genre de S' est alors $1 + g(S)$. On dit que le semigroupe S' est un *fils* du semigroupe S. Nous construisons ainsi l'arbre de tous les semigroupes numériques. La racine de l'arbre est l'unique semigroupe numérique de genre 0, à savoir $\mathbb{N}$. Le dessin suivant montre les 5 premiers niveaux de l'arbre ainsi obtenu.



Les semigroupes numériques de genre g sont exactement ceux qui sont à distance g de la racine de l'arbre.

Conjectures de M. Bras-Amorós

Pour $g \in \mathbb{N}$, on note n_g le nombre de semigroupes numériques de genre g. Les premières valeurs de n_g sont $1, 1, 2, 4, 7, 12, 23, 39, 67, 118, 204, 343, 592, 1001, 1693, 2857, \ldots$

En 2008, M. Bras-Amorós formule [13] plusieurs conjectures sur la suite n_g. En particulier, elle conjecture la relation $n_{g+2} \geqslant n_g + n_{g+1}$ pour $g \in \mathbb{N}$. À ce jour, cette conjecture est toujours ouverte. Même la conjecture plus faible $n_{g+1} \geqslant n_g$, pour tout $g \in \mathbb{N}$, n'est toujours pas établie. Pour obtenir ses conjectures M. Bras-Amorós a déterminé les valeurs de n_g pour $g \leqslant 52$. Le calcul de $n_{50} = 101\,090\,300\,128$ à partir de la liste des semigroupes de genre 49 lui a pris 18 jours à l'aide d'un Pentium D cadencé à la fréquence de 3GHz. Ce résultat a ensuite été amélioré par M. Delgado qui a obtenu la valeur de n_{55}.

Exploration de l'arbre des semigroupes numériques [69]

Avec F. Hivert [69], nous avons introduit une nouvelle façon de représenter les semigroupes numériques propice à une optimisation multi-échelles. Les semigroupes numériques sont alors représentés par des tableaux finis d'entiers. L'exploration de l'arbre des semigroupes numériques se fait alors en modifiant les tableaux ainsi obtenus. Grâce au jeu d'instructions SSE des processeurs modernes nous pouvons traiter simultanément 16 entrées d'un tel tableau. Nous parallélisons ensuite l'exploration de l'arbre en utilisant les différents coeurs du ou des processeurs disponibles. Avec cette approche, le calcul de n_{50} prend 489 secondes sur un ordinateur muni d'un processeur équipé de quatre cœurs cadencés à la fréquence de 3.8 GHz. Finalement nous avons obtenu toutes les valeurs de n_g pour $g \leqslant 70$ en un peu moins d'un mois. En particulier nous obtenons la valeur $n_{70} = 1\,607\,394\,814\,170\,158$.

Sur les conjectures de M. Bras-Amorós [51, 53]

La *profondeur* q d'un semigroupe numérique S est $q = \lceil c/m \rceil$. Remarquons qu'un semigroupe de genre g a une profondeur au plus g. On note n'_g le nombre de semigroupes numériques de genre g vérifiant $q \leqslant 3$. Par un résultat de A. Zhai [134] nous savons que le rapport n'_g/n_g converge vers 1. Les semigroupes numériques vérifiant la relation $q \leqslant 3$ sont ainsi *génériques*. Avec S. Eliahou, nous avons développé [53] un nouveau point de vue pour l'étude des semigroupes numériques, basé sur la notion de *filtration de gouffre* d'un

semigroupe numérique. En utilisant cette nouvelle approche nous établissons une version *générique* de la conjecture de M. Bras-Amorós. Plus précisément nous obtenons

$$n'_{g-1} + n'_{g-2} \leqslant n'_g \leqslant n'_{g-1} + n'_{g-2} + n'_{g-3}.$$

En reprenant les idées développées dans [53] nous obtenons, avec S. Eliahou, une preuve conceptuelle [51] de la croissance de la suite n_g dans le cas restreint des semigroupes de multiplicité 3 et 4. Ce résultat avait déjà été obtenu par P. A. García-Sánchez, D. Marín-Aragón et A. M. Robles-Pérez en 2018 [72] par ordinateur, à l'aide des coordonnées de Kunz et grâce au recours à un logiciel de calcul symbolique.

Sur la conjecture de Wilf [52]

Avec S. Eliahou nous nous sommes intéressés à la conjecture de Wilf [52]. Nous associons à tout semigroupe S un nombre $W_0(S)$ vérifiant $W(S) \geqslant W_0(S)$. La relation $W_0(S) \geqslant 0$ pour tout S permettrait ainsi d'établir la conjecture de Wilf. Dans [47], S. Eliahou a établi que tout semigroupe numérique générique vérifie $W_0(S) \geqslant 0$ et donc la conjecture de Wilf. En utilisant l'algorithme d'exploration de l'arbre des semigroupes numériques introduit dans [69] nous avons pu montrer que parmi les plus de 10^{13} semigroupes numériques S de genre $g \leqslant 60$ seulement 5 ne vérifient pas $W_0(S) \geqslant 0$. Ces exceptions sont de genres respectifs $43, 51, 55, 55$ et 59 et vérifient toutes $W_0(S) = -1$ ainsi que la conjecture de Wilf ; les valeurs de $W(S)$ étant 35, 53, 62, 62 et 71. Leur étude nous a permis de prouver l'existence, pour tout entier $n \geqslant 3$, d'un semigroupe numérique S satisfaisant $W_0(S) = -\binom{n}{3}$. Les semigroupes ainsi obtenus vérifient tous la conjecture de Wilf.

Théorie de Ramsey

Triplets Pythagoriciens [54]

Un triplet d'entiers (x, y, z) de $\mathbb{N} \setminus \{0\}$ est dit Pythagoricien s'il satisfait $x^2 + y^2 = z^2$. Une *coloration* d'un ensemble X avec k couleurs est une application de X dans un ensemble de cardinal k fixé. Une question typique en théorie de Ramsey est de déterminer si pour toute coloration de $\mathbb{N}\setminus\{0\}$ avec k couleurs, il existe au moins un triplet Pythagoricien monochromatique. Autrement dit, nous nous demandons si l'équation $X^2 + Y^2 = Z^2$ est k-régulière pour $k \geqslant 2$. Ce problème a été posé pour la première fois en 1980 par P. Erdős et R. L. Graham [59] dans le cas à deux couleurs ($k = 2$). En 2016, M. J. H. Heule, O. Kullmann et V. W. Marek montrent [80] que pour toute coloration en 2 couleurs de l'intervalle d'entiers $[1, 7825]$ il existe un triplet Pythagoricien monochromatique. La preuve donnée utilise des calculs `SAT` massifs. La validité du calcul est donnée par une certification `DART`.

Avec S. Eliahou, V. Marion-Poty et D. Robilliard nous avons étudié [54] des colorations particulières en 2 et 3 couleurs. Au lieu de colorier tous les entiers, nous colorions les nombres premiers avec des éléments de $\mathbb{Z}/k\mathbb{Z}$. Nous étendons alors le coloriage à tous les éléments de $\mathbb{N} \setminus \{0\}$ de manière morphique. Dans le cas dichromatique, $k = 2$, nous prouvons que pour tout coloriage morphique de l'intervalle d'entiers $I_2 = [1, 533]$, il existe un triplet Pythagoricien monochromatique dans I_2, et 533 est minimal pour cette propriété. Nous obtenons un résultat similaire pour 3 couleurs avec l'intervalle d'entiers $I_3 = [1, 4633]$.

Nombres de Schur faibles [56]

Un ensemble P de $\mathbb{N} \setminus \{0\}$ est dit *faiblement libre de somme* s'il ne contient pas d'éléments x, y, z avec $z = x + y$ et $x \neq y$. En 1941 R. Rado [105] montre que pour tout $k \geqslant 1$, il existe un entier n maximal tel que l'intervalle d'entiers $[1, n]$ admette une partition en k sous-ensembles faiblement libres de somme, c'est le k-ème nombre de Schur faible, noté $WS(k)$. On obtient assez facilement WS(1) = 2, WS(2) = 8 et WS(3) = 23. En 2006, P.F. Blanchard, F. Harary et R. Reis [10] obtiennent WS(4) = 66 qui est le dernier nombre de Schur faible connu à ce jour. En 2002, S. Eliahou, J.M. Marín, M.P. Revuelta et M.I. Sanz [56] obtiennent les relations WS(5) $\geqslant$ 196 et WS(6) $\geqslant$ 572.

À l'aide d'une méthode d'exploration de Monte-Carlo, nous avons obtenu WS(6) $\geqslant$ 582 avec S. Eliahou, C. Fonlupt, V. Marion-Poty, D. Robilliard et F. Teytaud [49].

Organisation du texte

Ce mémoire est composé de deux parties.

La première partie traite des groupes des tresses et de la théorie des nœuds et est divisée en quatre chapitres. Le chapitre I est une introduction aux groupes des tresses généralisées ainsi qu'à leurs structures de Garside ; des résultats de ce chapitre seront utilisés aux chapitres II et III. Le chapitre II est consacré à la forme normale tournante. Après un bref aperçu des résultats obtenus durant ma thèse nous montrons que les mots tournants forment un langage rationnel. Dans le chapitre III nous étudions la combinatoire des suites normales de Garside pour les monoïdes d'Artin–Tits. Nous montrons alors que la combinatoire est donnée par une matrice d'adjacence d'un certain graphe. Dans le cas des monoïdes des tresses de type **B** nous montrons, à l'aide d'une algèbre de Hopf définie sur les permutations signées, que le polynôme caractéristique de la matrice d'adjacence de rang n divise celui de rang $n + 1$. Le chapitre IV est consacré à la construction d'une famille infinie de nœuds premiers ayant un polynôme de Jones trivial modulo n'importe quelle puissance donnée de 2.

La seconde partie traite de la combinatoire additive et de la théorie de Ramsey. Le chapitre V est une introduction aux semigroupes numériques et présente l'approche algorithmique que nous avons développée pour explorer efficacement l'arbre des semigroupes numériques. Les résultats que nous avons obtenus autour de la conjecture de Wilf sont présentés dans ce chapitre. Le chapitre VI présente la notion de filtration de gouffre de semigroupes numériques et les résultats que cela nous a permis d'obtenir sur les conjectures de M. Bras-Amorós. Ce chapitre repose sur le chapitre précédent. Dans le chapitre VII, nous nous intéressons aux coloriages morphiques ou partiellement morphiques des entiers positifs évitant les triplets pythagoriciens monochromatiques. Le dernier chapitre de cette partie est consacré aux nombres de Schur faibles et à la façon dont nous avons exploité une méthode d'exploration de Monte-Carlo pour obtenir la plus longue partition faiblement libre de somme à 6 couleurs connue à ce jour.

Notations

Dans tous ce mémoire $\mathbb{N}_+$ désigne l'ensemble des entiers strictement positifs et si a, b sont des entiers de $\mathbb{Z}$ vérifiant $a \leqslant b$, la notation $[a, b]$ désigne l'ensemble $\{a, a+1, \ldots, b\}$.

Groupes des tresses et théorie des nœuds

I. Groupes des tresses

Les groupes des tresses sont des objets fascinants, en particulier parce qu'ils sont assez simples pour être accessibles à l'étude et en même temps assez difficiles pour donner lieu à des résultats profonds. Une autre raison de l'intérêt des groupes des tresses est sans doute les approches variées qu'ils offrent : algébrique, combinatoire, algorithmique, géométrique ou topologique.

Il semble que la première référence où les groupes des tresses soient explicitement introduits et étudiés soit un texte de E. Artin qui fût publié en 1925 [2]. Ce texte a ensuite été republié sous une forme légèrement différente en 1947 [3]. Cependant la notion de tresse et plusieurs idées qui y sont liées remontent au XIXe siècle, dans les travaux d'A. Hurwitz, F. Klein, B. Riemann et certainement d'autres. On peut même trouver un schéma de tresse dans des notes de C. F. Gauß.

Aux alentours de 1984, V. Jones découvre [85] un lien profond entre les groupes des tresses et la théorie des opérateurs, la mécanique statistique et d'autres notions de physique mécanique. En 1994, P. Dehornoy a montré [26] que les groupes des tresses sont des groupes ordonnables compatibles avec la multiplication à gauche. Au début des années 2000, D. Krammer [88, 89] et S. Bigelow [6] ont établi la linéarité des groupes des tresses, c'est-à-dire l'existence d'une représentation fidèle dans un espace vectoriel de dimension finie.

De nombreuses généralisations des groupes des tresses ont été introduites. En 1966, J. Tits a défini et étudié les groupes des tresses associés à des groupes de Coxeter quelconques [127]. Cette étude a été poursuivie en 1972 par P. Deligne dans [44] et E. Brieskorn avec K. Saito dans [15]. En 1998, M. Broué, G. Malle et R. Rouquier ont étendu l'étude aux groupes des tresses de groupes de réflexions complexes [17]. En 1999, P. Dehornoy et L. Paris ont introduit la notion de groupe de Garside [39], une version abstraite de l'approche développée par F. A. Garside pour les groupes des tresses dans [73].

La section 1 de ce chapitre est une introduction aux groupes des tresses classiques tandis que les sections 2 et 3 sont des introductions aux groupes d'Artin–Tits et aux groupes de Garside respectivement. Ce chapitre n'a pas pour but d'être exhaustif et ne présente aucun de mes travaux de recherche mais il servira de base aux chapitres 2 et 3.

1 Groupes des tresses

Originellement introduit par E. Artin en 1925 dans [2] comme le groupe des classes d'isotopie des tresses géométriques, le groupe des tresses B_n peut être décrit de façon purement algébrique à l'aide de générateurs et de relations.

Théorème 1.1 (E. Artin [3]). *Le groupe des tresses B_n admet la présentation suivante*

$$B_n = \left\langle \sigma_1, ..., \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\,\sigma_j = \sigma_j\,\sigma_i & \textit{pour } |i-j| \geqslant 2 \\ \sigma_i\,\sigma_j\,\sigma_i = \sigma_j\,\sigma_i\,\sigma_j & \textit{pour } |i-j| = 1 \end{array} \right\rangle. \tag{1.1}$$

D'un point de vue géométrique, le générateur σ_i désigne la tresse élémentaire où seulement les brins i et $i+1$ se croisent, le brin originellement à la position $i+1$ passant au dessus de l'autre (voir figure 1).

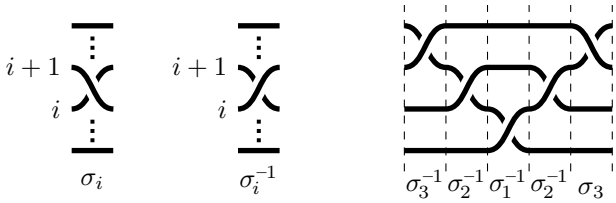


FIGURE 1.1 – Interprétation d'un mot en les lettres $\sigma_i^{\pm 1}$ comme diagramme de tresse géométrique.

Notation 1.2. On note $\mathscr{S}_n$ l'alphabet $\{\sigma_1, \ldots, \sigma_{n-1}\}$ et $\mathscr{S}_n^{\pm}$ l'alphabet

$$\mathscr{S}_n^{\pm} = \mathscr{S}_n \sqcup \mathscr{S}_n^{-1} = \{\sigma_1^{\pm 1}, \ldots, \sigma_{n-1}^{\pm 1}\}.$$

Les mots sur un alphabet donné apparaîtront à divers endroits de cette partie. Fixons dès maintenant une notation générale.

Définition 1.3. Un mot sur un alphabet $\mathscr{A}$ quelconque est appelé $\mathscr{A}$-mot. Le mot vide est noté ε.

Le théorème 1.1 nous permet ainsi de décrire une tresse de B_n comme une classe d'équivalence de $\mathscr{S}_n^{\pm}$-mots.

Définition 1.4. Pour w un $\mathscr{S}_n^{\pm}$-mot on note $\overline{w}$ la tresse associée à w et on dit alors que w est un *représentant* de $\overline{w}$. L'équivalence entre les $\mathscr{S}_n^{\pm}$-mots donnée à la présentation (1.1) est notée $\equiv$.

La description du groupe des tresses B_n donnée au théorème 1.1 n'est donc utilisable, en pratique, que si nous sommes capable de décider si deux $\mathscr{S}_n^{\pm}$-mots quelconques sont équivalents vis-à-vis de $\equiv$ et donc s'ils représentent la même tresse. C'est le *problème des mots*.

1.1 Problème des mots

Considérons une présentation $\langle \mathscr{A} \mid R \rangle^+$ d'un monoïde M quelconque. Une présentation de groupe est alors une présentation de monoïde particulière comme l'illustre l'isomorphisme suivant :

$$\langle \mathscr{A} \mid R \rangle \simeq \left\langle \mathscr{A} \sqcup \mathscr{A}^{-1} \mid R \cup \{aa^{-1} = a^{-1}a = \varepsilon \mid a \in \mathscr{A}\} \right\rangle^+$$

Problème 1.5 (dit des mot)**.** Décider si deux $\mathscr{A}$-mots u et v sont équivalents vis à vis de la plus petite congruence de monoïde $\equiv_R$ contenant les relations de R.

En 1947, E. Post établit que le problème des mots pour les monoïdes est indécidable en général [103]. Ce résultat est amélioré la même année par A. A. Markov.

Théorème 1.6 (A. A. Markov [94])**.** *Il existe un alphabet $\mathscr{A}$ de cardinal* 13 *et un ensemble fini de* 33 *relations R tels que le problème des mots pour la présentation de monoïde $\langle \mathscr{A} \mid R \rangle^+$ soit indécidable.*

En 1955, P. S. Novikov obtient le même résultat d'indécidabilité pour une présentation finie de groupe [98].

Heureusement pour nous, le cas des groupes des tresses est plus simple. E. Artin donne dans [3] une solution du problème des mots pour (1.1) à l'aide de la construction d'une injection du groupe des tresses B_n dans les automorphismes du groupe libre F_n, connu sous le nom de *représentation d'Artin.*

1.2 Ordre des tresses

Un ordre total $<$ défini sur un groupe G est dit *invariant à gauche* si la relation $g < h$ implique $fg < fh$ pour tous f, g et h de G. En 1994, P. Dehornoy construit [26] un ordre total invariant à gauche sur le groupe des tresses B_n. Cet ordre est facilement décrit à l'aide de mots de tresse d'un type particulier.

Définition 1.7. Un $\mathscr{S}_n^{\pm}$-mot est *σ-défini* si la lettre σ_i de plus haut indice apparaît

— soit que positivement (pas de σ_i^{-1}), nous disons alors que ce mot est σ_i-positif,

— soit que négativement (pas de σ_i), nous disons alors que ce mot est σ_i-négatif.

Une tresse est dite σ_i-positive, *resp.* σ_i-négative, si elle admet un représentant σ_i-positif, *resp.* σ_i-négatif.

Par exemple le mot $\sigma_2\sigma_1\sigma_2^{-1}$ n'est pas σ-défini car le générateur d'Artin de plus haut indice σ_2 apparaît positivement et négativement. Par contre le mot $\sigma_1^{-1}\sigma_2\sigma_1$, qui lui est $\equiv$-équivalent, est σ_2-positif, et donc σ-défini.

Définition 1.8. Pour β et γ deux tresses de B_n, nous posons $\beta < \gamma$ si la tresse quotient $\beta^{-1}\gamma$ peut être représentée par un mot σ_i-positif.

D'après l'exemple précédent nous avons donc $\sigma_1 < \sigma_2\sigma_1$.

Théorème 1.9 (P. Dehornoy [26])**.** *Pour tout $n \geqslant 2$, la relation $<$ est un ordre total invariant par multiplication à gauche sur B_n.*

La démonstration du théorème repose sur l'établissement des deux propriétés suivantes :

Propriété A (d'Acyclicité). Une tresse représentée par un mot σ-défini est non triviale.

Propriété C (de Comparaison). Une tresse non triviale admet un représentant σ-défini.

Des démonstrations variées de ces deux propriétés sont disponibles dans le livre [37] de P. Dehornoy avec I. Dynnikov, D. Rolfsen et B. Wiest. Notons que la propriété **A** peut être démontrée à l'aide de la représentation d'Artin et qu'une démonstration algorithmique à l'aide de *réductions de poignées* est décrite par P. Dehornoy dans [27].

Remarque 1.10. Une conséquence des propriétés **A** et **C** est que pour une tresse β non triviale donnée il existe un unique $i \geqslant 1$ tel que β soit ou bien σ_i-positive ou bien σ_i-négative.

Remarquons que l'ordre des tresses donne une solution au problème des mots. Pour deux $\mathscr{S}_n^{\pm}$-mots u et v nous posons $w = u^{-1}v$ et décidons, à l'aide de l'algorithme de réduction des poignées, par exemple, si la tresse $\overline{w}$ est représentée par un mot σ-défini. Si c'est le cas alors u et v ne sont pas équivalents, et ils sont équivalents sinon.

1.3 Monoïde des tresses positives

En 1969, F. A. Garside décrit dans [73] une solution au problème des mots à l'aide du monoïde des tresses positives B_n^+.

Définition 1.11. Le *monoïde des tresses positives à n brins*, noté B_n^+ est le monoïde admettant la présentation suivante :

$$B_n^+ = \left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\,\sigma_j = \sigma_j\,\sigma_i & \text{pour } |i-j| \geqslant 2 \\ \sigma_i\,\sigma_j\,\sigma_i = \sigma_j\,\sigma_i\,\sigma_j & \text{pour } |i-j| = 1 \end{array} \right\rangle^+ . \tag{1.2}$$

Remarquons que la présentation du monoïde B_n^+ est la même que celle de B_n à l'exception que c'est une présentation de monoïde et non celle d'un groupe. À ce stade nous ne pouvons rien dire sur les liens existant entre le monoïde B_n^+ et le groupe B_n. Il se pourrait, par exemple, que B_n^+ ne soit pas inclus dans B_n et ce malgré la similarité des deux présentations, comme l'illustre l'exemple suivant

Exemple 1.12. Soit M le monoïde de présentation $\langle a, b \,|\, a\,b = a\rangle^+$ et G le groupe de présentation $\langle a, b \,|\, ab = a\rangle$. Notons $\equiv_M$ et $\equiv_G$ les équivalences associées aux présentations de M et G respectivement. Pour $\equiv_G$ nous avons $a\,b \equiv_G a$ puis $a^{-1}\,a\,b \equiv_G a^{-1}\,a$ et donc $b \equiv_G \varepsilon$. Pour $\equiv_M$ nous constatons que b est seul dans sa classe d'équivalence et donc $b \not\equiv_M \varepsilon$. Il ne peut donc pas exister d'injection de M dans G.

Le théorème 1.15 donne des conditions suffisantes pour qu'un monoïde donné par une présentation s'injecte dans le groupe de même présentation. Avant d'énoncer ce théorème nous avons besoin de deux définitions.

Définition 1.13. Un monoïde M est *simplifiable à gauche*, *resp. à droite*, si pour tous a, b, c de M la relation $ca = cb$, *resp.* $ac = bc$, implique $a = b$. Il est dit *simplifiable* s'il est simplifiable à gauche et à droite.

Remarquons que le monoïde de l'exemple 1.12 n'est pas simplifiable à gauche car nous avons la relation $ab \equiv_M a$ sans avoir $b \equiv_M \varepsilon$.

Définition 1.14. Soit M un monoïde, et soient x et y deux éléments de M. Nous disons que x est un *diviseur à gauche* de y, ou de manière équivalente, que y est un *multiple à droite* de x, noté $x \preccurlyeq y$, si la relation $y = xz$ est vérifiée pour un certain élément z de M. De même nous définissons les notions de *diviseur à droite*, de *multiple à gauche* et la relation $y \succcurlyeq x$ lorsque nous avons $y = zx$ avec $z \in M$.

Nous pouvons maintenant énoncer le théorème de Ore.

Théorème 1.15 (O. Ore [99])**.** *Supposons que M soit un monoïde simplifiable et que deux éléments quelconques de M admettent un multiple commun à gauche. Alors il existe un unique groupe G à isomorphisme près ayant les propriétés suivantes :*

- *il existe un morphisme injectif ι de M dans G,*
- *tout élément de G, peut être exprimé comme fraction $\iota(a)^{-1}\,\iota(b)$ avec a et b des éléments de M.*

De plus si M admet la présentation $\langle S, R\rangle^+$ alors $\langle S, R\rangle$ est une présentation de G.

Une démonstration élémentaire du théorème de Ore est donnée dans [34]. Comme l'énonce la proposition suivante, le monoïde des tresses positives satisfait les conditions de Ore.

Proposition 1.16 (F.A. Garside [73])**.** *Le monoïde B_n^+ est simplifiable et admet des multiples communs à gauche.*

Ainsi grâce au théorème 1.15 nous savons que le monoïde B_n^+ s'injecte dans le groupe des tresses B_n et que ce dernier est le groupe des fractions du monoïde des tresses positives B_n^+. En fait nous avons mieux.

Définition 1.17. Nous définissons une tresse positive Δ_n de B_n^+ par récurrence sur $n \geqslant 1$, en posant $\Delta_1 = 1$ et

$$\Delta_n = (\sigma_1 \cdot \ldots \cdot \sigma_{n-1}) \cdot \Delta_{n-1}$$

Les premières valeurs de Δ_n sont

$$\Delta_2 = \overline{\sigma_1}, \quad \Delta_3 = \overline{\sigma_1\sigma_2\sigma_1} \quad \text{et} \quad \Delta_4 = \overline{\sigma_1\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1}.$$

Proposition 1.18 (F.A. Garside [73])**.** *Soit $n \in \mathbb{N}$. Pour toute tresse $\beta \in B_n$, il existe un unique entier $k \in \mathbb{N}$ et une unique tresse positive β' de B_n^+ non divisible à gauche par Δ_n tels que nous ayons $\beta = \Delta_n^{-k}\beta'$ avec $k \in \mathbb{N}$.*

Comme les relations de la présentation de B_n^+ donnée en (1.2) préservent la longueur des mots, une tresse positive est représentée par un nombre fini de $\mathscr{S}_n$-mots. Il est donc possible, partant d'un $\mathscr{S}_n$-mot, de déterminer tous les $\mathscr{S}_n$-mots qui lui sont $\equiv$-équivalents. Nous obtenons ainsi une solution au problème des mots pour le groupe B_n vis-à-vis de la présentation (1.1) dès que nous savons déterminer l'entier k et la tresse positive β' donnée à la proposition 1.18 pour toute tresse β de B_n.

L'étude du monoïde de B_n^+ faite par F. A. Garside dans [73] permet d'obtenir une solution bien plus efficace au problème des mots pour le monoïde B_n^+, puis pour le groupe B_n, à l'aide de la *forme normale de Garside*. P. Dehornoy et L. Paris ont généralisé la construction de cette forme normale à une famille plus vaste connue sous le nom de *monoïde de Garside*.

2 Groupes d'Artin–Tits

En 1966, J. Tits introduit [127] une généralisation des groupes des tresses. L'idée est de faire jouer le rôle du groupe symétrique $\mathfrak{S}_n$ naturellement associé au groupe des tresses B_n par n'importe quel groupe de Coxeter. Cette étude a été poursuivie en 1972 par P. Deligne dans [44] et E. Brieskorn avec K. Saito dans [15].

2.1 Groupe de Coxeter

Commençons par une notation.

Notation 2.1. Pour s et t deux lettres d'un alphabet $\mathscr{S}$ et m un entier de $\mathbb{N}$, on désigne par $\mathrm{prod}(s,t;m)$ le mot $ststst\cdots$ de longueur m.

Définition 2.2. Un groupe W est dit de *Coxeter* s'il existe un sous-ensemble $\mathscr{S}$ de W tel qu'on ait

$$W \simeq \left\langle \mathscr{S} \;\middle|\; \begin{array}{rll} s^2 & = 1 & \text{pour } s \in \mathscr{S} \\ \text{prod}(s,t;m_{s,t}) & = \text{prod}(t,s;m_{t,s}) & \text{pour } s,t \in \mathscr{S} \end{array} \right\rangle \tag{1.3}$$

où la matrice $(m_{s,t})$ est à valeur dans $\mathbb{N}\cup\{\infty\}$, est symétrique ($m_{s,t} = m_{t,s}$) et vérifie $m_{s,s} = 1$ ainsi que $m_{s,t} \geqslant 2$ pour $s \neq t$. Par convention $m_{s,t} = \infty$ signifie qu'il n'y a pas de relation imposée entre s et t. La paire $(W, \mathscr{S})$ est appelée *système de Coxeter*.

Remarquons que la présentation (1.3) est entièrement déterminée par la paire de Coxeter $(W, \mathscr{S})$. En effet pour s et t dans W, l'entier $m_{s,t}$ est alors le plus petit entier $k \geqslant 1$ tel que les éléments de W représentés par $\text{prod}(s,t;k)$ et $\text{prod}(t,s;k)$ soient égaux, dans le cas où un tel k existe. Si k n'existe pas nous posons $m_{s,t} = \infty$.

Exemple 2.3. Le groupe $\mathfrak{S}_3$ est un groupe de Coxeter car nous avons

$$\mathfrak{S}_3 \simeq \left\langle s_1, s_2 \;\middle|\; s_1^2 = 1,\ s_2^2 = 1,\ s_1 s_2 s_1 = s_2 s_1 s_2 \right\rangle$$

où s_1 et s_2 désignent les transpositions (1 2) et (2 3) respectivement.

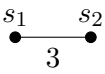
2.2 Diagramme de Dynkin

La présentation associée à un système de Coxeter peut être synthétisée à l'aide de son diagramme de Dynkin.

Définition 2.4. Un *diagramme de Dynkin* est un graphe simple, non orienté, étiqueté, sans boucle où les étiquettes sont à valeurs dans $\{3, \ldots\} \cup \{\infty\}$.

Le diagramme de Dynkin associé à une paire de Coxeter $(W, \mathscr{S})$ est alors le graphe ayant $\mathscr{S}$ comme ensemble de sommets et possédant une arête entre deux sommets distincts s et t si $m_{s,t} \geqslant 3$, l'arête est alors étiquetée $m_{s,t}$. Ainsi deux sommets s et t distincts ne sont pas reliés par une arête si et seulement si $m_{s,t}$ vaut 2 et donc si et seulement si les générateurs s et t de W commutent entre eux.

Exemple 2.5. Le diagramme de Dynkin associé à la paire de Coxeter $(\mathfrak{S}_3, \{s_1, s_2\})$ de l'exemple 2.3 est



Dans la pratique on caractérisera un système de Coxeter $(W, \mathscr{S})$ à l'aide de son diagramme de Dynkin.

Notation 2.6. Soit $\mathbf{\Gamma}$ un diagramme de Dynkin de sommets $\mathscr{S}$. On note $W_{\mathbf{\Gamma}}$ le groupe de Coxeter admettant la présentation de générateurs $\mathscr{S}$ et ayant pour relations celles associées aux arêtes de $\mathbf{\Gamma}$.

En notant $\mathbf{\Gamma_1}, \ldots, \mathbf{\Gamma_k}$ les composantes connexes d'un diagramme de Dynkin, nous obtenons que $W_{\mathbf{\Gamma}}$ est le produit direct $W_{\mathbf{\Gamma_1}} \times \cdots \times W_{\mathbf{\Gamma_k}}$.

Définition 2.7. Un diagramme de Dynkin $\mathbf{\Gamma}$ est dit de type *sphérique* si le groupe de Coxeter $W_{\mathbf{\Gamma}}$ associé est fini.

Pour les diagrammes de Dynkin connexes de type sphérique, qui sont en bijection avec les groupes de Coxeter irréductibles finis, H. S. M. Coxeter donne en 1935 la classification suivante :

Proposition 2.8 (H. S. M. Coxeter [24])**.** *Tout diagramme de Dynkin connexe de type sphérique appartient à l'une des familles infinies*

$$\mathbf{A_n} \text{ pour } n \geqslant 1, \ \mathbf{B_n} \text{ pour } n \geqslant 2, \ \mathbf{D_n} \text{ pour } n \geqslant 4 \text{ et } \mathbf{I_2}(p) \text{ pour } p \geqslant 5$$

ou à l'un des six diagrammes exceptionnels $\mathbf{E_6}$, $\mathbf{E_7}$, $\mathbf{E_8}$, $\mathbf{F_4}$, $\mathbf{H_3}$ *ou* $\mathbf{H_4}$.

Pour $\mathbf{\Gamma} = \mathbf{A_n}$, le groupe $W_{\mathbf{\Gamma}}$ est le groupe symétrique $\mathfrak{S}_{n+1}$.

2.3 Groupes et monoïdes d'Artin–Tits

Nous pouvons maintenant donner les définitions de groupes et de monoïdes d'Artin–Tits.

Définition 2.9. Pour tout diagramme de Dynkin $\mathbf{\Gamma}$ de sommets $\mathscr{S}$, le *groupe des tresses* $B_{\mathbf{\Gamma}}$ est le groupe présenté par :

$$B_{\mathbf{\Gamma}} = \big\langle \mathscr{S} \;\big|\; \mathrm{prod}(s,t;m_{s,t}) = \mathrm{prod}(t,s;m_{t,s}) \text{ pour } s,t \in \mathscr{S} \big\rangle,$$

et le monoïde des tresses positives est le monoïde présenté par :

$$B^+_{\mathbf{\Gamma}} = \big\langle \mathscr{S} \;\big|\; \mathrm{prod}(s,t;m_{s,t}) = \mathrm{prod}(t,s;m_{t,s}) \text{ pour } s,t \in \mathscr{S} \big\rangle^+.$$

Pour $\mathbf{\Gamma} = \mathbf{A_n}$, le groupe des tresses $B_{\mathbf{A_n}}$ est le groupe des tresses classiques B_{n+1} et le monoïde $B^+_{\mathbf{A_n}}$ est le monoïde des tresses positives B^+_{n+1} introduit à la sous-section 1.3.

Question 2.10. Soit $\mathbf{\Gamma}$ un diagramme de Dynkin. Le problème des mots sur $B_{\mathbf{\Gamma}}$ a-t-il une solution vis à vis de la présentation donnée à la définition 2.9 ?

Excepté pour un petit nombre de cas nous ne connaissons pas de solution générale à la question précédente. Dans le cas où le diagramme de Dynkin $\mathbf{\Gamma}$ est de type sphérique alors nous montrons, voir sous-section 3.3, que le monoïde de $B^+_{\mathbf{\Gamma}}$ admet une structure de Garside qui donne une solution au problème des mots pour $B^+_{\mathbf{\Gamma}}$ puis pour $B_{\mathbf{\Gamma}}$. Une telle structure n'existe pas lorsque $\mathbf{\Gamma}$ n'est plus de type sphérique : les diviseurs de l'élément de Garside, qui doivent être en nombre fini (voir définition 3.1), étant en bijection avec les éléments du groupe de Coxeter $W_{\mathbf{\Gamma}}$ qui est infini.

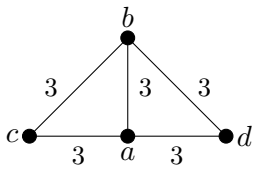
Comme dans le cas du groupe des tresses, le monoïde $B^+_{\mathbf{\Gamma}}$ s'injecte dans le groupe $B_{\mathbf{\Gamma}}$. Dans le cas des groupes d'Artin–Tits de type sphérique nous utilisons, comme pour les tresses classiques, la structure de Garside de $B^+_{\mathbf{\Gamma}}$ décrite à la sous-section 3.3. Lorsque $\mathbf{\Gamma}$ n'est plus de type sphérique, la preuve de l'injection de $B^+_{\mathbf{\Gamma}}$ dans $B_{\mathbf{\Gamma}}$ a été donnée par L. Paris en 2002 dans [101].

En 2015, dans [36], P. Dehornoy, M. Dyer et C. Hohlweg ont montré que le monoïde $B^+_{\mathbf{\Gamma}}$ admet toujours une *famille de Garside* qui est close par supremum et infimum vis à vis de l'ordre faible défini sur le groupe de Coxeter $W_{\mathbf{\Gamma}}$. Cette famille pourrait permettre de faire des avancées sur le problème des mots de certains groupes des tresses généralisées de type autre que sphérique.

D'autres solutions à la question 2.10 pourraient venir de la notion de *multifraction* introduite par P. Dehornoy et ses collaborateurs dans [32, 33, 38] en 2017. Cette approche a permis de donner de nouvelles solutions au problème des mots pour les groupes de type 3-Ore, de type FC et ceux de type suffisamment grand. Il est intéressant de noter que le plus petit exemple pour lequel rien n'est connu est le groupe

$$\langle a, b, c, d \mid aba = bab, aca = cac, bcb = cbc, ada = dad, bdb = dbd, cd = dc \rangle,$$

associé au diagramme de Dynkin



3 Monoïdes et groupes de Garside

Cette section présente une brève introduction à la théorie de Garside. Pour plus de détails, le lecteur pourra consulter l'article fondateur de P. Dehornoy et L. Paris [39] ou encore le livre [35] écrit par P. Dehornoy avec F. Digne, E. Godelle, D. Krammer et J. Michel.

3.1 Définitions

Les définitions de monoïde et de groupe de Garside ont mis un peu de temps à se stabiliser en fonction des auteurs et des propriétés souhaitées. Dans ce mémoire nous utilisons celle de [35].

Définition 3.1 (Définition I.2.1 de [35])**.** Un *monoïde de Garside* est un couple (M, Δ), où M est un monoïde et Δ un élément de M vérifiant

- M est simplifiable,
- il existe une application $\lambda : M \to \mathbb{N}$ satisfaisant $\lambda(fg) \geqslant \lambda(f) + \lambda(g)$ et $\lambda(g)$ est non nul pour tout $g \neq 1$,
- deux éléments quelconques de M admettent des ppcm et des pgcd à gauche et à droite,
- Δ est un *élément de Garside* de M, c'est-à-dire, les diviseurs à gauche et à droite de Δ coïncident et engendrent M,
- l'ensemble des diviseurs de Δ est fini.

Un groupe G est appelé *groupe de Garside* s'il est le groupe des fractions d'un monoïde de Garside.

Par définition, les diviseurs à gauche et à droite de Δ coïncident, nous pouvons donc parler des diviseurs de Δ.

Définition 3.2. Soit (M, Δ) un monoïde de Garside, les diviseurs de Δ sont les *simples* de (M, Δ).

Tous les monoïdes de Garside M que nous considérons dans ce mémoire sont donnés à l'aide d'une présentation préservant la longueur des mots, comme pour le monoïde des tresses positives B_n^+. Dans ce cas, nous pouvons définir sur M une fonction *longueur* par

$$\begin{array}{rccc} \ell : M & \to & \mathbb{N} \\ \overline{w} & \mapsto & |w| \end{array} \tag{1.4}$$

Sans surprise, l'étude de B_n^+ faite par F. A. Garside dans [73] donne le résultat suivant.

Proposition 3.3 (F. A. Garside [73])**.** *Pour tout $n \geqslant 2$, la paire (B_n^+, Δ_n) est un monoïde de Garside.*

3.2 Forme normale de Garside

Nous pouvons maintenant donner la définition de la forme normale de Garside.

Proposition 3.4 (Proposition I.2.4 de [35])**.** *Soit (M, Δ) un monoïde de Garside. Notons G le groupe des fractions de M. Tout élément de G admet une décomposition unique de la forme $\Delta^k s_1 \cdot \ldots \cdot s_p$ avec $k \in \mathbb{Z}$ et où $s_1, \ldots, s_p$ sont des simples de M satisfaisant $s_1 \neq \Delta$, $s_p \neq 1$ et, pour tout i,*

$$\forall g \in M \setminus \{1\} \ \ (g \preccurlyeq s_{i+1} \Rightarrow s_i\, g \not\preccurlyeq \Delta)\,. \tag{1.5}$$

Remarquons que la condition (1.5) est équivalente à

$$\mathrm{pgcd}_g(s_i\, s_{i+1}, \Delta_n) = s_i. \tag{1.6}$$

où $\mathrm{pgcd}_g(a, b)$ désigne le plus grand diviseur à gauche commun à a et b.

Nous obtenons immédiatement le corollaire suivant.

Corollaire 3.5. *Soit (M, Δ) un monoïde de Garside. Tout élément de M admet une décomposition unique de la forme $s_1 \cdot \ldots \cdot s_p$ où $s_1, \ldots, s_p$ sont des simples de M vérifiant $s_p \neq 1$ et* (1.5) *pour tout i.*

3.3 Structure de Garside de $B_{\mathbf{\Gamma}}^+$

Dans la suite $\mathbf{\Gamma}$ désigne un diagramme de Dynkin de type sphérique et $(W_{\mathbf{\Gamma}}, \mathscr{S}_{\mathbf{\Gamma}})$ le système de Coxeter associé.

Comme $\mathscr{S}_{\mathbf{\Gamma}}$ est une partie génératrice du groupe $W_{\mathbf{\Gamma}}$, tout élément de $W_{\mathbf{\Gamma}}$ peut être représenté par un $\mathscr{S}_{\mathbf{\Gamma}}$-mot. Un élément g de $W_{\mathbf{\Gamma}}$ peut être représenté par différents $\mathscr{S}_{\mathbf{\Gamma}}$-mots qui peuvent être de longueurs différentes à cause de la relation $s^2 = 1$ qui est valide pour tout générateur s de $\mathscr{S}_{\mathbf{\Gamma}}$.

Définition 3.6. Soit g un élément de $W_{\mathbf{\Gamma}}$. La *longueur* de g, notée $\ell(g)$, est la plus petite longueur d'un $\mathscr{S}_{\mathbf{\Gamma}}$-mot u représentant g. Le mot u est alors dit *réduit*.

Le lemme suivant est une conséquence non triviale du lemme d'échange et décrit comment passer d'une expression réduite d'un élément de $W_{\mathbf{\Gamma}}$ à une autre.

Lemme 3.7 (H. Matsumoto [95])**.** *Soient u et v deux $\mathscr{S}_{\mathbf{\Gamma}}$-mots réduits représentant le même élément dans $W_{\mathbf{\Gamma}}$. Nous pouvons passer de u à v sans utiliser les relations du type $s^2 = 1$. En particulier u et v sont de même longueur.*

Une démonstration du lemme de Matsumoto est donnée page 441 de [35].

Définition 3.8. Pour tous éléments g et h de $W_{\mathbf{\Gamma}}$ nous posons $g \preccurlyeq_{\mathbf{\Gamma}} h$ dès que la relation $\ell(h) = \ell(g) + \ell(g^{-1}h)$ est vérifiée.

La relation $\preccurlyeq_{\mathbf{\Gamma}}$ est connue sous le nom d'*ordre faible* de $W_{\mathbf{\Gamma}}$ et munit le groupe de Coxeter $W_{\mathbf{\Gamma}}$ d'une structure de treillis. Le lecteur intéressé pourra, par exemple, consulter le chapitre 3 du livre de A. Björner et F. Brenti [9]. En particulier il existe un unique élément $\preccurlyeq_{\mathbf{\Gamma}}$-maximal dans $W_{\mathbf{\Gamma}}$.

Définition 3.9. L'élément maximum de $W_{\mathbf{\Gamma}}$ vis-à-vis de $\preccurlyeq_{\mathbf{\Gamma}}$, noté $w_{\mathbf{\Gamma}}$, est l'*élément de Coxeter* de $W_{\mathbf{\Gamma}}$.

L'élément de Coxeter $w_{\mathbf{\Gamma}}$ peut aussi être caractérisé comme l'unique élément g du groupe $W_{\mathbf{\Gamma}}$ tel que $\ell(g)$ soit maximal.

Remarquons que le groupe de Coxeter $W_{\mathbf{\Gamma}}$ est un quotient du monoïde d'Artin–Tits $B^+_{\mathbf{\Gamma}}$ par les relations $s^2 = 1$. Afin de lever toute ambiguïté nous utiliserons les notations suivantes qui ne seront utilisées que dans ce chapitre.

Notation 3.10. Pour $s \in \mathscr{S}_{\mathbf{\Gamma}}$, on note $\tilde{s}$ l'image de s dans $W_{\mathbf{\Gamma}}$ et $\check{s}$ l'image de s dans $B^+_{\mathbf{\Gamma}}$.

Nous avons ainsi un homomorphisme surjectif π naturel défini par :

$$\begin{array}{rccc} \pi : & B^+_{\mathbf{\Gamma}} & \to & W_{\mathbf{\Gamma}} \\ & \check{s} & \mapsto & \tilde{s} \end{array} \tag{1.7}$$

Construisons maintenant une section ensembliste de l'application π.

Définition 3.11. Pour $g \in W_{\mathbf{\Gamma}}$ nous définissons $r(g)$ comme étant la tresse $\check{x_{i_1}} \cdots \check{x_{i_k}}$ où $x_{i_1} \cdots x_{i_k}$ est un $\mathscr{S}_{\mathbf{\Gamma}}$-mot réduit représentant g.

Le lemme 3.7 garantit que l'application r est bien définie. Nous obtenons immédiatement la propriété désirée.

Lemme 3.12. *L'application $r : W_{\mathbf{\Gamma}} \to B^+_{\mathbf{\Gamma}}$ vérifie $\pi \circ r = \mathbf{1}_{W_{\mathbf{\Gamma}}}$.*

Définition 3.13. Pour tout diagramme de Dynkin $\mathbf{\Gamma}$ de type sphérique, nous posons $\Delta_{\mathbf{\Gamma}} = r(w_{\mathbf{\Gamma}})$, où $w_{\mathbf{\Gamma}}$ est l'élément de Coxeter de $W_{\mathbf{\Gamma}}$.

Nous avons finalement tout mis en place pour établir la structure de Garside du monoïde $B^+_{\mathbf{\Gamma}}$.

Théorème 3.14 (Proposition IX.1.29 de [35])**.** *Pour tout diagramme de Dynkin $\mathbf{\Gamma}$ de type sphérique la paire $(B^+_{\mathbf{\Gamma}}, \Delta_{\mathbf{\Gamma}})$ est un monoïde de Garside.*

De plus nous avons l'isomorphisme de treillis suivant :

Proposition 3.15. *Pour tout diagramme de Dynkin $\mathbf{\Gamma}$ de type sphérique nous avons l'isomorphisme de treillis*

$$(W_{\mathbf{\Gamma}}, \preccurlyeq_{\mathbf{\Gamma}}) \simeq (r\,(W_{\mathbf{\Gamma}}), \preccurlyeq)$$

où $\preccurlyeq$ est la relation de divisibilité à gauche *sur $B^+_{\mathbf{\Gamma}}$ définie à la définition 1.14.*

En particulier nous obtenons la caractérisation suivante des tresses simples de $B^+_{\mathbf{\Gamma}}$.

Proposition 3.16. *Une tresse x de $B^+_{\mathbf{\Gamma}}$ est simple si et seulement si x appartient à $r\,(W_{\mathbf{\Gamma}})$.*

II. Forme normale tournante

En 1998, J. S. Birman, K. H. Ko et S .J. Lee [8] ont introduit et étudié un nouveau sous-monoïde B_n^{+*} de B_n. Ce monoïde est connu sous le nom de *monoïde de Birman–Ko–Lee*. Le terme *monoïde des tresses duales* a été proposé ultérieurement et provient du fait que certains paramètres obtiennent des valeurs symétriques s'ils sont évalués dans B_n^+ ou B_n^{+*} ; une correspondance qui a été étendue par D. Bessis en 2003 au contexte plus général des groupes d'Artin–Tits [4]. Nous savons depuis les travaux de J. S. Birman, K. H. Ko et S. J. Lee que le monoïde des tresses duales B_n^{+*} peut être muni d'une structure de Garside.

En 1996, R. Laver a montré [90] que la restriction de l'ordre des tresses $<$ à une famille de sous-monoïdes de B_n, contenant en particulier le monoïde des tresses positives et le monoïde des tresses duales, donné lieu à des bons ordres, c'est-à-dire, des ordres sans suite infinie décroissante. En 1997, S. Burckel a montré [18] que la restriction de $<$ au monoïde B_n^+ était un bon ordre de type $\omega^{\omega^{n-2}}$.

C'est dans ce contexte que j'ai commencé ma thèse en 2006 sur la détermination du type d'ordre de la restriction de $<$ au monoïde des tresses duales. Pour répondre à la question, j'ai construit et étudié une nouvelle forme normale sur les monoïdes B_n^{+*} appelée *forme normale tournante* [65]. Nous pouvons considérer cette nouvelle forme normale comme une adaptation au contexte *dual* de la forme normale alternante introduite par P. Dehornoy en 2007 dans [31]. La forme normale tournante équipe naturellement le monoïde B_n^{+*} d'un bon ordre total $<^*$ de type $\omega^{\omega^{n-2}}$. Cependant la compatibilité de $<^*$ avec la multiplication à gauche dans B_n^{+*} est loin d'être évidente. À l'aide d'une étude approfondie de la forme normale tournante, j'ai montré dans [66] que les ordres $<$ et $<^*$ coïncident sur B_n^{+*}. En particulier le type d'ordre de la restriction de $<$ à B_n^{+*} est aussi $\omega^{\omega^{n-2}}$. Les techniques employées pour démontrer la coïncidence de ces deux ordres a permis d'obtenir une nouvelle démonstration algorithmique de la Propriété **C** (voir page 17) et de résoudre une conjecture ouverte depuis une quinzaine d'années sur l'existence d'un représentant σ-défini court pour chaque tresse de B_n [67]. Par la suite nous avons proposé, avec L. Paris, un algorithme simple permettant d'obtenir de tels représentants σ-définis courts [70].

À la fin de ma thèse j'ai commencé à étudier la forme normale tournante pour elle-même. En particulier, j'ai montré que le langage des mots tournants forme un langage rationnel et j'ai construit des automates finis déterministes reconnaissant ces langages. Bien que les résultats de ce chapitre soient en partie établis dans mon rapport de thèse, je n'ai publié ces travaux qu'en 2018 [68]. Beaucoup d'améliorations ont été apportées par rapport à ce qui avait été fait alors. Les énoncés sont plus généraux et plus clairs et des conséquences portant sur les représentants σ-définis sont développés dans [68].

1 Introduction

Le monoïde des tresses duales B_n^{+*} est un sous-monoïde de B_n engendré par des conjugués des tresses σ_i.

Notation 1.1. Pour tous $1 \leqslant i < j$, nous posons

$$a_{p,q} = \sigma_p \cdots \sigma_{q-2}\, \sigma_{q-1}\, \sigma_{q-2}^{-1} \cdots \sigma_p^{-1},$$

et pour tout $n \geqslant 2$, nous notons $\mathscr{A}_n$ l'ensemble $\{a_{p,q} \,|\, 1 \leqslant p < q \leqslant n\}$.

D'un point de vue géométrique, la tresse $a_{p,q}$ correspond au croisement des brins p et q, tous les deux passant en-dessous des brins intermédiaires.

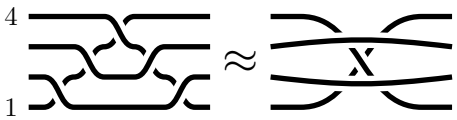


FIGURE 2.1 – Dans la tresse géométrique $a_{1,4}$, les brins 1 et 4 se croisent en dessous des brins 2 et 3.

Définition 1.2. Le *monoïde des tresses duales* B_n^{+*} est le sous-monoïde de B_n engendré par les tresses de $\mathscr{A}_n$.

Remarque 1.3. Dans [8], la tresse $a_{p,q}$ est définie comme étant $\sigma_{q-1} \cdots \sigma_{p+1}\, \sigma_p\, \sigma_{p+1}^{-1} \cdots \sigma_{q-1}^{-1}$, correspondant au croisement des brins p et q, **au dessus** des brins intermédiaires. Les deux définitions fournissent des monoïdes isomorphes. Notre choix est le seul autorisant le monoïde B_{n-1}^{+*} à être un segment initial de B_n^{+*} vis-à-vis de l'ordre des tresses $<$.

Pour p, q, r et s des entiers, nous disons que l'intervalle $[p, q]$ est *niché* dans l'intervalle $[r, s]$ si la relation $r < p < q < s$ est vérifiée.

Proposition 1.4 (J.S. Birman, K.H. Ko, S.J. Lee [8])**.** *Le monoïde des tresses duales* B_n^{+*} *est présenté par les générateurs* $\mathscr{A}_n$ *et les relations*

$$a_{p,q}a_{r,s} = a_{r,s}a_{p,q} \quad \textit{pour } [p,q] \textit{ et } [r,s] \textit{ disjoints ou nichés}, \tag{2.1}$$

$$a_{p,q}a_{q,r} = a_{q,r}a_{p,r} = a_{p,r}a_{p,q} \quad \textit{pour } 1 \leq p < q < r \leq n. \tag{2.2}$$

Notons que, comme pour le monoïde des tresses positives, les relations (2.1) et (2.2) préservent la longueur des $\mathscr{A}_n$-mots.

Définition 1.5. Pour tout $n \geqslant 1$, nous définissons la tresse δ_n de B_n^{+*} en posant

$$\delta_n = a_{1,2}\, a_{2,3}\, \cdots\, a_{n-1,n} = \sigma_1\, \sigma_2\, \cdots \sigma_{n-1}. \tag{2.3}$$

Nous avons déjà rencontré la tresse δ_n lors de la construction de la tresse Δ_n par récurrence sur n à la définition 1.17 du chapitre I, en effet pour tout $n \geqslant 2$ nous avons la relation $\Delta_n = \delta_n \cdot \Delta_{n-1}$.

Proposition 1.6 (J.S. Birman, K.H. Ko, S.J. Lee [8])**.** *Le monoïde* (B_n^{+*}, δ_n) *est un monoïde de Garside.*

Ainsi, tout comme le monoïde des tresses positives B_n^+, le monoïde B_n^{+*} s'injecte dans son groupe des fractions qui n'est autre que le groupe des tresses B_n. De plus le monoïde est muni d'une forme normale de Garside.

Remarquons que le nombre de générateurs de B_n^+ est $n-1$ tandis que celui de B_n^{+*} est $\binom{n}{2}$. D'autre part la longueur de l'élément de Garside Δ_n de B_n^+ est $\binom{n}{2}$ tandis que la longueur de l'élément de Garside δ_n de B_n^{+*} est $n-1$. C'est cette symétrie *nombre de générateurs / longueur élément de Garside* entre B_n^+ et B_n^{+*} qui justifie en particulier la terminologie *monoïde des tresses duales* introduite dans [4].

1.1 Forme normale tournante

La forme normale tournante est une autre forme normale définie sur le monoïde de tresses duales B_n^{+*}, introduite durant ma thèse dans [65] et [66]. Elle permet, pour chaque tresse duale β de B_n^{+*}, d'isoler un unique $\mathscr{A}_n$-mot parmi tous ceux qui représentent β. Elle peut être vue comme une application r_n du monoïde des tresses duales B_n^{+*} dans l'ensemble $\mathscr{A}_n^*$ de tous les $\mathscr{A}_n$-mots.

La construction de la forme normale tournante repose sur l'automorphisme de Garside du monoïde des tresses duales B_n^{+*}.

Définition 1.7. L'*automorphisme de Garside* de B_n^{+*} est défini par

$$\phi_n(\beta) = \delta_n \, \beta \, \delta_n^{-1}. \tag{2.4}$$

En termes des générateurs $\mathscr{A}_n$ de B_n^{+*} un calcul immédiat utilisant les relations (2.1) et (2.2) donne

$$\phi_n(a_{p,q}) = \begin{cases} a_{p+1,q+1} & \text{pour } q \leq n-1, \\ a_{1,p+1} & \text{pour } q = n. \end{cases} \tag{2.5}$$

L'application ϕ_n induit ainsi un homomorphisme de $\mathscr{A}_n$-mot. Géométriquement, ϕ_n peut être vue comme une rotation, ce qui prend tout son sens lorsque les diagrammes de tresses de B_n^{+*} sont dessinés dans un cylindre plutôt que sur un rectangle.

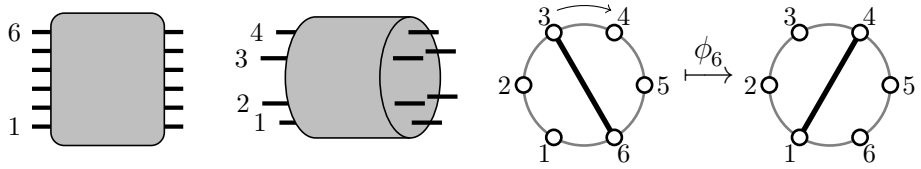


FIGURE 2.2 – Enrouler le diagramme de tresse usuel aide à visualiser les symétries des tresses $a_{p,q}$. Sur le cercle ainsi obtenu, la tresse $a_{p,q}$ correspond naturellement à la corde reliant les points p et q. Avec cette représentation, l'automorphisme ϕ_n agit comme une rotation d'angle $2\pi/n$ dans le sens des aiguilles d'une montre.

Comme pour la forme normale de Garside (voir proposition 3.4 du chapitre I), la forme normale tournante permet de décomposer une tresse en prenant successivement le plus gros diviseur satisfaisant certaines propriétés. Ici nous ne considérerons pas des diviseurs à gauche, comme pour la forme normale de Garside, mais des diviseurs à droite. Ce choix peut paraître maladroit de prime abord mais il est justifié par le lien existant entre la forme normale tournante et l'ordre des tresses établi dans [66] qui est expliqué dans l'introduction de ce chapitre. Notons que nous avons aussi une version *droite* de la forme normale de Garside en considérant des diviseurs à droite et non à gauche.

Définition 1.8. Pour $n \geqslant 3$ et $\beta \in B_n^{+*}$, la plus grande tresse β_1 de B_{n-1}^{+*} qui divise β à droite est appelée B_{n-1}^{+*}-*fin* de β.

En exploitant des propriétés élémentaires du monoïde de Garside B_n^{+*} nous obtenons le résultat suivant exprimant toute tresse de B_n^{+*} comme suite finie d'éléments de B_{n-1}^{+*}.

Proposition 1.9 (Proposition 2.5 de [67]). *Soit $n \geqslant 3$. Pour toute tresse non triviale β de B_n^{+*} il existe une unique suite $(\beta_b, \ldots, \beta_1)$ de tresses de B_{n-1}^{+*} satisfaisant $\beta_b \neq 1$ et*

$$\beta = \phi_n^{b-1}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_2) \cdot \beta_1, \tag{2.6}$$

pour tout $k \geqslant 1$, la B_{n-1}^{+*}-fin de $\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1})$ est triviale. (2.7)

Définition 1.10. La suite $(\beta_b, \ldots, \beta_1)$ introduite à la proposition 1.9 est le *ϕ_n-éclatement* de la tresse duale β de B_n^{+*}.

Comme indiqué dans [67] la condition (2.7) peut être remplacée par

$$\text{pour tout } k \geqslant 1,\ \beta_k \text{ est la } B_{n-1}^{+*}\text{-fin de } \phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1}) \cdot \beta_k. \tag{2.8}$$

Nous utiliserons indistinctement l'une ou l'autre des conditions.

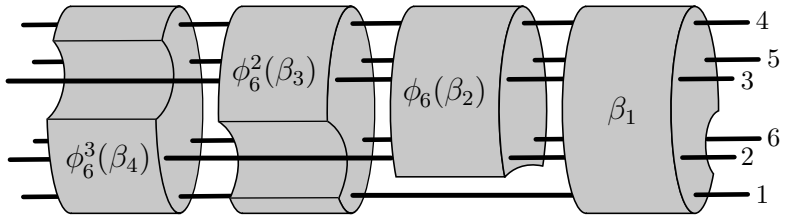


FIGURE 2.3 – Le ϕ_6-éclatement d'une tresse de B_6^{+*}. En commençant par la droite, nous extrayons le plus grand diviseur à droite laissant le sixième brin invariant, puis nous extrayons le plus grand diviseur à droite laissant le premier brin invariant et ainsi de suite.

Exemple 1.11. Considérons la tresse $\beta = \delta_3^2 = a_{1,2}a_{2,3}a_{1,2}a_{2,3}$ de B_3^{+*}. En utilisant les relations (2.2) sur le facteur souligné nous obtenons :

$$\beta = a_{1,2}a_{2,3}\underline{a_{1,2}a_{2,3}} = a_{1,2}\underline{a_{2,3}a_{1,3}}a_{1,2} = a_{1,2}a_{1,3}a_{1,2}a_{1,2}.$$

Nous décomposons alors β comme le produit $\phi_3(\gamma_1)\cdot\beta_1$ avec $\gamma_1 = \phi_3^{-1}(a_{1,2}a_{1,3}) = a_{1,3}a_{2,3}$ et $\beta_1 = a_{1,2}a_{1,2}$. Comme le mot $a_{1,2}a_{1,3}$ est seul dans sa classe d'équivalence, la tresse $\phi_3(\gamma_1) = a_{1,2}a_{1,3}$ n'est pas divisible à droite par $a_{1,2}$ et donc sa B_2^{+*}-fin est triviale. La tresse $\phi_3(\gamma_1)$ est exactement celle de (2.7) pour $n = 3$ et $k = 1$. Considérant γ_1 à la place de β nous obtenons $\gamma_1 = \phi_3(\gamma_2)\cdot\beta_2$ avec $\gamma_2 = \phi_3^{-1}(a_{1,3}a_{2,3}) = a_{2,3}a_{1,2}$ et $\beta_2 = 1$. Comme le mot $a_{1,3}a_{2,3}$ est seul dans sa classe d'équivalence, la tresse $\phi_3(\gamma_2) = a_{1,3}a_{2,3}$ n'est pas divisible à droite par $a_{1,2}$ et donc sa B_2^{+*}-fin est triviale. La tresse $\phi_3(\gamma_2)$ est celle de (2.7) pour $n = 3$ et $k = 2$. Nous décomposons maintenant la tresse γ_2 en $\phi_3(\gamma_3)\cdot\beta_3$ avec $\gamma_3 = \phi_3^{-1}(a_{2,3}) = a_{1,2}$ et $\beta_3 = a_{1,2}$. Comme la tresse $\phi_3(\gamma_3) = a_{2,3}$ n'est pas divisible à droite par $a_{1,2}$, sa B_2^{+*}-fin est triviale. La tresse $\phi_3(\gamma_3)$ est celle de (2.7) pour $n = 3$ et $k = 3$. Finalement, nous avons $\gamma_3 = \phi_3(\gamma_4)\cdot\beta_4$ avec $\gamma_4 = 1$ et $\beta_4 = a_{1,2}$. La tresse restante γ_4 étant triviale, nous obtenons que le ϕ_3-éclatement de β est $(\beta_4, \beta_3, \beta_2, \beta_1) = (a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$.

La *n-forme normale tournante* est une application injective r_n de B_n^{+*} dans l'ensemble $\mathscr{A}_n^*$ des $\mathscr{A}_n$-mots. Elle est définie par induction sur $n \geqslant 2$ en utilisant le ϕ_n-éclatement.

Définition 1.12. La *2-forme normale tournante* $r_2(\beta)$ d'une tresse $\beta \in B_2^{+*}$ est définie comme étant l'unique $\mathscr{A}_2$-mot $a_{1,2}^k$ représentant β. La *n-forme normale tournante* d'une tresse $\beta \in B_n^{+*}$ avec $n \geqslant 3$ est :

$$r_n(\beta) = \phi_n^{b-1}(r_{n-1}(\beta_b)) \cdot \ldots \cdot \phi_n(r_{n-1}(\beta_2)) \cdot r_{n-1}(\beta_1),$$

où $(\beta_b, \dots, \beta_1)$ est le ϕ_n-éclatement de β. Pour tout $n \geqslant 2$, un $\mathscr{A}_n$-mot est dit *n-tournant* s'il est la forme normale tournante d'une tresse de B_n^{+*}.

Comme la n-forme normale tournante d'une tresse de B_{n-1}^{+*} est égale à sa $(n-1)$-forme normale tournante, nous pouvons parler, sans ambiguïté, de la *forme normale tournante* d'une tresse duale. De même nous dirons que le mot est *tournant* s'il est n-tournant pour un certain $n \geqslant 2$.

Exemple 1.13. Reprenons la tresse $\beta = \delta_3^2$ de l'exemple 1.11. Nous savons que le ϕ_3-éclatement de β est $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$. De $r_2(1) = \varepsilon$, $r_2(a_{1,2}) = a_{1,2}$ et $r_2(a_{1,2}^2) = a_{1,2}^2$, nous obtenons :

$$r_3(\beta) = \phi_3^3(a_{1,2}) \cdot \phi_3^2(a_{1,2}) \cdot \phi_3(\varepsilon) \cdot a_{1,2}^2 = a_{1,2}a_{1,3}a_{1,2}a_{1,2}.$$

Ainsi la forme normale tournante de la tresse δ_3^2 est le $\mathscr{A}_3$-mot $a_{1,2}a_{1,3}a_{1,2}a_{1,2}$.

2 Caractérisation

Le but de cette section est d'établir des critères syntaxiques simples afin de détecter si un $\mathscr{A}_n$-mot donné est n-tournant ou non. Une première difficulté réside dans le fait que la forme tournante d'une tresse est obtenue à partir de son éclatement. Or, par la proposition 1.9, un éclatement est construit à partir de diviseurs maximaux qui semblent assez éloignés des critères syntaxiques simples que nous recherchons. Une étape clé consiste à remplacer la condition 2.8 faisant intervenir le terme k puis les termes $k+1$ jusque b d'un ϕ_n-éclatement par une version plus locale faisant intervenir seulement les termes k et $k+1$.

Les critères que nous obtiendrons utiliseront la notion de *barrières* que nous introduisons maintenant.

Définition 2.1. Pour $n \geqslant 3$ et p, r, s des entiers de $[1, n-1]$, nous disons que la lettre $a_{r,s}$ est une *$a_{p,n}$-barrière* si la relation $r < p < s$ est satisfaite.

Il n'existe pas de $a_{p,n}$-barrière pour $n \leqslant 3$ et la seule $a_{p,4}$-barrière est $a_{1,3}$, qui est une $a_{2,4}$-barrière. Par définition, si la lettre x est une $a_{p,n}$-barrière alors la présentation de B_n^{+*} donnée à la proposition 1.4 ne contient pas de relation de la forme $a_{p,n} \cdot x = y \cdot a_{p,n}$ permettant de pousser la lettre $a_{p,n}$ à droite de la lettre x : la lettre x agit donc en quelque sorte comme une barrière empêchant la migration de $a_{p,n}$ plus à droite.

À l'aide de la notion de barrière nous pouvons énoncer la caractérisation syntaxique suivante des mots n-tournants.

Théorème 2.2. *Pour $n \geqslant 3$, un $\mathscr{A}_n$-mot w est n-tournant si et seulement s'il existe une suite $(w_b, \dots, w_1)$ de $\mathscr{A}_{n-1}$-mots vérifiant*

$$w = \phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1, \tag{2.9}$$

ainsi que les conditions suivantes :

(i) pour $k \geqslant 1$, le mot w_k est $(n-1)$-tournant,

(ii) pour $k \geqslant 3$, le mot w_k est non vide et se termine par $a_{..,n-1}$,

(iii) le mot w_2 est soit vide (sauf pour $b = 2$) soit se termine par $a_{..,n-1}$,

(*iv*) *si, pour* $k \geqslant 3$*, le mot* w_k *se termine par* $a_{p-1,n-1}$ *avec* $p \neq n-1$ *alors le mot* w_{k-1} *contient une* $a_{p,n}$*-barrière.*

L'écriture (2.9) et la condition (*i*) découlent naturellement de la construction inductive de la forme normale tournante. La condition (*ii*) porte uniquement sur le deuxième terme de l'éclatement tandis que la condition (*iii*) ne fait intervenir qu'un seul de ces termes pour chaque valeur de k. La condition (*iv*) est une version *locale* de la condition (2.8).

Le reste de cette section est consacré à la démonstration du théorème 2.2 et n'est pas nécessaire à la compréhension de la suite de ce chapitre.

2.1 Dernière lettre

Comme nous le constatons aux conditions (*ii*) à (*iv*) du théorème 2.2 les dernières lettres des mots $(n-1)$-tournants w_k jouent un rôle majeur.

Définition 2.3. Pour tout $\mathscr{A}_n$ mot non vide w, nous notons $w^{\#}$ la dernière lettre de w. Pour toute tresse β non triviale de B_n^{+*} avec $n \geqslant 2$, nous définissons la *dernière lettre* de la tresse β, notée $\beta^{\#}$, comme étant la dernière lettre de sa forme normale tournante.

Le résultat suivant montre que les conditions (*ii*) et (*iii*) du théorème 2.2 sont nécessaires.

Lemme 2.4 (Lemme 3.2 de [67])**.** *Soit* $n \geqslant 3$ *et* $(\beta_b, \ldots, \beta_1)$ *le* ϕ_n*-éclatement d'une tresse duale de* B_n^{+*}*.*

(*i*) *Pour* $k \geqslant 2$*, la lettre* $\beta_k^{\#}$ *est de la forme* $a_{\cdot\cdot,n-1}$ *excepté pour* $\beta_k = 1$*.*

(*ii*) *Pour* $k \geqslant 3$ *ou pour* $k = b$*, nous avons* $\beta_k \neq 1$*.*

En fait nous avons le résultat plus général suivant qui caractérise les tresses duales ayant une B_{n-1}^{+*}-fin triviale.

Lemme 2.5. *Pour* $n \geqslant 3$*, une tresse non triviale* $\beta \in B_n^{+*}$ *admet une* B_{n-1}^{+*}*-fin triviale si et seulement s'il existe une unique lettre dans* $\mathscr{A}_n$ *qui divise* β *à droite ; cette lettre est nécessairement de la forme* $a_{\cdot\cdot,n}$*.*

Démonstration. Si $a_{p,n}$ est la seule lettre qui divise β à droite, alors la B_{n-1}^{+*}-fin de β est nécessairement triviale. Réciproquement, supposons que la B_{n-1}^{+*}-fin de β soit triviale. Aucune lettre $a_{p,q}$ avec $q \leqslant n-1$ ne peut ainsi être diviseur à droite de β. Supposons par l'absurde que deux lettres distinctes $a_{p,n}$ et $a_{q,n}$ vérifiant $p < q < n$ divise β à droite. La tresse β serait alors divisible à droite par leur plus petit multiple commun à gauche

$$a_{p,n} \vee_g a_{q,n} = a_{p,q}a_{q,n} = a_{q,n}a_{p,n} = a_{p,n}a_{p,q},$$

et donc par $a_{p,q}$, ce qui est impossible car la B_{n-1}^{+*}-fin de β est supposée triviale. □

2.2 Barrières et échelles

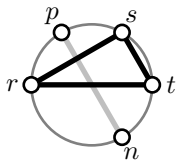
La condition (*iv*) du théorème 2.2 impose l'existence d'une barrière dans la tresse β_k d'un ϕ_n-éclatement si la dernière lettre de β_{k+1} satisfait certaines conditions. Nous commençons par un résultat indiquant que le fait de contenir une barrière n'est pas une propriété d'un $\mathscr{A}_n$-mot mais une propriété de la tresse elle-même.

Lemme 2.6. *Soit* $n \geqslant 3$*. Pour toute tresse* β *de* B_n^{+*}*, il y a équivalence entre*

(*i*) *un* $\mathscr{A}_n$*-mot représentant* β *contient une* $a_{p,n}$*-barrière,*

(*ii*) *tout $\mathscr{A}_n$-mot représentant β contient une $a_{p,n}$-barrière.*

Démonstration. La relation (*ii*) $\Rightarrow$ (*i*) étant évidente montrons (*i*) $\Rightarrow$ (*ii*). Pour cela il est suffisant d'établir que les relations de la proposition 1.4 préservent les $a_{p,n}$-barrières. Pour la relation de commutation 2.1 c'est immédiat car elle préserve les lettres dans leurs ensembles. Pour la relation 2.2, nous avons que si l'un des mots $a_{r,s}a_{s,t}$, $a_{s,t}a_{r,t}$ et $a_{r,t}a_{r,s}$ contient une $a_{p,n}$-barrière alors les deux autres aussi, comme illustré par le de diagramme de cordes suivant.



En effet, une lettre $a_{r,s}$ est une $a_{p,n}$-barrière si et seulement si la corde associée à $a_{r,s}$ intersecte proprement celle de $a_{p,n}$. □

Supposons que $(\beta_b, \dots, \beta_1)$ soit le ϕ_n-éclatement d'une tresse de B_n^{+*}. Soit k un entier vérifiant $1 \leqslant k \leqslant b-2$. Posons $a_{p-1,n-1} = \beta_{k-2}^{\#}$. La condition (2.7) implique alors que la B_{n-1}^{+*}-fin de $\phi_n^2(a_{p-1,n-1}) \cdot \phi_n(\beta_{k+1}) = \phi_n(a_{p,n}\beta_{k+1})$ est triviale.

Lemme 2.7 (Lemme 3.4 de [67])**.** *Supposons $n \geqslant 4$. Soit p un entier de $[2, n-2]$ et soit β une tresse de B_{n-1}^{+*} telle que la B_{n-1}^{+*}-fin de $\phi_n(a_{p,n}\beta)$ soit triviale. Alors la forme normale tournante de β est non vide et contient une $a_{p,n}$-barrière.*

Si nous retournons dans le contexte d'un ϕ_n-éclatement le lemme précédent devient.

Corollaire 2.8. *Supposons $n \geqslant 3$ et soit $(\beta_b, \dots, \beta_1)$ le ϕ_n-éclatement d'une tresse de B_n^{+*}. Alors, pour tout $k \in [2, b-1]$ tel que $\beta_{k+1}^{\#}$ n'est pas $a_{n-2,n-1}$ (si β_{k+1} est non vide), la forme normale tournante de β_k contient une $\phi_n(\beta_{k+1}^{\#})$-barrière.*

Nous pouvons faire mieux. La forme normale tournante d'un terme d'un ϕ_n-éclatement doit non seulement contenir une barrière mais former ce qu'on appelle une *échelle*, qui peut être vue comme une suite de barrières se bloquant successivement.

Définition 2.9. Pour $n \geqslant 3$ et $p, q \in [2, n-1]$, nous disons qu'un mot n-tournant w est une *$a_{p,n}$-échelle* s'il existe une décomposition

$$w = v_0\, x_1\, v_1 \cdots v_{h-1}\, x_h\, v_h,$$

une suite strictement croissante $j(0), \dots, j(h)$ avec $j(0) = p$ et $j(h) = n-1$, et une suite $i(1), \dots, i(h)$ telles que :

(*i*) pour tout $k \leqslant h$, la lettre x_k est $a_{i(k),j(k)}$ avec $i(k) < j(k-1) < j(k)$,

(*ii*) pour tout $k < h$, le mot v_k ne contient pas de $a_{j(k),n}$-barrière,

La condition (*i*) de la définition 2.9 est équivalente à dire que la lettre x_k est une $a_{j(k-1),n}$-barrière de la forme $a_{\cdot\cdot,j(k)}$.

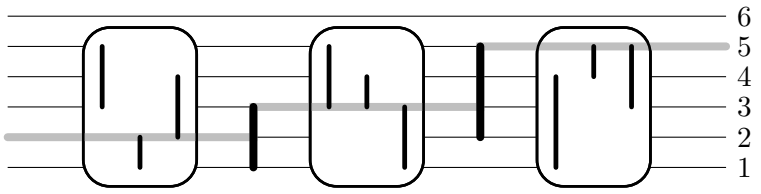


FIGURE 2.4 – Une $a_{2,6}$-échelle. La ligne grise commence à la position 2 et grimpe à la position 5 en utilisant les barreaux de l'échelle (traits verticaux noir un peu plus épais) correspondant aux lettres x_t de la définition 2.9. Les espaces entre les barreaux de l'échelle sont représentés par des boîtes rectangulaires correspondant aux mots v_t. Dans une telle boîte les lignes verticales représentent des lettres $a_{i,j}$ qui ne traversent pas la ligne grise.

Pour établir, sous certaines conditions, que la forme normale tournante d'un terme d'un ϕ_n-éclatement soit une échelle nous aurons besoin du lemme suivant.

Lemme 2.10 (Lemme 3.8 de [67])**.** *Supposons $n \geqslant 4$ et que w soit le suffixe d'un $(n-1)$-mot tournant. S'il existe $a_{p,q}$ dans $\mathscr{A}_{n-2}$ telle que la B^{+*}_{n-1}-fin de $\phi_n(a_{p,q}\overline{w})$ soit trivial alors le mot w contient une $a_{q,n}$-barrière.*

En appliquant successivement le lemme précédent nous obtenons.

Lemme 2.11. *Supposons $n \geqslant 4$ et soit p un entier de $[2, n-2]$. Soit β une tresse de B^{+*}_{n-1} telle que la B^{+*}_{n-1}-fin de $\phi_n(\beta)$ soit triviale et telle que β contienne une $a_{p,n}$-barrière. Alors la forme normale tournante de β est une $a_{p,n}$-échelle.*

La démonstration du lemme précédent est exactement la même que celle de la proposition 3.9 de [67] mais comme les deux énoncés sont légèrement différents et que les notations le sont aussi je préfère la redonner.

Démonstration. Posons $j(0) = p$ et notons w la forme normale tournante de β. Par hypothèse nous pouvons écrire $w = v_0 x_1 w_0$, où v_0 est le préfixe maximal de w ne contenant pas de $a_{p,n}$-barrière et $x_1 = a_{\cdot\cdot,j}(1)$ est une $a_{j(0),n}$-barrière. Comme, toujours par hypothèse, la B^{+*}_{n-1}-fin de $\phi_n(\beta)$ est triviale, il en est de même pour la B^{+*}_{n-1}-fin de $\phi_n(x_1\overline{w_0})$. Supposons $j(1) \neq n-1$. Le lemme 2.10 implique alors que le mot w_0 peut être décomposé en $v_1\, x_2\, w_1$, où v_1 est le préfixe maximal de w_0 ne contenant pas de $a_{j(1),n}$-barrière et où x_2 est une $a_{j(1),n}$-barrière. Nous répétons le même argument jusqu'à obtenir

$$w = v_0\, x_1\, w_1 \cdots x_h w_{h-1},$$

avec $j(h) = n-1$. En posant $v_h = w_{h-1}$ nous obtenons une écriture de w satisfaisant toutes les conditions de la définition 2.9 d'une $a_{p,n}$-échelle. □

Soit $(\beta_b, \ldots, \beta_1)$ un ϕ_n-éclatement. La condition (2.7) implique, que pour tout $k \geqslant 2$, la B^{+*}_{n-1}-fin de $\phi_n(\beta_k)$ est nécessairement triviale et donc, par le corollaire 2.8 et le lemme 2.11, la forme normale tournante de β_k est une échelle si la dernière lettre de β_{k+1} est différente de $a_{n-2,n-1}$. Plus précisément nous avons le résultat suivant.

Corollaire 2.12. *Supposons $n \geqslant 3$ et soit $(\beta_b, \ldots, \beta_1)$ le ϕ_n-éclatement d'une tresse de B^{+*}_n. Alors, pour tout $k \in [2, b-1]$ tel que $\beta^{\#}_{k+1}$ n'est pas $a_{n-2,n-1}$ (si β_{k+1} est non vide), la forme normale tournante de β_k est une $\phi_n(\beta^{\#}_{k+1})$-échelle.*

2.3 Retournement à gauche

Le *retournement à gauche* a été introduit par P. Dehornoy dans [28]. Il est défini pour tout monoïde M muni d'une présentation adaptée. Lorsque le monoïde M admet de *bonnes propriétés* (satisfaites par un monoïde de Garside), le retournement à gauche fournit un cadre théorique et algorithmique pour étudier la divisibilité à droite. Bien entendu il existe une version *retournement à droite* pour l'étude de la divisibilité à gauche.

Définition 2.13. La présentation $\langle \mathscr{S} \,|\, R\rangle^+$ est *complémentée à gauche* s'il existe une application $f : \mathscr{S} \times \mathscr{S} \to \mathscr{S}^*$ satisfaisant :

$$R = \big\{ f(x,y)x = f(y,x)y \,|\, (x,y) \in \mathscr{S}^2,\ x \neq y \big\}$$

avec $f(x,x) = \varepsilon$ pour tout $x \in \mathscr{S}$.

Le monoïde B_3^{+*} avec sa présentation donnée à la proposition 1.4 est complémenté à gauche pour l'application f donnée par

$$\begin{aligned} f(a_{1,2}, a_{2,3}) &= f(a_{1,2}, a_{1,3}) = a_{1,3}, \\ f(a_{2,3}, a_{1,2}) &= f(a_{2,3}, a_{1,3}) = a_{1,2}, \\ f(a_{1,3}, a_{1,2}) &= f(a_{1,3}, a_{2,3}) = a_{2,3}. \end{aligned}$$

Cependant le monoïde B_4^{+*} avec sa présentation donnée à la proposition 1.4 n'est pas complémenté à gauche. En effet, il n'existe aucune relation du type $\cdots a_{1,3} = \cdots a_{2,4}$. Il en suit que les mots $f(a_{1,3}, a_{2,4})$ et $f(a_{2,4}, a_{1,3})$ ne sont pas bien définis. De manière générale pour $1 \leqslant p < r < q < s \leqslant n$, les mots $f(a_{p,q}, a_{r,s})$ et $f(a_{r,s}, a_{p,q})$ ne peuvent directement être obtenus de la présentation de B_n^{+*} donnée à la proposition 1.4.

Pour obtenir une présentation complémentée à gauche de B_n^{+*} nous devons ajouter de nouvelles relations. Nous pouvons, par exemple, ajouter la relation

$$a_{2,3}a_{1,4}\, a_{1,3} = a_{3,4}a_{1,2}\, a_{2,4}$$

qui est vérifiée dans B_4^{+*} et ainsi choisir de poser $f(a_{1,3}, a_{2,4}) = a_{2,3}a_{1,4}$. Cependant, la relation $a_{1,4}a_{2,3}\, a_{1,3} = a_{3,4}a_{1,2}\, a_{2,4}$ est aussi satisfaite dans B_4^{+*} et donc $f(a_{1,3}, a_{2,4}) = a_{1,4}a_{2,3}$ est un autre choix valide.

Lemme 2.14. *Pour $n \geqslant 2$, l'application $f_n : \mathscr{A}_n \times \mathscr{A}_n \to \mathscr{A}_n^*$ définie par :*

$$f_n(a_{p,q}, a_{r,s}) = \begin{cases} \varepsilon & \text{pour } a_{p,q} = a_{r,s}, \\ a_{p,s} & \text{pour } q = r, \\ a_{s,q} & \text{pour } p = r \text{ et } q > s, \\ a_{r,p} & \text{pour } q = s \text{ et } p > r, \\ a_{r,q}a_{p,s} & \text{pour } p < r < q < s, \\ a_{s,q}a_{r,p} & \text{pour } r < p < s < q, \\ a_{r,s} & \text{sinon.} \end{cases}$$

fournit à B_n^{+*} une présentation complémentée à gauche.

Démonstration. Un calcul direct utilisant la proposition 1.4 établit l'équivalence de mots $f_n(x,y) \cdot x \equiv f_n(y,x) \cdot y$ pour tout $(x,y) \in \mathscr{A}_n^2$. □

Supposons $n \geqslant 2$. Comme mentionné précédemment, la caractérisation de l'application f_n à partir de la présentation de B_n^{+*} n'est pas unique : plusieurs choix sont possibles. Le choix que nous avons fait pour f_n admet la propriété suivante : pour toutes lettres $a_{p,q}$ et $a_{r,s}$ de $\mathscr{A}_n$, la dernière lettre du mot $f_n(a_{p,q}, a_{r,s})$ est de la forme $a_{\dots,s}$ pour $q < s$. Cette propriété nous sera utile dans la suite, par exemple lors de la démonstration du lemme 2.20.

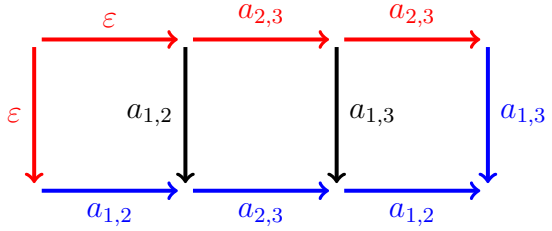
Définition 2.15. Soit $n \geqslant 2$. Pour w et w' deux $\mathscr{A}_n^{\pm}$-mots, nous disons que w se *retourne à gauche en une étape* en w', noté $w \curvearrowright^1 w'$, si nous pouvons obtenir w' de w en substituant un facteur xy^{-1} de w (avec $x, y \in \mathscr{A}_n$) par $f_n(x,y)^{-1} f_n(y,x)$. Nous disons que w se *retourne à gauche* en w', noté $w \curvearrowright w'$, s'il existe une suite finie $(w_1, \dots, w_\ell)$ de $\mathscr{A}_n^{\pm}$-mots satisfaisant $w_1 = w$, $w_\ell = w'$ et $w_k \curvearrowright^1 w_{k+1}$ pour $k \in [1, \ell - 1]$.

Le retournement à gauche est facilement décrit à l'aide d'un diagramme de flèches étiquetées. Supposons que $(w_1, \dots, w_\ell)$ soit une suite de retournements à gauche. Au mot w_1 nous associons un chemin étiqueté par ses lettres successives : à une lettre positive x nous associons une flèche horizontale dirigée vers la droite et étiquetée x, à une lettre négative x^{-1} nous associons une flèche verticale dirigée vers le bas et étiquetée y. Nous représentons alors successivement les mots $w_2, \dots, w_\ell$ de la manière suivante : si w_{k+1} est obtenu de w_k en remplaçant le facteur $x\,y^{-1}$ de w_k par $f_n(x,y)^{-1}\, f_n(y,x)$ alors nous complétons le motif correspondant à $x\,y^{-1}$ en ajoutant une flèche verticale étiquetée $f_n(x,y)$ et une flèche horizontale étiquetée $f_n(y,x)$ afin d'obtenir un carré :

Exemple 2.16. Le mot $u = a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1}$ se retourne à gauche en $a_{2,3}a_{2,3}$ comme en témoigne la suite suivante de retournements à gauche en une étape (nous soulignons le facteur retourné)

$$a_{1,2}a_{2,3}\underline{a_{1,2}a_{1,3}^{-1}} \curvearrowright^1 a_{1,2}\underline{a_{2,3}a_{1,3}^{-1}}a_{2,3} \curvearrowright^1 \underline{a_{1,2}a_{1,2}^{-1}}a_{2,3}a_{2,3} \curvearrowright^1 a_{2,3}a_{2,3},$$

ce qui est noté $a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1} \curvearrowright a_{2,3}a_{2,3}$. Cette suite de retournements est aussi donnée par le diagramme



illustrant que le mot $a_{1,2}a_{1,2}a_{1,2}a_{1,3}^{-1}$ se retourne à gauche en $a_{2,3}a_{2,3}$.

À partir du lemme 1.1 de [28] nous obtenons les définitions suivantes de dénominateur et numérateur à gauche d'un $\mathscr{A}_n^{\pm}$-mot.

Définition 2.17. Supposons $n \geqslant 2$. Pour un $\mathscr{A}_n^{\pm}$-mot w, nous notons $D(w)$ et $N(w)$ les $\mathscr{A}_n$-mots tels qu'on ait $w \curvearrowright D(w)^{-1} N(w)$, s'ils existent. Si de tels mots existent ils sont uniques et les notations $D(w)$ et $N(w)$ sont sans ambiguïté. Le mot $N(w)$ est le *numérateur à gauche* de w tandis que le mot $D(w)$ est son *dénominateur à gauche*.

En reconsidérant l'exemple 2.16, nous obtenons que le dénominateur à gauche de u est $D(u) = \varepsilon$ et que son numérateur à gauche est $N(u) = a_{2,3}a_{2,3}$.

Supposons $n \geqslant 2$. Comme B_n^{+*} est un monoïde de Garside et que l'application f_n est un *sélecteur de multiple commun à gauche*, le lemme 4.3 de [39] implique que pour tout mot w de $\mathscr{A}_n^{\pm}$, les mots $N(w)$ et $D(w)$ existent. Une adaptation de la proposition 3.4 de [39] au contexte du monoïde des tresses duales donne :

Proposition 2.18 (Proposition 3.4 de [39])**.** *Supposons $n \geqslant 2$. Pour un $\mathscr{A}_n$-mot w et une lettre $a_{p,q}$ de $\mathscr{A}_n$, la tresse $\overline{w}$ est divisible à droite par $a_{p,q}$ si et seulement si $D(w\, a_{p,q}^{-1})$ est vide.*

Comme le dénominateur à gauche du mot $u = a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1}$ de l'exemple 2.16 est vide, nous avons que la tresse $a_{1,3}$ divise à droite la tresse $\overline{a_{1,2}a_{2,3}a_{1,2}}$.

2.4 Conditions équivalentes

Nous avons vu au lemme 2.7 que sous certaines conditions une tresse de B_{n-1}^{+*} devait contenir une $a_{p,n}$-barrière. Le résultat suivant montre que nous avons en fait une équivalence.

Proposition 2.19. *Soit $n \geqslant 4$. Pour $\beta \in B_{n-1}^{+*}$ et $p \in [2, n-2]$ il y a équivalence entre :*

(i) la B_{n-1}^{+*}-fin de $\phi_n(a_{p,n}\beta)$ est triviale ;

(ii) la B_{n-1}^{+*}-fin de $\phi_n(\beta)$ est triviale et β contient une $a_{p,n}$-barrière.

La démonstration de la proposition 2.19 utilise le lemme suivant :

Lemme 2.20. *Supposons $n \geqslant 3$ et soient u un $\mathscr{A}_{n-1}$-mot et p un entier de $[1, n-1]$. Alors le dénominateur à gauche de $D(ua_{p,n}^{-1})$ est non vide. Plus précisément, il existe un entier q de l'intervalle $[1, p]$ tel que $D(ua_{p,n}^{-1})^{-1}$ commence par la lettre $a_{q,n}^{-1}$.*

Démonstration. Supposons que $w_1, \ldots, w_\ell$ soit une suite de retournements à gauche du mot $w_1 = ua_{p,n}^{-1}$ en le mot $D(w_1)^{-1}N(w_1)$. Pour $k \in [1, \ell]$ nous notons y_k^{-1} le lettre négative la plus à gauche dans w_k, si une telle lettre existe. Montrons par induction sur $k \in [1, \ell]$ l'existence de la lettre y_k et d'une suite décroissante $r(k)$ telle qu'on ait $y_k = a_{r(k),n}$.

Par construction, nous avons $r(1) = p$ et $y_1 = a_{r(1),n}$. Chaque étape élémentaire de retournement à gauche consiste à remplacer un facteur xy^{-1} de w_k par $f_n(x, y)^{-1}f_n(y, x)$. Si, pour $k \in [1, \ell-1]$, le facteur à retourner de w_k, ne contient pas la lettre négative la plus à gauche de w_k, nous avons $y_{k+1} = y_k$ et donc $r(k+1) = r(k)$. Supposons maintenant que le facteur à retourner xy^{-1} contienne la lettre négative la plus à gauche de w_k. Nous avons alors $y = y_k = a_{r(k),n}$. Comme toutes les lettres de w_k à gauche du facteur xy^{-1} sont positives et appartiennent à $\mathscr{A}_{n-1}$, la lettre $x = a_{i,j}$ vérifie $1 \leqslant i < j < n$. Par le lemme 2.14 nous obtenons

$$f_n(x, y_k) = f_n(a_{i,j}, a_{r(k),n}) = \begin{cases} a_{i,n} & \text{pour } j = r(k), \\ a_{r(k),j}a_{i,n} & \text{pour } i < r(k) < j, \\ a_{r(k),n} & \text{sinon,} \end{cases}$$

ce qui donne en particulier

$$xy_k^{-1} = a_{i,j}a_{r(k),n}^{-1} \curvearrowright \begin{cases} a_{i,n}^{-1}\cdots & \text{pour } i < r(k) \leqslant j, \\ a_{r(k),n}^{-1}\cdots & \text{sinon.} \end{cases} \tag{2.10}$$

La lettre $y_{k+1} = a_{r(k+1),n}$ vaut donc $a_{i,n}$ avec $i < r(k)$ ou $a_{r(k),n}$. La relation $r(k+1) \leqslant r(k)$ est ainsi vérifiée. Finalement nous obtenons que $ua_{p,n}^{-1}$ se retourne à gauche en $a_{r(\ell),n}^{-1}\cdots$. Le mot $D(ua_{p,n})^{-1}$ commence donc par la lettre $a_{r(\ell),n}^{-1}$ où $r(\ell)$ vérifie la relation $r(\ell) \leqslant r(1) = p$. □

Démonstration de la proposition 2.19. Supposons (i). Comme la B_{n-1}^{+*}-fin de $\phi_n(\beta)$ est un diviseur à droite de la tresse $\phi_n(a_{p,n}\,\beta)$, la première partie de (ii) est vérifiée. La seconde est le lemme 2.7.

Montrons maintenant $(ii) \Rightarrow (i)$. Par le lemme 2.5 et la condition (ii), il existe une unique lettre de $\mathscr{A}_n$ qui divise $\phi_n(\beta)$ à droite et elle est de la forme $a_{\cdot,n}$. La dernière lettre $\beta^{\#}$ de β est donc de la forme $a_{\cdot,n-1}$. Notons w la forme normale tournante de β. Soit $a_{r,s}$ une lettre de $\mathscr{A}_n$ différente de $\beta^{\#}$. Par le lemme 2.5 il est suffisant de montrer que $a_{r,s}$ n'est pas un diviseur à droite de $a_{p,n}\,\beta$ pour obtenir le (i). Ceci, par la proposition 2.18, est équivalent à montrer que le dénominateur $D(a_{p,n}\,w\,a_{r,s}^{-1})$ est vide.

Cas $s \leqslant n-1$. Alors la lettre $a_{r,s}$ appartient à $\mathscr{A}_{n-1}$. Comme β est une tresse de B_{n-1}^{+*}, le lemme 2.5 garantit que $a_{r,s}$ ne peut pas être un diviseur de β. Ainsi, par la proposition 2.18, le mot $D(w\,a_{r,s}^{-1})$ doit être non vide. Comme le retournement à gauche d'un $\mathscr{A}_{n-1}^{\pm}$-mot est encore un $\mathscr{A}_{n-1}^{\pm}$-mot, il existe une lettre $a_{t,t'}$ vérifiant $t' < n$ tel que nous ayons :

$$a_{p,n}\,w\,a_{r,s}^{-1} \curvearrowright a_{p,n}\,a_{t,t'}^{-1}\cdots .$$

La tresse $a_{t,t'}$ n'est pas un diviseur à droite de $a_{p,n}$ (car $t' < n$). Donc, par la proposition 2.18, le dénominateur à gauche de $a_{p,n}\,w\,a_{r,s}^{-1}$ est non vide, et nous concluons que $a_{r,s}$ n'est pas un diviseur à droite de $a_{p,n}\beta$.

Cas $s = n$. Les hypothèses faites sur β et le lemme 2.11 impliquent que w est une $a_{p,n}$-échelle. En suivant la définition 2.9, nous posons

$$w = v_0\,x_1\,v_1\,\cdots\,v_{h-1}\,x_h\,v_h.$$

Par le lemme 2.20, il existe deux applications η et μ de $\mathbb{N}$ dans lui-même tel qu'on ait

$$wa_{r,n}^{-1} = w_h a_{\eta(h),n}^{-1} \curvearrowright w'_h a_{\mu(h),n}^{-1}\cdots \curvearrowright \ldots \curvearrowright w_0 a_{\eta(0),n}^{-1}\cdots \curvearrowright w'_0 a_{\mu(0),n}^{-1}\cdots ,$$

où pour tout $k \in [0,h]$, on a

$$\begin{aligned} w_k &= v_0\,x_1\,v_1\,\cdots\,v_{k-1}\,x_k\,v_k, \\ w'_k &= v_0\,x_1\,v_1\,\cdots\,v_{k-1}\,x_k. \end{aligned}$$

Par construction w_0 est égal à v_0 tandis que w'_0 est le mot vide et $\eta(h)$ vaut r. Pour $k \in [0,h]$, le lemme 2.20 avec $u = v_k$ et $p = \eta(k)$ implique que le mot

$$w_k\,a_{\eta(k),n}^{-1}\cdots = w'_k\,v_k\,a_{\eta(k),n}^{-1}\cdots$$

se retourne à gauche en $w'_k\,a_{\mu(k),n}^{-1}\cdots$ avec $\mu(k) \leqslant \eta(k)$. Alors, pour $k \neq 0$, le lemme 2.20 (avec $u = v_{k-1}$ et $p = \mu(k)$) implique que le mot

$$w'_k\,a_{\mu(k),n}^{-1}\cdots = w_{k-1}\,x_k\,a_{\mu(k),n}^{-1}\cdots$$

se retourne à gauche en $w_{k-1}\,a_{\eta(k-1),n}^{-1}\cdots$ avec $\eta(k-1) \leqslant \mu(k)$. En utilisant une induction sur $k = h,\ldots,0$ nous obtenons :

$$\mu(0) \leqslant \eta(0) \leqslant \mu(1) \leqslant \ldots \leqslant \mu(h) \leqslant \eta(h) = r. \tag{2.11}$$

En suivant la définition 2.9 on pose $x_k = a_{i(k),j(k)}$. Montrons que pour tout $k \in [0,h-1]$ nous avons

$$\mu(k+1) \leqslant j(k+1) \Rightarrow \eta(k) < j(k). \tag{2.12}$$

Soit $k \in [0, h-1]$ et supposons $\mu(k+1) \leqslant j(k+1)$. Par définition d'une échelle nous avons $i(k+1) < j(k) < j(k+1)$. Dans le cas $\mu(k+1) \leqslant i(k+1)$ nous obtenons alors :

$$\eta(k) \leqslant \mu(k+1) \leqslant i(k+1) < j(k),$$

et nous avons fini. Le cas restant est $\mu(k+1) > i(k+1)$. Grâce à la relation (2.10), avec $i = i(k+1)$, $j = j(k+1)$ et $r = \mu(k+1)$ (qui satisfont $i < r \leqslant j$) nous obtenons

$$x_{k+1}\, a^{-1}_{\mu(k+1),n} = a_{i(k+1),j(k+1)}\, a^{-1}_{\mu(k+1),n} \curvearrowright a^{-1}_{i(k+1),n} v,$$

pour un certain $\mathscr{A}_n^{\pm}$-mot v. En particulier, nous avons $\eta(k) = i(k+1) < j(k)$ et la relation (2.12) est établie.

Pour $k = h-1$ le membre gauche de (2.12) est satisfait car $j(h)$ vaut $n-1$ et

$$\mu(h) \leqslant \eta(h) = r \leqslant n-1$$

est vérifiée par définition de r. Les propriétés (2.11) et (2.12) impliquent $\mu(k) < j(k)$ pour tout k appartenant à $[0, h-2]$. En particulier nous avons $\mu(0) < j(0) = p$ ainsi que $w a^{-1}_{r,n} \curvearrowright a^{-1}_{\mu(0),n} \cdots$. Comme $a_{\mu(0),n}$ ne peut pas être un diviseur à droite de $a_{p,n}$, nous obtenons que le dénominateur à gauche du mot $a_{p,n}\, w\, a^{-1}_{r,n}$ est aussi non-vide. Ainsi, par la proposition 2.18, $a_{r,n}$ n'est pas un diviseur à droite de $a_{p,n}\beta$. □

Nous remarquons que le cas $p = n-1$ est exclu de la proposition 2.19. Ce cas est traité par le résultat suivant.

Proposition 2.21. *Supposons $n \geqslant 3$. Pour toute tresse non triviale β de B^{+*}_{n-1} il y a équivalence entre :*

(i) la B^{+*}_{n-1}-fin de $\phi_n(a_{n-1,n}\beta)$ est triviale ;

(ii) la B^{+*}_{n-1}-fin de $\phi_n(\beta)$ est triviale.

Démonstration. Comme un diviseur à droite de $\phi_n(\beta)$ est aussi un diviseur à droite de $\phi_n(a_{n-1,n}\,\beta)$, l'implication $(i) \Rightarrow (ii)$ est immédiate.

Montrons maintenant $(ii) \Rightarrow (i)$. Pour une lettre x de $\mathscr{A}_{n-1}$ et y, z des lettres de $\mathscr{A}_n$, les seules relations dans B^{+*}_n de la forme $a_{n-1,n}\, x = y\, z$ avec $(y,z) \neq (a_{n-1,n}, x)$ sont des relations de commutations dans lesquelles x est de la forme $a_{p,q}$ avec $p < q < n-1$. Soit w un $\mathscr{A}_n$-mot représentant β. Tout $\mathscr{A}_n$-mot équivalent à $a_{n-1,n}w$ est de la forme $u\, a_{n-1,n}\, v$. Par ce qui précède, u est un $\mathscr{A}_{n-2}$-mot représentant une tresse qui commute avec $a_{n-1,n}$ et donc $u\, v$ représente la tresse β. Par le lemme 2.5 la seule lettre de $\mathscr{A}_n$ qui divise à droite $\phi_n(\beta)$ est du type $a_{..,n}$. Ainsi tout $\mathscr{A}_n$-mot représentant β doit se terminer par une lettre de la forme $a_{..,n-1}$. En particulier v n'est pas un $\mathscr{A}_{n-2}$-mot et donc $\overline{v}$ est non trivial et admet seulement $\beta^{\#}$ comme dernière lettre. Nous venons donc d'établir que tout mot $\mathscr{A}_n$-mot représentant $a_{n-1,n}\,\beta$ finit par la lettre $\beta^{\#}$ qui est du type $a_{..,n-1}$. Grâce au lemme 2.5 nous obtenons que la B^{+*}_{n-1}-fin de $\phi_n(a_{n-1,n}\,\beta)$ est triviale. □

2.5 Caractérisation syntaxique

Nous sommes maintenant en mesure de caractériser les ϕ_n-éclatements parmi les suites finies d'éléments de B^{+*}_{n-1}.

Proposition 2.22. *Supposons $n \geqslant 3$. Une suite finie $(\beta_b, \ldots, \beta_1)$ de tresses de B^{+*}_{n-1} est le ϕ_n-éclatement d'une tresse de B^{+*}_n si et seulement si :*

(i) pour $k \geqslant 3$ ou $k = b$, la tresse β_k est non triviale ;

(ii) pour $k \geqslant 2$, la B^{+*}_{n-1}-fin de $\phi_n(\beta_k)$ est triviale ;

(iii) si, pour $k \geqslant 3$, nous avons $\beta_k^{\#} \neq a_{n-2,n-1}$; alors β_{k-1} contient une $\phi_n(\beta_k^{\#})$-barrière.

Démonstration. Soit $(\beta_b, \dots, \beta_1)$ le ϕ_n-éclatement d'une tresse de B_n^{+*}. La condition (i) est le (ii) du lemme 2.4. La condition(2.8) implique que la B_{n-1}^{+*}-fin de

$$\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1})$$

est triviale pour $k \geqslant 1$. En particulier la B_{n-1}^{+*}-fin de $\phi_n(\beta_{k+1})$ doit être triviale pour $k \geqslant 1$, ce qui implique la condition (ii). La condition (iii) est le lemme 2.10.

Réciproquement, montrons qu'une suite $(\beta_b, \dots, \beta_1)$ de tresses de B_{n-1}^{+*} satisfaisant aux conditions (i) à (iii) est le ϕ_n-éclatement d'une tresse de B_n^{+*}. La condition (i) implique que la tresse β_b est non triviale. Pour $k \geqslant 2$ notons γ_k la tresse

$$\gamma_k = \phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1}) \cdot \beta_k.$$

Montrons que pour $k \geqslant 3$, et aussi $k = 2$ dans le cas $\beta_2 \neq 1$, nous avons la propriété

$$\beta_k^{\#} \text{ est la seule lettre de } \mathscr{A}_n \text{ qui divise } \gamma_k \text{ à droite.} \tag{2.13}$$

Remarquons que la condition (i) garantit l'existence de $\beta_k^{\#}$ pour $k \geqslant 3$. Pour $k = b$, la condition (ii) implique que la B_{n-1}^{+*}-fin de $\phi_n(\beta_b)$ est triviale. Ainsi par le lemme 2.5 la seule lettre de $\mathscr{A}_{n-1}$ qui divise la tresse β_b à droite est $\beta_b^{\#}$. Comme tout diviseur à droite d'un élément de B_{n-1}^{+*} appartient à B_{n-1}^{+*}, nous avons établi la relation (2.13) pour $k = b$.

Supposons que (2.13) est vérifiée pour $k \geqslant 4$, ou $k \geqslant 3$ dans le cas $\beta_2 \neq 1$, et montrons-la pour $k-1$. Par la condition (ii), il existe p tel que $\beta_k^{\#}$ soit $a_{p-1,n-1}$. Les conditions (ii) et (iii) impliquent que la B_{n-1}^{+*}-fin de $\phi_n(\beta_{k-1})$ est triviale et que β_{k-1} contient une $a_{p,n}$-barrière lorsque nous avons $p < n-1$. Ainsi par la proposition 2.19 (pour $p < n-1$) et la proposition 2.21 (pour $p = n-1$), la B_{n-1}^{+*}-fin de la tresse $\phi_n(a_{p,n}\beta_{k-1})$ est triviale. En utilisant le lemme 2.5, nous obtenons que $\phi_n(a_{p,n}\beta_{k-1})$ est divisible à droite par une unique lettre de $\mathscr{A}_n$. Il en suit que $\beta_{k-1}^{\#}$ est l'unique lettre de $\mathscr{A}_n$ divisant $a_{p,n}\,\beta_{k-1}$ à droite. Notons $ua_{p-1,n-1}$ et v deux $\mathscr{A}_n$-mots représentant γ_k et β_{k-1} respectivement. La tresse γ_{k-1} est alors représentée par $\phi_n(u)a_{p,n}v$. Soit y une lettre de $\mathscr{A}_n$ différente de $\beta_{k-1}^{\#}$. Comme y n'est pas un diviseur à droite de $a_{p,n}\,\beta_{k-1}$, la proposition 2.18 implique l'existence d'une lettre x de $\mathscr{A}_n$ différente de $a_{p,n}$ satisfaisant

$$\phi_n(u)a_{p,n}vy^{-1} \curvearrowright \phi_n(u)a_{p,n}x^{-1} \cdots .$$

Le mot $\phi_n(u)a_{p,n}$ représente la tresse $\phi_n(\gamma_k)$. Par hypothèse d'induction x n'est pas un diviseur à droite de $\phi_n(\gamma_k)$. La proposition 2.18 implique alors que le mot $D(\phi_n(u)a_{p,n}x^{-1})$ est non vide. Il en suit $D(\phi_n(u)a_{p,n}vy^{-1}) \neq \varepsilon$ et donc, toujours par la proposition 2.18, la lettre y n'est pas un diviseur à droite de la tresse γ_{k-1}. Nous venons ainsi d'établir (2.13) pour $k \geqslant 3$, et aussi $k = 2$ dans le cas $\beta_2 \neq 1$.

Une conséquence directe de (2.13) et la condition (ii) est que la seule lettre de $\mathscr{A}_n$ divisant à droite la tresse $\phi_n(\gamma_k)$ est de la forme $a_{..,n}$ et donc, par le lemme 2.5, la B_{n-1}^{+*}-fin de la tresse γ_k est triviale pour $k \geqslant 3$ et pour $k = 2$ dans le cas $\beta_k \neq 1$. Il reste à établir que la B_{n-1}^{+*}-fin de $\phi_n(\gamma_2)$ est aussi triviale dans le cas $\beta_2 = 1$.

Supposons donc $\beta_2 = 1$. La condition (iii) implique $\beta_3^{\#} = a_{n-2,n-1}$. Par la relation (2.13), $a_{n-2,n-1}$ est la seule lettre de $\mathscr{A}_n$ qui divise γ_3 à droite. Comme $\gamma_2 = \phi_n(\gamma_3)$ est vérifiée, la lettre $\phi_n^2(a_{n-2,n-1}) = a_{1,n}$ est la seule qui divise $\phi_n(\gamma_2)$ à droite. En particulier la B_{n-1}^{+*}-fin de $\phi_n(\gamma_2)$ est triviale par le lemme 2.5. □

Les conditions (i), (ii) et (iii) de la proposition 2.22 sont faciles à vérifier lorsque les tresses $\beta_1, \dots, \beta_b$ sont données par leur forme normale tournante.

Corollaire 2.23. *Supposons $n \geqslant 3$. Soit $(w_b, \dots, w_1)$ une suite finie de $\mathscr{A}_{n-1}$-mots. Alors le $\mathscr{A}_n$-mot*

$$\phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1, \tag{2.14}$$

est n-tournant si et seulement si les conditions suivantes sont satisfaites :

- (i) *pour $k \geqslant 1$, le mot w_k est $(n-1)$-tournant ;*
- (ii) *pour $k \geqslant 3$, le mot w_k se termine par $a_{..,n-1}$;*
- (iii) *le mot w_2 est vide (sauf pour $b = 2$) ou se termine par $a_{..,n-1}$;*
- (iv) *si, pour $k \geqslant 3$, le mot w_k se termine par $a_{p-1,n-1}$ avec $p \neq n-1$ alors le mot w_{k-1} contient une $a_{p,n}$-barrière.*

Démonstration. Supposons que la suite de $\mathscr{A}_{n-1}$-mots $(w_b, \dots, w_1)$ satisfait les conditions (i) à (iv) et montrons que le mot w défini en (2.14) est n-tournant. Notons β_i (resp. β) la tresse représentée par w_i (resp. w). Par la condition (i) et la définition 1.12, le mot w est tournant si et seulement si $(\beta_b, \dots, \beta_1)$ est un ϕ_n-éclatement. Les conditions (ii) et (iii) impliquent la condition (i) de la proposition 2.22. La condition (iii) de la proposition 2.22 est une conséquence des conditions (ii) et (iv).

Établissons maintenant la condition (ii) de la proposition 2.22. Soit k un entier de $[2, b]$. Si la B_{n-1}^{+*}-fin de $\phi_n(\beta_k)$ n'est pas triviale, alors il existe $a_{p,q}$, avec $1 \leqslant p < q < n$, divisant $\phi_n(\beta_k)$ à droite. Comme la tresse β_k appartient à B_{n-1}^{+*}, nous devons avoir $p \neq 1$ et donc β_k est divisible à droite par $a_{p-1,q-1}$ avec $q - 1 \leqslant n - 2$. La B_{n-1}^{+*}-fin de w_k est donc non triviale. Comme le mot w_k est $(n-1)$-tournant, sa dernière lettre doit provenir de sa B_{n-1}^{+*}-fin. Ainsi w_k devrait finir par une lettre $a_{i,j}$ satisfaisant $j \leqslant n - 2$, ce qui est en contradiction avec les conditions (ii) et (iii). Nous concluons en utilisant la proposition 2.22. □

Il n'est pas vrai en général que toute décomposition d'un mot n-tournant comme en (2.14) satisfait les conditions $(i) - (iv)$ du corollaire 2.23. Cependant nous avons le résultat suivant.

Proposition 2.24. *Pour $n \geqslant 3$ et tout mot n-tournant w, il existe une unique suite $(w_b, \dots, w_1)$ de mots $(n-1)$-tournants telle que w se décompose comme en* (2.14) *et que les conditions $(ii) - (iv)$ du corollaire 2.23 soient vérifiées.*

Démonstration. Par définition de mot n-tournant et par le lemme 2.5 une telle suite existe. Montrons qu'elle est unique. Supposons que w soit un mot n-tournant et que $(w_b, \dots, w_1)$ et $(w'_c, \dots, w'_1)$ soient deux suites distinctes de mots $(n-1)$-tournants satisfaisant aux conditions (ii) à (iv) du corollaire 2.23 et que nous ayons

$$w = \phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1 = \phi_n^{c-1}(w'_c) \cdot \ldots \cdot \phi_n(w'_2) \cdot w'_1.$$

Soit k le plus petit entier vérifiant $w_k \neq w'_k$. Comme les sommes des longueurs des mots des deux suites sont les mêmes nous avons $k \leqslant \min\{b, c\}$. Sans perte de généralité, nous pouvons supposer que w'_k est un suffixe propre de w_k, c'est-à-dire, $w_k = u\, w'_k$. Soit x la dernière lettre de w'_{k+1} ou la dernière lettre de w'_{k+2} si w_{k+1} est vide. Par les conditions (ii) et (iii) du corollaire 2.23, nous avons $x = a_{p-1,n-1}$ pour un certain p et w_k admet alors

$$\phi_n(a_{p-1,n-1})w'_k = a_{p,n}w'_k \quad \text{ou bien} \quad \phi_n^2(a_{p-1,n-1})w'_k = a_{1,p+1}w'_k$$

comme suffixe. Le premier cas est impossible car w_k est un $\mathscr{A}_{n-1}$-mot. Le second cas peut se produire seulement pour $k = 1$ et $w'_2 = \varepsilon$. Le mot w'_2 est alors vide et la condition (iv) du corollaire 2.23 implique que la dernière lettre de w'_3, qui est x, est égale à $a_{n-2,n-1}$. Nous obtenons ainsi que w_k admet $a_{1,n}u$ comme suffixe, ce qui est impossible parce que w_k est un $\mathscr{A}_{n-1}$-mot. □

Le théorème 2.2 est une conséquence immédiate du corollaire 2.23 et de la proposition 2.24.

3 Rationnalité

Dans cette section nous allons exploiter la description syntaxique de la forme normale tournante donnée au théorème 2.2 afin de montrer que le langage des mots n-tournants est rationnel.

Notation 3.1. Pour $n \geqslant 1$, nous notons R_n l'ensemble des mots n-tournants.

Pour établir que le langage R_n est rationnel nous allons montrer qu'il existe un automate déterministe fini le reconnaissant. Comme la forme normale tournante est définie à partir de divisions à droite il est plus naturel pour un automate de lire les mots tournants à partir de la droite. Pour un $\mathscr{A}_n$-mot $w = x_0 \cdot \ldots \cdot x_k$ nous notons $\Pi(w)$ le mot

miroir $x_k \cdot \ldots \cdot x_0$. Par le théorème 1.2.8 de [58] le langage R_n est rationnel si et seulement si le langage $\Pi(R_n)$ l'est. Le but de cette section est de construire, pour tout $n \geqslant 2$, un automate fini déterministe reconnaissant le langage $\Pi(R_n)$.

Définition 3.2. Un *automate fini déterministe* est un 5-uplet $(E \cup \{\otimes\}, \mathscr{A}, \mu, F, i)$ où $E \cup \{\otimes\}$ est l'ensemble fini des *états*, $\mathscr{A}$ est un *alphabet* fini,

$$\mu : (E \cup \{\otimes\}) \times \mathscr{A} \to E \cup \{\otimes\}$$

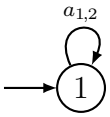
est la *fonction de transition*, $F \subseteq S$ est l'ensemble des *états acceptant* et i est l'*état initial*.

Dans ce chapitre tous les automates sont équipés d'un état poubelle $\otimes$ qui ne sera pas dessiné. Ainsi pour tout état $e \in E$, nous avons $\mu(e, \otimes) = \otimes$ et nous avons $\mu(e, x) = \otimes$ si l'image de (e, x) n'est pas précisée. Une autre particularité des automates décrits dans ce chapitre, est que tous les états de E sont acceptants, c'est-à-dire, $F = E$.

Par exemple un automate reconnaissant le langage $R_2 = \Pi(R_2)$ est

$$\mathcal{A}_2 = (\{1, \otimes\}, \{a_{1,2}\}, \mu_2, \{1\}, 1),$$

avec $\mu_2(1, a_{1,2}) = 1$. Le dessin suivant donne une description complète de $\mathcal{A}_2$:



La flèche horizontale pointe vers l'état initial.

Construisons maintenant un automate $\mathcal{A}_3$ reconnaissant le langage $\Pi(R_3)$.

Proposition 3.3. *Un $\mathscr{A}_3$-mot est tournant si et seulement s'il peut s'écrire*

$$x_b^{e_b} \cdot \ldots \cdot a_{1,3}^{e_3}\, a_{2,3}^{e_2}\, a_{1,2}^{e_1}$$

avec $e_k \neq 0$ pour tout $k \geqslant 3$ et où

$$x_k = \begin{cases} a_{1,2} & \text{si } k \equiv 1 \mod 3, \\ a_{2,3} & \text{si } k \equiv 2 \mod 3, \\ a_{1,3} & \text{si } k \equiv 3 \mod 3. \end{cases}$$

Démonstration. Les mots 2-tournants sont les puissances de $a_{1,2}$. Soit w un $\mathscr{A}_3$-mot. Il existe alors une unique suite $e_1, \ldots, e_b$ d'entiers telle qu'on ait

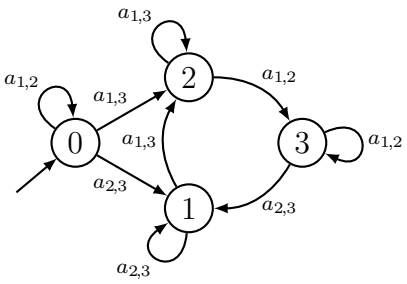
$$w = x_b^{e_b} \cdot \ldots \cdot a_{1,3}^{e_3}\, a_{2,3}^{e_2}\, a_{1,2}^{e_1}.$$

En posant $w_k = a_{1,2}^{e_k}$, nous obtenons

$$w = \phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1.$$

Comme tout mot non vide w_k se termine par $a_{1,2}$, la condition (iv) du théorème 2.2 est vide. Ainsi le mot w est tournant si et seulement s'il satisfait les conditions (ii) et (iii) du théorème 2.2, c'est-à-dire, si et seulement si e_k est différent de 0 pour $k \geqslant 3$. □

La proposition 3.3 permet de construire l'automate $\mathcal{A}_3$ suivant pour reconnaître le langage $\Pi(R_3)$:



Voyons maintenant le principe de construction d'un automate $\mathcal{A}_n$ reconnaissant le langage $\Pi(R_n)$ pour $n \geqslant 4$. La condition (i) du théorème 2.2 suggère une construction par induction sur n. Bien que naturelle, la construction des automates $\mathcal{A}_n$ pour $n \geqslant 4$ est bien plus délicate que pour $n = 2$ ou 3 car la condition (iv) du théorème 2.2 est non vide dans ce cas et doit donc être vérifiée. Comme suggéré par la condition (ii), le langage $R_n^\bullet$ (voir notation 3.4) des mots n-tournants finissant par une lettre de la forme $a_{..,n}$ est au cœur de la construction. Ainsi, au lieu de construire directement l'automate $\mathcal{A}_n$ nous allons commencer par construire un automate $\mathcal{A}_n^\bullet$ reconnaissant le langage $\Pi(R_n^\bullet)$. Tout mot w du langage $\Pi(R_n)$ étant obtenu par concaténation d'un mot w_1' de $\Pi(R_n^\bullet)$ et d'un mot w_1 de $\Pi(R_{n-1})$, l'automate $\mathcal{A}_n$ sera naturellement obtenu à partir des automates $\mathcal{A}_{n-1}$ et $\mathcal{A}_n^\bullet$.

Supposons que nous disposions d'un automate $\mathcal{A}_{n-1}^\bullet$ reconnaissant le langage $\Pi(R_{n-1}^\bullet)$. Afin de vérifier la condition (iv) du théorème 2.2, nous devons modifier $\mathcal{A}_{n-1}^\bullet$ pour qu'il puisse mémoriser si le mot lu contient des $a_{..,n}$-barrières. Une duplication des états de $\mathcal{A}_{n-1}^\bullet$ accompagnée de modifications standards de la fonction de transition permettent de stocker un bit d'information. Comme il y a exactement $n-3$ types de $a_{..,n}$-barrières nous devons multiplier le nombre d'états de $\mathcal{A}_{n-1}^\bullet$ par au plus 2^{n-3} afin d'obtenir un automate $\mathcal{B}_{n-1}^0$ reconnaissant $\Pi(R_{n-1}^\bullet)$ et détectant si le mot lu contient des $a_{..,n}$-barrières.

Puis, pour $k \in [1, n-1]$ nous construisons un automate $\mathcal{B}_{n-1}^k$ reconnaissant le langage $\Pi(\phi_n^k(R_{n-1}^\bullet))$ en appliquant ϕ_n^k à l'automate $\mathcal{B}_{n-1}^0$. Finalement, nous obtenons l'automate $\mathcal{A}_n^\bullet$ en connectant cycliquement les automates $\mathcal{B}_{n-1}^0, \ldots, \mathcal{B}_{n-1}^{n-1}$. Les connections entre les automates $\mathcal{B}_{n-1}^k$ et $\mathcal{B}_{n-1}^{k+1}$ seront faites afin de respecter la condition (iv) du théorème 2.2 grâce aux informations, portant sur les barrières rencontrées, stockées dans $\mathcal{B}_{n-1}^k$.

Notation 3.4. Pour $n \geqslant 2$, nous notons $R_n^\bullet$ le langage des n-mots tournants qui sont soit vides soit finissant avec une lettre de la forme $a_{..,n}$:

$$R_n^\bullet = \{w \in R_n \,|\, w^\# = a_{..,n}\}$$

Nous introduisons maintenant la notion d'automate partiel qui nous sera utile pour décrire séparément les différentes parties constituant l'automate $\mathcal{A}_n^\bullet$.

Définition 3.5. Un *automate partiel* est un 5-uplet $P = (E \cup \{\otimes\}, \mathscr{A}, \mu, E, I)$ où E, $\mathscr{A}$ et μ sont définis comme pour un automate et $I : \mathscr{A} \to E \cup \{\otimes\}$ est l'*application initiale*. La *clôture de l'automate partiel* P est l'automate

$$\mathcal{A}(P) = (E \cup \{\circ, \otimes\}, \mathscr{A}, \mu^c, E \cup \{\circ\}, \circ)$$

admettant la fonction de transition

$$\mu^c(e, x) = \begin{cases} I(x) & \text{si } e = \circ, \\ \mu(e, x) & \text{sinon.} \end{cases}$$

La fonction I d'un automate partiel P peut être considérée comme les entrées de P. Nous connecterons un automate partiel Q à un automate partiel P en ajoutant des transitions entre les états de Q et l'état $I(x)$ de P pour la lecture de la lettre x. Un automate partiel est dessiné de la même façon qu'un automate à l'exception de l'application initiale I : pour tout $x \in \mathscr{A}$ nous dessinons une flèche pointant sur $I(x)$ (si différent de $\otimes$) et étiquetée x.

Nous disons qu'un automate partiel reconnaît un langage donné si c'est le cas pour sa clôture.

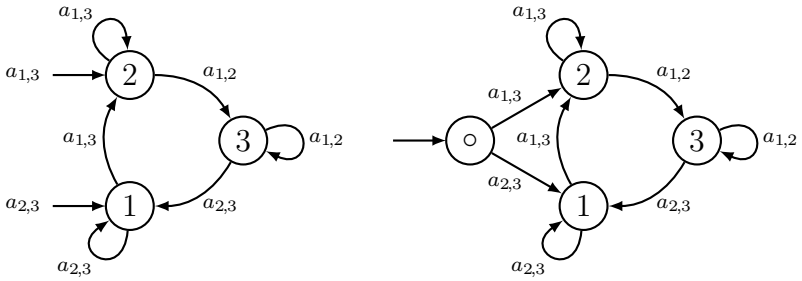


FIGURE 2.5 – L'automate partiel $P_3^\bullet$ et sa clôture $\mathcal{A}(P_3^\bullet)$, qui reconnaîssent le langage $\Pi(R_3^\bullet)$.

Voyons maintenant comment construire inductivement un automate partiel $P_n^\bullet$ reconnaissant le langage $\Pi\left(R_n^\bullet\right)$ pour $n \geqslant 3$. Pour $n = 3$ nous avons déjà l'automate partiel $P_3^\bullet$ de la figure 2.5. Pour la suite supposons $n \geqslant 4$ et que nous disposions d'un automate partiel

$$P_{n-1}^\bullet = (E_{n-1}^\bullet \cup \{\otimes\}, \mathscr{A}_{n-1}, \mu_{n-1}^\bullet, E_{n-1}^\bullet, I_{n-1}^\bullet)$$

reconnaissant le langage $\Pi\left(R_{n-1}^\bullet\right)$.

Nous commençons par construire un automate partiel P_n^0 reconnaissant $\Pi(R_{n-1}^\bullet)$ et mémorisant des informations sur les barrières rencontrées. Nous définissons un ensemble d'état E_n^0 en posant

$$E_n^0 = \{0\} \times E_{n-1}^\bullet \times \mathcal{P}(\{a_{2,n}, \ldots, a_{n-2,n}\}),$$

où $\mathcal{P}(X)$ désigne l'ensemble des parties d'un ensemble X.

Un état de E_n^0 sera alors noté $(0, e, m)$. L'entier 0 est utilisé pour identifier cet automate partiel particulier parmi les n qui constitueront $P_n^\bullet$. L'ensemble m est une mémoire permettant de stocker les informations sur les barrières rencontrées.

Notation 3.6. Pour $a_{i,j} \in \mathscr{A}_{n-1}$ nous notons $\mathrm{bar}(a_{i,j})$ l'ensemble des lettres $a_{p,n}$ telles que $a_{i,j}$ soit une $a_{p,n}$-barrière :

$$\mathrm{bar}(a_{i,j}) = \{a_{p,n} \,|\, i < p < j\}.$$

Définition 3.7. L'automate partiel $P_n^0 = (E_n^0 \cup \{\otimes\}, \mathscr{A}_{n-1}, \mu_n^0, E_n^0, I_n^0)$ est défini par : pour tout $x \in \mathscr{A}_{n-1}$,

$$I_n^0(x) = \begin{cases} (0, I_{n-1}^\bullet(x), \mathrm{bar}(x)) & \text{si } I_{n-1}^\bullet(x) \neq \otimes, \\ \otimes & \text{si } I_{n-1}^\bullet(x) = \otimes, \end{cases}$$

et pour tout $(0, s, m) \in E_n^0$ et tout $x \in \mathscr{A}_{n-1}$,

$$\mu_n^0((0, e, m), x) = \begin{cases} (0, \mu_{n-1}^\bullet(e, x), m \cup \mathrm{bar}(x)) & \text{si } \mu_{n-1}^\bullet(e, x) \neq \otimes, \\ \otimes & \text{si } \mu_{n-1}^\bullet(s, x) = \otimes. \end{cases}$$

Proposition 3.8. *L'automate partiel P_n^0 reconnaît le langage $\Pi(R_{n-1}^\bullet)$. De plus un mot de la forme $\Pi(w)$ accepté par P_n^0 contient une $a_{p,n}$-barrière si et seulement si P_n^0 est dans l'état $(0,e,m)$ avec $a_{p,n} \in m$ après avoir lu $\Pi(w)$.*

Démonstration. Notons $\mathcal{A}$ et $\mathcal{A}'$ les clôtures de $P_{n-1}^\bullet$ et P_n^0 respectivement. Supposons que $w = w_1 \cdot \ldots \cdot w_\ell$ soit un $\mathscr{A}_n$-mot de longueur ℓ. Pour tout $k \in [1,\ell]$, notons e_k (*resp.* e'_k) l'état de l'automate $\mathcal{A}$ (*resp.* $\mathcal{A}'$) après avoir lu la k-ème lettre de $\Pi(w)$, c'est-à-dire, la lettre $w_{\ell-k+1}$. Par construction de μ_n^0, pour tout $k \in [1,\ell]$, nous avons

$$e'_k = \begin{cases} \otimes & \text{si } e_k = \otimes, \\ (0, e_k, m_k) & \text{sinon (pour un certain ensemble } m_k). \end{cases}$$

En particulier $e'_\ell \neq \otimes$ si et seulement si $e_\ell \neq \otimes$. Ainsi les deux automates acceptent ou pas le mot $\Pi(w)$. L'automate partiel P_n^0 reconnaît donc le langage $\Pi(R_{n-1}^\bullet)$ car c'est le cas pour $P_{n-1}^\bullet$ par hypothèse.

Montrons maintenant le résultat concernant m_ℓ lorsque le mot $\Pi(w)$ est accepté par P_n^0. Une induction immédiate sur $k \in [1,\ell]$ établit

$$m_k = \mathrm{bar}(w_\ell) \cup \cdots \cup \mathrm{bar}(w_{\ell-k+1}).$$

En particulier pour $k = \ell$, nous avons $m_\ell = \mathrm{bar}(w_1) \cup \cdots \cup \mathrm{bar}(w_\ell)$. Nous concluons, en utilisant la définition de bar(..), que w contient une $a_{p,n}$-barrière si et seulement si $a_{p,n}$ appartient à m_ℓ. □

Comme la seule $a_{p,4}$-barrière de $\mathscr{A}_4$ est $a_{1,3}$, l'automate partiel P_4^0 est obtenu de $P_3^\bullet$ en connectant des arêtes étiquetées $a_{1,3}$ à une copie de P_3, comme illustré à la figure 2.6.

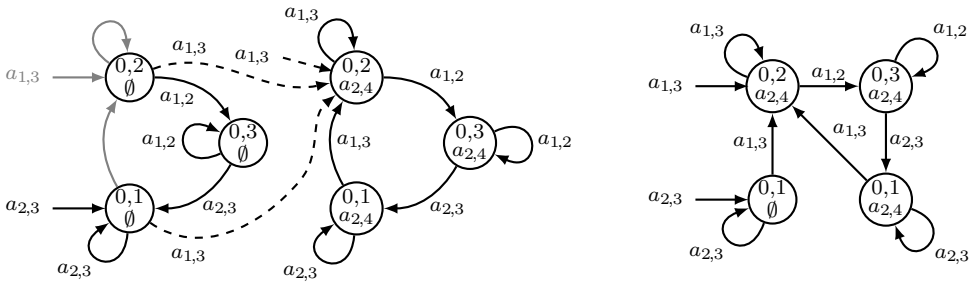


FIGURE 2.6 – L'automate partiel P_4^0. Les transitions obsolètes de $P_3^\bullet$ sont grisées. Les nouvelles transitions sont en tiretées. L'automate partiel de droite est obtenu de P_4^0 en retirant les états inaccessibles.

Nous construisons maintenant $n-1$ copies déformées de P_n^0 en utilisant l'homomorphisme de mot ϕ_n.

Définition 3.9. Pour $f = (0,e,m) \in E_n^0$ et $k \in [1, n-1]$, nous posons $\Phi_n^k(f) = (k,e,m)$ puis $E_n^k = \Phi_n^k(E_n^0)$. Nous construisons alors un automate partiel

$$P_n^k = \left(E_n^k \cup \{\otimes\}, \phi_n^k(\mathscr{A}_{n-1}), \mu_n^k, E_n^k, I_n^k\right),$$

en posant $I_n^k(\phi_n^k(x)) = \Phi_n^k(I_n^0(x))$ ainsi que

$$\mu_n^k((k,e,m), \phi_n^k(x)) = \Phi_n^k\left(\mu_n^0((0,e,m),x)\right),$$

avec la convention $\Phi_n^k(\otimes) = \otimes$.

En d'autres mots, P_n^k est obtenu de P_n^0 en remplaçant une lettre x de P_n^0 par la lettre $\phi_n^k(x)$ et un état $(0,e,m)$ de P_n^0 par (k,e,m). De la proposition 3.8, nous obtenons

immédiatement que l'automate partiel P_n^k reconnaît le langage $\phi_n^k(\Pi(R_n^\bullet))$ et mémorise les informations utiles sur les barrières rencontrées.

Nous pouvons maintenant construire un automate partiel reconnaissant $\Pi(R_n^\bullet)$ en connectant cycliquement les n automates partiels P_n^k pour $k \in [0, n-1]$. Les transitions entre deux automates partiels adjacents sont faites en utilisant les applications initiales et en respectant la condition (iv) du théorème 2.2 grâce aux informations stockées sur les barrières rencontrées.

Définition 3.10. Nous définissons un automate partiel $P_n^\bullet = (E_n^\bullet \cup \{\otimes\}, \mathscr{A}_n, \mu_n^\bullet, E_n, I_n^\bullet)$, avec $E_n^\bullet = E_n^0 \sqcup \ldots \sqcup E_n^k$ en posant

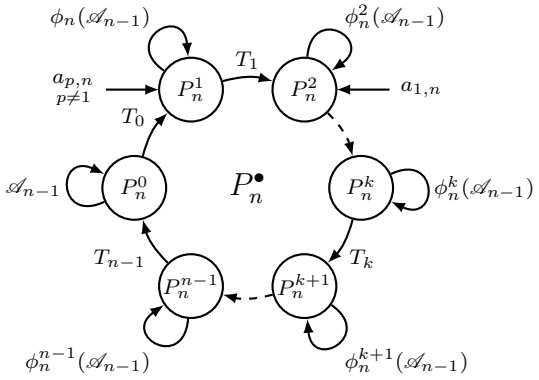
$$I_n^\bullet(x) = \begin{cases} I_n^1(x) & \text{si } x = a_{p,n} \text{ avec } p > 1, \\ I_n^2(x) & \text{si } x = a_{1,n}, \\ \otimes & \text{sinon,} \end{cases}$$

et ayant pour fonction de transition

$$\mu_n^\bullet((k,e,m),\phi_n^k(x)) = \begin{cases} \mu_n^k((k,e,m),\phi_n^k(x)) & \text{si } x \in \mathscr{A}_{n-1}, \\ I_n^{k+1}(\phi_n^k(x)) & \text{si } x = a_{n-1,n}, \\ I_n^{k+1}(\phi_n^k(x)) & \text{si } x = a_{p,n} \text{ avec } 2 \leqslant p \leqslant n-2 \\ & \text{et } a_{p,n} \in m, \\ \otimes & \text{sinon,} \end{cases}$$

avec la convention $I_n^n = I_n^0$.

Le diagramme suivant synthétise la construction de l'automate partiel $P_n^\bullet$ à partir des automates partiels $P_n^0, \ldots, P_n^{n-1}$.



Une arête étiquetée T_k désigne l'ensemble des transitions de la forme $\mu_n^\bullet((k,s,m),\phi_n^k(a_{\cdot,n}))$.

Lemme 3.11. *L'automate partiel $P_n^\bullet$ reconnaît le langage $\Pi(R_n^\bullet)$.*

Démonstration. Notons $\mathcal{A}^\bullet$ la clôture de $P_n^\bullet$. Soit w un $\mathscr{A}_n$-mot non vide. Il existe une unique suite $(w_b, \ldots, w_1)$ de $\mathscr{A}_{n-1}$-mots vérifiant $w_b \neq \varepsilon$,

$$w = \phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1$$

et telle que, pour tout i, le mot $\phi_n^i(w_i)$ est le suffixe maximal de $\phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n^i(w_i)$ appartenant à $\phi_n^i(\mathscr{A}_{n-1}^*)$. Par définition de $I_n^\bullet$, le mot $\Pi(w)$ est accepté par $P_n^\bullet$ seulement si w se termine par une lettre $a_{p,n}$ pour un certain entier p.

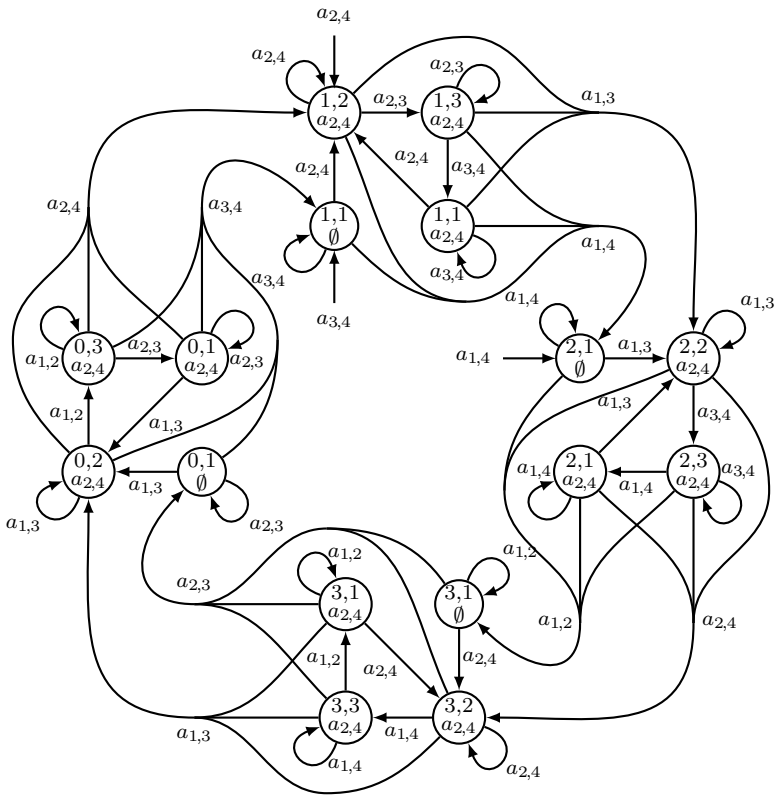


FIGURE 2.7 – Automate partiel $P_4^\bullet$ reconnaissant le langage $\Pi(R_4^\bullet)$.

Supposons que w soit un tel mot. Ainsi le premier entier j tel que w_j soit non vide est 2 ou 3. Plus précisément, nous avons $j = 2$ pour $p > 1$ et $j = 3$ pour $p = 1$. Dans les deux cas, l'automate est dans l'état $e \in E_n^j$ après avoir lu la première lettre de $\Pi(w)$. L'automate atteint un état en dehors de E_n^j s'il arrive sur l'état poubelle $\otimes$ ou s'il lit une lettre en dehors de $\phi_n^{j-1}(\mathscr{A}_{n-1})$, c'est-à-dire, une lettre de $\phi_n^j(\Pi(w_{j+1}))$. C'est un principe général : après avoir lu une lettre de $\phi_n^{i-1}(\Pi(w_i))$ l'automate $\mathcal{A}^\bullet$ se trouve dans l'état (t, s, m) avec $t \equiv i \mod n$. Par construction de P_n^t, le mot $\phi_n^{i-1}(\Pi(w_i))$ amène à un état acceptant si et seulement si w_i est un mot de R_{n-1}.

À ce stade nous avons montré qu'un mot $\Pi(w)$ est accepté par $\mathcal{A}^\bullet$ seulement si w est vide ou si w satisfait $w^\# = a_{p,n}$ ainsi que les conditions (i), (ii) et (iii) du théorème 2.2. Soit i un entier de $[j, k-1]$ et supposons que $\mathcal{A}^\bullet$ soit dans un état acceptant (t, e, m) avec $t \equiv i \mod n$ après avoir lu le mot

$$\Pi(\phi_n^{i-1}(w_i) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1).$$

Notons x la dernière lettre de w_{i+1}. Par construction de w_{i+1}, la lettre x n'appartient pas à $\phi_n^i(\mathscr{A}_{n-1})$ et donc nous avons $x = \phi_n^i(a_{p,n})$ pour un certain entier p. Par définition de $\mu_n^\bullet$ nous avons

$$\mu_n^\bullet((t, e, m), \phi_n^i(a_{p,n})) \neq \otimes$$

si et seulement si $p = n-1$ ou bien si $p \in [2, n-2]$ avec $a_{p,n} \in m$. Comme, par construction de P_n^t, nous avons $a_{p,n} \in m$ si et seulement si w_i contient une $a_{p,n}$-barrière, la condition (iv) du théorème 2.2 est satisfaite. Finalement, par le théorème 2.2, le mot $\Pi(w)$ est accepté par $\mathcal{A}^\bullet$ si et seulement si w appartient à $R_n^\bullet$. □

Supposons que nous disposions d'un automate

$$\mathcal{A}_{n-1} = (E_{n-1} \cup \{\otimes\}, \mathscr{A}_{n-1}, \mu_{n-1}, E_{n-1}, i)$$

reconnaissant le langage $\Pi(R_{n-1})$ pour $n \geqslant 4$.

Définition 3.12. En connectant l'automate $\mathcal{A}_{n-1}$ à l'automate partiel

$$P_n^\bullet = (E_n^\bullet \cup \{\otimes\}, \mathscr{A}_n, \mu_n^\bullet, E_n^\bullet, I_n^\bullet)$$

nous construisons un automate

$$\mathcal{A}_n = (E_n \cup \{\otimes\}, \mathscr{A}_n, \mu_n, E_n, i)$$

défini par $E_n = E_{n-1} \sqcup E_n^\bullet$ et

$$\mu_n(e,x) = \begin{cases} \mu_{n-1}(e,x) & \text{si } e \in E_{n-1} \text{ et } x \in \mathscr{A}_{n-1}, \\ I_n^\bullet(x) & \text{si } e \in E_{n-1} \text{ et } x \in \mathscr{A}_n \setminus \mathscr{A}_{n-1}, \\ \mu_n^\bullet(e,x) & \text{si } e \in E_n^\bullet. \end{cases}$$

Proposition 3.13. *Si $\mathcal{A}_{n-1}$ reconnaît le langage $\Pi(R_{n-1})$, l'automate $\mathcal{A}_n$ reconnaît le langage $\Pi(R_n)$.*

Démonstration. Soit w un $\mathscr{A}_n$-mot, w_1 le suffixe maximal de w qui soit un $\mathscr{A}_{n-1}$-mot et w' le préfixe associé. Par le théorème 2.2, le mot w est tournant si et seulement si w_1 et w' le sont. Par construction, l'automate $\mathcal{A}_n$ est dans un état différent de $\otimes$ après avoir lu $\Pi(w_1)$ si et seulement si w_1 est un mot $(n-1)$-tournant. Ainsi w est accepté seulement si w_1 est tournant. Supposons que c'est le cas. Par le lemme 3.11 l'automate $\mathcal{A}_n$ est dans un état acceptant après avoir lu $\Pi(w')$ si et seulement si le mot w' est tournant. Finalement, le mot $\Pi(w)$ est accepté par $\mathcal{A}_n$ si et seulement si w_1 et w' sont tous les deux tournants, ce qui est équivalent au fait que w soit un mot n-tournant. □

Par la proposition 3.13, le langage $\Pi(R_n)$ est rationnel et donc nous obtenons.

Théorème 3.14. *Le langage R_n des mots n-tournants est rationnel.*

L'automate partiel P_n^0 donnée à la définition 3.7 n'est clairement pas minimal car, comme illustré à la figure 2.6 il possède des états inaccessibles. Notons $\tilde{\mathcal{A}}_n$ l'automate construit à la définition 3.12 en remplaçant P_n^0 par l'automate partiel obtenu de P_n^0 après suppression de ses états inaccessibles. Pour $n = 2$ ou 3 nous posons $\tilde{\mathcal{A}}_n = \mathcal{A}_n$. Nous formulons alors la conjecture suivante.

Conjecture 3.15. *L'automate $\tilde{\mathcal{A}}_n$ est minimal et possède $\frac{(n+1)!}{6}$ états.*

Cette conjecture a été vérifiée sur ordinateur pour $n \leqslant 8$. À titre d'indication l'automate $\tilde{\mathcal{A}}_8$ est minimal et possède exactement 60 480 états.

3.1 Automaticité

Grâce à une caractérisation syntaxique des mots tournants nous avons établi que le langage des mots n-tournants est rationnel. Une question naturelle consiste à se demander si ce langage fournit une structure automatique au monoïde des tresses duales B_n^{+*}.

Notation 3.16. Pour un automate fini déterministe $\mathcal{A}$, on note $L(\mathcal{A})$ le langage reconnu par $\mathcal{A}$.

Suivant [19] et [58] nous introduisons la définition suivante :

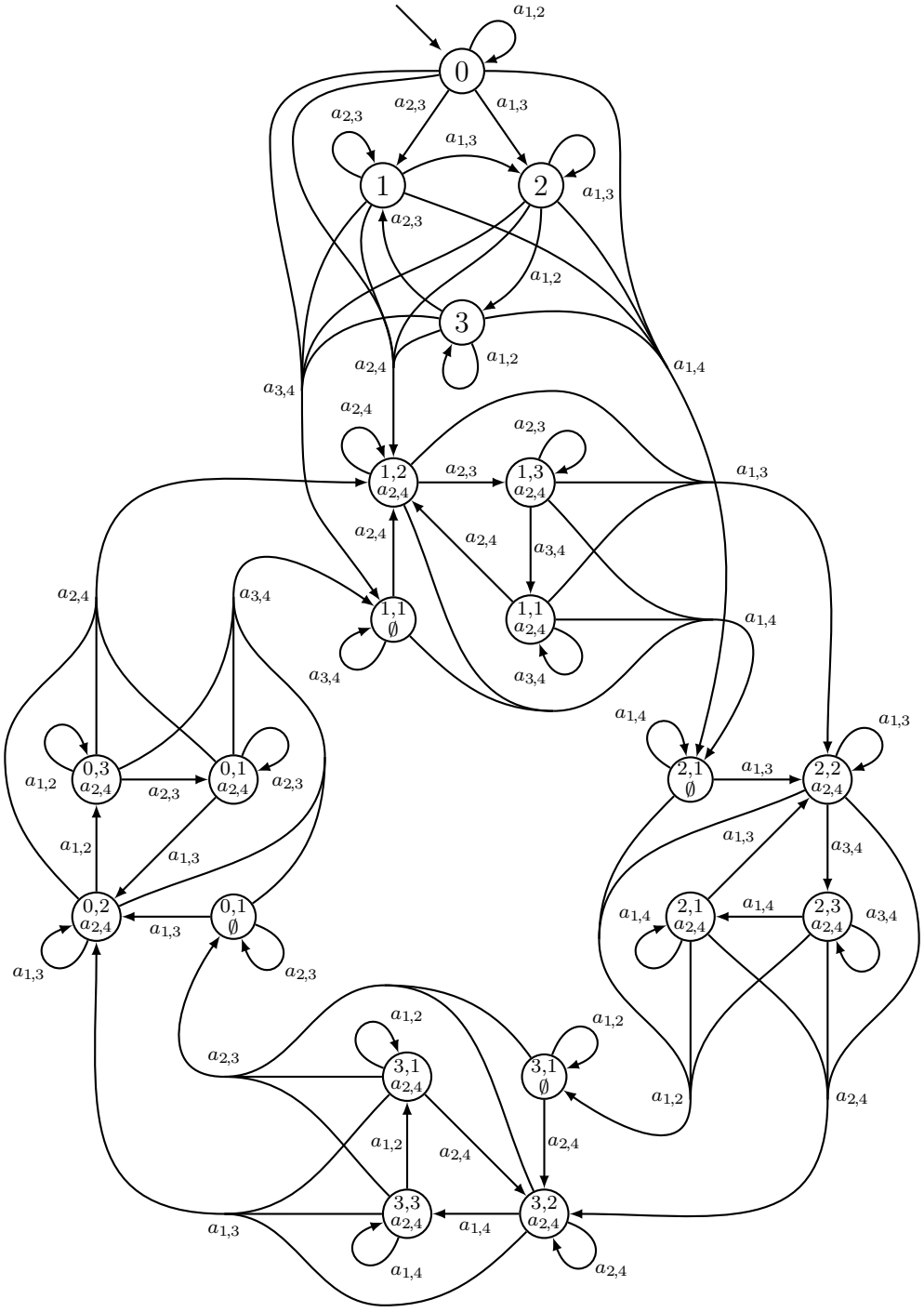


FIGURE 2.8 – Automate $\tilde{\mathcal{A}}_4$ reconnaissant le langage $\Pi(R_4)$.

Définition 3.17. Soit M un monoïde. Une *structure automatique à droite*, *resp.* à gauche, sur M consiste en un ensemble $\mathscr{A}$ de générateurs de M, un automate fini déterministe $\mathcal{A}$ sur l'alphabet $\mathscr{A}$ et des automates finis déterministes $\mathcal{M}_x$ sur l'alphabet $\mathscr{A} \times \mathscr{A}$, pour $x \in \mathscr{A}$, satisfaisant aux conditions suivantes :

(i) l'application $\pi_{\mathcal{A}} : L(\mathcal{A}) \to M$ est surjective,

(ii) pour tout $x \in \mathscr{A}$, le couple (u, v) appartient à $L(\mathcal{M}_x)$ si et seulement si $\overline{ux} = \overline{v}$, *resp.* $\overline{xu} = \overline{v}$ pour tous mots u et v de $L(\mathcal{A})$.

Reprenons les notations de la définition 3.17 et notons Γ le graphe de Cayley de M relativement à $\mathscr{A}$. Un chemin dans Γ reliant les éléments a et b de M est une suite d'arêtes (sans considération sur l'orientation) reliant a à b dans Γ. La *distance* $d_{\mathscr{A}}(a, b)$ est alors la longueur d'un plus court chemin dans Γ reliant a à b. Pour w un mot de $\mathscr{A}^*$ et t un entier de $\mathbb{N}$, nous notons $w(t)$ le préfixe de longueur t de w. Si t est supérieur à la longueur de w, nous posons $w(t) = w$. Nous disons que le monoïde M satisfait la propriété du compagnon de voyage à droite s'il existe une constante K telle que tous mots u et v de $L(\mathcal{A})$ vérifiant $d_{\mathscr{A}}(\overline{u}, \overline{v}) = 1$ nous ayons $d_{\mathscr{A}}(\overline{u(t)}, \overline{v(t)}) \leqslant K$ pour tout $t \geqslant 0$. La condition $d_{\mathscr{A}}(\overline{u}, \overline{v}) = 1$ signifie qu'il existe une lettre $x \in \mathscr{A}$ telle qu'on ait $\overline{ux} = \overline{v}$ ou $\overline{u} = \overline{vx}$.

Une conséquence du théorème 2.3.5 de [58] est que l'automaticité d'un groupe est équivalente à la propriété du *compagnon de voyage*. Comme précisé dans [19], la situation est plus compliquée dans le cas des monoïdes. Cependant la proposition 3.12 de [19] implique que l'automaticité à droite (*resp.* à gauche) d'un monoïde implique la propriété à droite (*resp.* à gauche) du compagnon de voyage.

Montrons que pour tout $n \geqslant 4$, la forme normale tournante ne munit pas B_n^{+*} d'une structure de monoïde automatique à droite. Pour tout entier $k \geqslant 0$, nous définissons deux mots

$$u_k = (a_{2,3}a_{1,2}a_{1,3})^k a_{1,2}^{3k}, \quad \text{et} \quad v_k = (a_{1,3}a_{2,3}a_{1,2})^k a_{1,4}a_{2,3}^{3k}.$$

Le ϕ_4-éclatement de $\overline{u_k}$ est (u_k) et u_k est 3-tournant par la proposition 3.3 et donc 4-tournant. Le ϕ_4-éclatement de $\overline{v_k}$ est

$$(\underbrace{a_{2,3}, \ldots, a_{2,3}}_{3k+1}, 1, a_{2,3}^{3k}).$$

En utilisant le théorème 2.2 nous montrons que v_k est 4-tournant. Nous observons

$$a_{2,3}a_{1,2}a_{1,3}a_{1,2}^3 \equiv a_{1,3}a_{2,3}a_{1,2}a_{2,3}^3 \equiv \delta_3^3.$$

Comme par [8] la tresse δ_3^3 est dans le centre de B_3^{+*} nous avons $u_k \equiv \delta_3^{3k}$ puis

$$v_k \equiv (a_{1,3}a_{2,3}a_{1,2})^k a_{2,3}^{3k}a_{1,4} \equiv \delta_3^{3k}a_{1,4} \equiv u_k a_{1,4},$$

et ainsi la distance $d_{\mathscr{A}_4}(\overline{u_k}, \overline{v_k}) = 1$. Finalement, u_k et v_k se terminent par $3k$ copies de deux lettres différentes de $\mathscr{A}_4$, ainsi la propriété du compagnon de voyage à droite ne peut pas être satisfaite. La forme normale tournante n'est donc pas automatique à droite pour $n = 4$ (et donc pour $n \geqslant 4$).

À ce jour, nous ne savons pas si la forme normale tournante est automatique à gauche. Nous pensons que contrairement à l'exemple précédent, si w est un mot n-tournant et x est une lettre de $\mathscr{A}_n$ alors l'existence de barrières peut empêcher le déplacement de x trop à droite durant le calcul de la forme normale tournante de xw.

3.2 Application aux représentants σ-définis.

Nous renvoyons le lecteur à la sous-section 1.2 du chapitre 1 pour la notion de mot σ-défini et son utilisation dans la construction de l'ordre des tresses. Grâce à l'homomorphisme de mot défini par

$$a_{p,q} \mapsto \sigma_p \cdots \sigma_{q-1}\, \sigma_q\, \sigma_{q-1}^{-1} \cdots \sigma_p^{-1}$$

les notions de mot σ-défini, σ_i-positif et σ_i-négatif s'étendent naturellement aux $\mathscr{A}_n^{\pm}$-mots.

Nous disons qu'une tresse a pour *indice* $k \geqslant 2$ si elle appartient à B_k mais pas à B_{k-1} avec la convention $B_1 = \{1\}$. Chaque $\mathscr{S}_n^{\pm}$-mot représentant une tresse d'indice $k \geqslant 2$ doit contenir une lettre σ_{k-1} ou une lettre σ_{k-1}^{-1}. Ainsi, par la remarque 1.10 du chapitre 1 une tresse d'indice $k \geqslant 2$ est soit σ_{k-1}-positive soit σ_{k-1}-négative.

Une conséquence de la proposition 3.4 du chapitre 1 est :

Corollaire 3.18 (Proposition 6.1 de [67])**.** *Supposons $n \geqslant 3$. Toute tresse β de B_n admet une unique expression $\delta_n^{-t}\, w$ où t est un entier positif, w est un mot n-tournant, et la tresse $\overline{w}$ n'est pas divisible à gauche par δ_n sauf si t est nul.*

Une adaptation immédiate de la proposition 4.4 de [70], établie avec L. Paris, au contexte des tresses duales donne :

Proposition 3.19. *Supposons $n \geqslant 3$ et que β soit une tresse de B_n^{+*}. Soit t un entier positif et $(w_b, \ldots, w_1)$ le ϕ_n-éclatement de β. Pour $t \geqslant b-1$, le quotient $\delta_n^{-t}\, \beta$ est représenté par le $\mathscr{A}_n^{\pm}$-mot σ_{n-1}-négatif*

$$\delta_n^{-t+b+1}\, w_b\, \delta_n^{-1}\, w_{b-1}\, \delta_n^{-1} \cdots w_2\, \delta_n^{-1}\, w_1, \tag{2.15}$$

(où δ_n est donnée par le mot $a_{1,2}\, a_{2,3} \cdots a_{n-1,n}$). Pour $t < b-1$, le quotient $\delta_n^{-t}\, \beta$ n'est pas σ_{n-1}-négatif.

La proposition 3.19 fournit des représentants σ_{n-1}-négatifs spécifiques pour chaque tresse σ_{n-1}-négative de B_n. Malheureusement ce représentant σ_{n-1}-négatif n'est pas unique.

Notation 3.20. Notons $\mathrm{R}_n^{\sigma^{-1}}$ l'ensemble des mots de la forme (2.15) tels que la tresse représentée par

$$\phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1$$

ne soit pas divisible à gauche par δ_n.

Supposons que $(w_b, \ldots, w_1)$ soit une suite de $\mathscr{A}_{n-1}$-mots satisfaisant aux conditions (i) à (iv) du théorème 2.2. À la section 3 nous avons construit explicitement un automate fini déterministe reconnaissant le miroir du mot $\phi_n^{b-1}(w_b) \cdots w_1$. Cette construction est basée sur la vérification des conditions du théorème 2.2 et sur la détection des transitions entre les mots $\phi_n^{i-1}(w_i)$ et $\phi_n^i(w_{i+1})$. Ainsi, si nous ajoutons une lettre $ à l'alphabet $\mathscr{A}_n$ nous pouvons construire un automate fini déterministe reconnaissant le miroir des mots

$$w_b\$w_{b-1}\$\cdots\$w_2\$w_1.$$

Comme $\mathscr{A}_n$ ne contient pas de lettre négative, le mot δ_n^{-1} peut jouer le rôle de la lettre $. Il existe donc un automate fini déterministe reconnaissant le miroir du mot

$$w_b\, \delta_n^{-1}\, w_{b-1}\, \delta_n^{-1} \cdots w_2\, \delta_n^{-1}\, w_1.$$

Nous obtenons ainsi que l'image miroir des mots de (2.15) constitue un langage rationnel.

Proposition 3.21. *Pour $n \geqslant 2$, le langage $R_n^{\sigma^{-1}}$ est rationnel.*

Démonstration. Le résultat est immédiat pour $n = 2$. Supposons $n \geqslant 3$. Notons W_n l'ensemble des mots comme en (2.15). Comme discuté précédemment le langage W_n est rationnel. Soit $\mathcal{B}_n$ un automate fini déterministe reconnaissant W_n et soit w un mot comme en (2.15). En suivant la section 9.2 de [58] nous pouvons modifier $\mathcal{B}_n$ pour qu'il mémorise le plus grand simple, noté tete(w), de B_n^{+*} qui divise à gauche la tresse duale $\phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1$. Comme une tresse est divisible à gauche par δ_n si et seulement si sa tete est δ_n, nous obtenons un automate fini déterministe reconnaissant le langage $\mathrm{R}_n^{\sigma^{-1}}$, en modifiant l'automate obtenu pour qu'il accepte seulement les mots w tels que tete(w) soit différent de δ_n. □

Comme l'inverse d'une tresse σ_{n-1}-positive est une tresse σ_{n-1}-négative, toute tresse d'index n admet un représentant ou bien dans $\mathrm{R}_n^{\sigma^{-1}}$ ou dans son image inverse $\mathrm{R}_n^{\sigma^+} = \{w^{-1} \,|\, w \in \mathrm{R}_n^{\sigma^{-1}}\}$. Comme $\mathrm{R}_n^{\sigma^{-1}}$ est rationnel, le langage $\mathrm{R}_n^{\sigma^+}$ l'est aussi. En introduisant les deux langages rationnels $\mathrm{R}_2^{\sigma^{-1}} = \{a_{1,2}^k \,|\, k < 0\}$ et $\mathrm{R}_2^{\sigma^+} = \{a_{1,2}^k \,|\, k > 0\}$ nous obtenons immédiatement :

Proposition 3.22. *Supposons $n \geqslant 2$. Toute tresse de B_n admet un unique représentant σ-défini appartenant à*

$$S_n^\sigma = \{\varepsilon\} \sqcup \bigsqcup_{k=2}^{n} \left(R_k^{\sigma^{-1}} \sqcup R_k^{\sigma^+} \right). \tag{2.16}$$

Comme l'union de langages rationnels forme un langage rationnel, nous obtenons :

Théorème 3.23. *Pour $n \geqslant 2$ le langage S_n^σ de représentants σ-définis des tresses de B_n est rationnel.*

Par construction les mots de S_n^σ sont des $(\mathscr{A}_n \sqcup \{\delta_n^{-1}\})$-mots. Pour n fixé, il serait intéressant de construire explicitement un automate fini déterministe reconnaissant le langage S_n^σ et ainsi obtenir la série génératrice qui lui est associée. De même nous pourrions essayer de déterminer si S_n^σ est un langage géodésique.

III. Combinatoire des tresses

Considérons une présentation $\langle \mathscr{A} \mid R \rangle^+$ d'un monoïde M. Si les relations de R préservent la longueur nous pouvons définir une longueur $\ell_M^{\mathscr{A}}$ sur M à partir de celle des $\mathscr{A}$-mots : la longueur d'un élément x de M est alors $\ell_M^{\mathscr{A}}(x) = |u|$ où $|.|$ désigne la longueur des mots et u est un $\mathscr{A}$-mot quelconque représentant x.

Cette construction n'est plus légitime lorsque les relations de R ne préservent pas la longueur. Par exemple dans le monoïde introduit à l'exemple 1.12 du chapitre I, qui est présenté à l'aide de l'unique relation $ab = a$, l'élément $\overline{a}$ peut être représenté par les mots $a, ab, abb, \ldots$ qui sont tous de longueurs différentes.

Définition. Soit M un monoïde et $\mathscr{A}$ une partie génératrice de M. Pour tout $x \in M$ la *$\mathscr{A}$-longueur géodésique* de x, notée $\ell_M^{\mathscr{A}}$, est la longueur d'un des $\mathscr{A}$-mots les plus courts représentant x.

Se pose alors la question de déterminer la longueur géodésique d'un élément de M. Si M est donné par une présentation finie $\langle \mathscr{A} \mid R \rangle^+$ pour laquelle on sait résoudre le problème du mot alors nous pouvons calculer la $\mathscr{A}$-longueur géodésique de M. En effet si un élément x de M est donné par un mot w il suffit de déterminer le sous-ensemble des mots équivalents à w parmi tous les $\mathscr{A}$-mots de longueur au plus $|w|$.

En 1991, M. S. Paterson et A. A. Razborov donnent le résultat suivant

Théorème (M. S. Paterson et A. A. Razborov [102])**.** *Soit w un $\mathscr{S}_n^{\pm}$-mot. Déterminer la $\mathscr{S}_n^{\pm}$-longueur géodésique de la tresse $\overline{w}$ est un problème co-NP-complet en $n + |w|$.*

C'est donc sans surprise que nos connaissances sur la $\mathscr{S}_n^{\pm}$-longueur géodésique du groupe des tresses B_n soient limitées. La réalité est qu'à part pour $n = 2$ (qui est trivial car isomorphe à $\mathbb{Z}$) et $n = 3$, nous ne savons rien. En 2004, L. Sabalka obtient le résultat suivant :

Théorème (L. Sabalka [117])**.** *Le langage des $\mathscr{S}_3^{\pm}$-mots géodésiques est rationnel et la série génératrice de B_3 relativement à la $\mathscr{S}_3^{\pm}$-longueur géodésique est*

$$\frac{2t^4 + t^3 - 1}{(2t^3 + t^2 - 3t + 1)(t - 1)}.$$

Deux ans plus tard, J. Mairesse et F. Mathéus [92] redémontrent de manière indépendante le résultat de L. Sabalka et déterminent la vitesse de fuite d'une marche aléatoire sur le groupe des tresses B_3 relativement aux générateurs $\mathscr{S}_3^{\pm}$.

Contrairement au cas du groupe des tresses B_n, déterminer la $\mathscr{S}_n$-longueur géodésique d'une tresse β de B_n^+ est trivial car c'est la longueur de n'importe quel $\mathscr{S}_n$-mot représentant la tresse β. En 2001, A. Bronfman obtient le résultat suivant :

Théorème (A. Bronfman [16]). *La série génératrice de B_n^+ relativement à la $\mathscr{S}_n$-longueur est*

$$P_n(t) = \sum_{i=1}^{n} (-1)^{i+1} t^{\frac{i(i-1)}{2}} P_{n-i}(t)$$

en posant $P_0(t) = P_1(t) = 1$.

Ce résultat a été redémontré et étendu aux monoïdes des tresses de type **B** et **D** ainsi qu'aux monoïdes des tresses duaux de type **A** et **B** par M. Albenque et P. Nadeau en 2009 dans [1]. Le monoïde des tresses duales de type **A** aussi appelé monoïde de Birman–Ko–Lee est introduit au chapitre 2.

Dans ce chapitre nous allons nous intéresser à la combinatoire des monoïdes des tresses généralisées vis-à-vis de leur structure de Garside décrite à la sous-section 2.3 du chapitre I. Typiquement, si $\mathbf{\Gamma}$ est un diagramme de Dynkin de type sphérique et de sommets $\mathscr{S}$, alors les tresses de $B_{\mathbf{\Gamma}}^+$ ne seront pas comptées en fonction de leur $\mathscr{S}$-longueur comme fait jusque maintenant mais en fonction du nombre de termes dans leur forme normale de Garside.

Le chapitre est organisé de la façon suivante. À la section 1 nous décrivons la combinatoire des suites normales pour n'importe quel monoïde de Garside M à l'aide d'une matrice d'adjacence Adj_M. En particulier nous énoncerons une conjecture formulée par P. Dehornoy dans [30] portant sur la divisibilité de polynômes caractéristiques lorsque M est le monoïde des tresses positives. Nous décrirons brièvement comment cette conjecture a été prouvée par F. Hivert, J. C. Novelli et J. Y. Thibon dans [81]. La deuxième section est consacrée à l'étude des groupes de permutations signées et de leur identification avec le groupe de Coxeter de type **B**. Dans la troisième section nous introduisons l'algèbre de Hopf **BFQSym** sur les permutations signées. En exploitant les propriétés de **BFQSym** nous établissons, à la section 4, un résultat de divisibilité entre polynômes caractéristiques de matrices d'adjacence associée à la combinatoire des suites normales du monoïde de Garside $B_{\mathbf{B_n}}^+$. Des informations sur la combinatoire des suites normales pour les monoïdes d'Artin–Tits des autres types sphériques sont données dans la dernière section.

1 Introduction

Commençons par définir la longueur de Garside des éléments d'un monoïde de Garside quelconque.

1.1 Longueur de Garside

Définition 1.1. Soit (M, Δ) un monoïde de Garside. La *longueur de Garside* d'un élément x de M, notée $\ell_{M,\Delta}(x)$, est le plus petit $p \in \mathbb{N}$ tel que x s'écrive

$$x = s_1 \cdot s_2 \cdot \ldots \cdot s_p,$$

où les s_i sont des simples de M, c'est-à-dire, des diviseurs de Δ.

Par le corollaire 3.5 du chapitre I, nous savons que $\ell_{M,\Delta}(x)$ est fini pour tout x de M. En fait nous pouvons assez facilement montrer :

Proposition 1.2 (Proposition III.3.1 de [35])**.** *Soit (M, Δ) un monoïde de Garside. Pour tout x de M, la longueur de Garside de x est le nombre de simples intervenant dans la forme normale de Garside de x.*

Notation 1.3. Soit (M, Δ) un monoïde de Garside. Pour tout d on note $b_{M,d}$ le nombre d'éléments de M de longueur de Garside d.

Le seul élément de M ayant une longueur de Garside nulle est 1, qui est représenté par un produit vide de simples. De même $b_{M,1}$ est le nombre de simples non triviaux de M. Nous avons donc

$$b_{M,0} = 1 \quad \text{et} \quad b_{M,1} = \operatorname{card}(\{\text{simples de } M\}) - 1.$$

1.2 Suites normales

Définition 1.4. Soit (M, Δ) un monoïde de Garside. Une suite $(s_1, \dots, s_p)$ de simples de M est dite *normale* si elle vérifie les conditions du corollaire 3.5 du chapitre I.

Exemple 1.5. Pour tout simple s non trivial d'un monoïde de Garside (M, Δ), la suite (s) est normale. La cas du simple trivial est particulier car la suite normale qui lui est associée est la suite vide ().

Une conséquence immédiate de la proposition 1.2 est que le nombre $b_{M,d}$ d'éléments de M de longueur de Garside d correspond aux nombres de suites normales de M de longueur d :

Corollaire 1.6. *Pour tout monoïde de Garside (M, Δ) et tout $d \in \mathbb{N}$, nous avons*

$$b_{M,d} = \operatorname{card}(\{\textit{suites normales } (s_1, \dots, s_d) \textit{ de } M\}).$$

Comme l'établit le lemme suivant, une suite normale ne peut pas contenir de tresse triviale.

Lemme 1.7. *Pour toute suite normale $(s_1, \dots, s_p)$ d'un monoïde de Garside (M, Δ) nous avons $s_i \neq 1$.*

Démonstration. Supposons que l'un des s_i soit trivial. Soit k le plus grand entier tel que s_k soit trivial. Par le corollaire 3.5 du chapitre I on a nécessairement $k \neq p$. La condition 1.6 implique alors $s_k = \operatorname{pgcd}_g(s_k s_{k+1}, \Delta)$. Comme la tresse $s_k s_{k+1} = s_{k+1}$ est simple nous obtenons $\operatorname{pgcd}_g(s_k s_{k+1}, \Delta) = s_{k+1}$ puis $s_{k+1} = s_k$. La tresse s_{k+1} est donc triviale, ce qui est impossible par construction de k. □

La condition (1.6) demandée par le corollaire 3.5 du chapitre I est une condition locale qui justifie d'introduire la définition suivante.

Définition 1.8. Soient s et t deux simples d'un monoïde de Garside (M, Δ). La paire (s, t) est dite *en position normale* si la relation $\operatorname{pgcd}_g(s\,t, \Delta) = s$ est vérifié.

Remarquons que pour tout simple s, la paire $(s, 1)$ est en position normale mais n'est pas une suite normale. Pour qu'une paire (s, t) en position normale soit une suite normale il faut et il suffit que t soit différent de 1.

Le corollaire 3.5 du chapitre I et le lemme 1.7 donnent immédiatement le résultat suivant.

Corollaire 1.9. *Soit (M, Δ) un monoïde de Garside. Une suite $(s_1, \dots, s_p)$ de simples de M avec $s_p \neq 1$ est normale si et seulement si la paire (s_i, s_{i+1}) est en position normale pour tout $i \in [1, p-1]$.*

1.3 Une matrice d'adjacence

Le nombre $b_{M,d}$ de suites normales de longueur d peut ainsi être entièrement déterminé par la connaissance des paires en position normales de (M, Δ).

Définition 1.10. Pour tout monoïde de Garside (M, Δ) nous définissons une matrice d'adjacence $\mathrm{Adj}_M = (a_{s,t})$ indexées par les simples de M en posant :

$$a_{s,t} = \begin{cases} 1 & \text{si } (s,t) \text{ est en position normale,} \\ 0 & \text{sinon.} \end{cases}$$

La matrice Adj_M peut aussi être vue comme la matrice d'adjacence d'un graphe G orienté dont les sommets sont les simples de (M, Δ) et tel que G contient une arête de s vers t si et seulement si la paire (s, t) est en position normale. Toute suite normale de (M, Δ) de longueur d correspond ainsi à un chemin de longueur d du graphe G partant et menant à des sommets différents de 1.

Voyons maintenant comment la donnée de Adj_M nous permet de déterminer $b_{M,\ell}$ pour tout $\ell \in \mathbb{N}$. Un résultat standard en théorie des graphes (voir chapitre I de [7] par exemple) donne :

Proposition 1.11. *Soient (M, Δ) un monoïde de Garside et s, t deux simples de (M, Δ) avec $s \neq 1$ et $t \neq 1$ Pour tout $d \geqslant 1$, le nombre de suites normales $(s_1, \ldots, s_d)$ avec $s_1 = s$ et $s_d = t$ est :*

$$b_{M,d}(s,t) = {}^t s \cdot \mathrm{Adj}_M^{d-1} \cdot t.$$

Comme une suite normale ne peut ni commencer ni finir par le simple 1, nous obtenons le résultat suivant.

Proposition 1.12. *Pour tout monoïde de Garside (M, Δ) et tout entier $d \geqslant 1$, nous avons*

$$b_{M,d} = {}^t X \, \mathrm{Adj}_M^{d-1} \, X, \quad \text{où } X_s = \begin{cases} 0 & \text{si } s = 1 \\ 1 & \text{sinon.} \end{cases}$$

Démonstration. Soit $d \geqslant 1$. Par le lemme 1.7, $b_{M,d}$ est le nombre de suites normales $(s_1, \ldots, s_d)$ vérifiant $s_1 \neq 1$ et $s_d \neq 1$. Nous obtenons ainsi :

$$b_{M,d} = \sum_{\substack{s,\, t \text{ simples non} \\ \text{triviaux de } M}} b_{M,d}(s,t).$$

qui est égal, par la proposition 1.11, nous avons :

$$b_{M,d} = \sum_{\substack{s,\, t \text{ simples non} \\ \text{triviaux de } M}} {}^t s \cdot \mathrm{Adj}_M^{d-1} \cdot t = {}^t X \, \mathrm{Adj}_M^{d-1} \, X.$$

□

Corollaire 1.13. *Soit (M, Δ) un monoïde de Garside. La série génératrice de M par rapport à $\ell_{M,\Delta}$ est :*

$$\sum_{d \in \mathbb{N}} b_{M,d} t^d = 1 + t \cdot {}^t X (I - t \, \mathrm{Adj}_M)^{-1} X,$$

qui est rationnelle.

Exemple 1.14. Les simples de B_3^+ sont $1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1$ et $\Delta_3 = \sigma_1\sigma_2\sigma_1$. Par calcul direct utilisant l'énumération des simples donnée, nous obtenons

$$\mathrm{Adj}_{B_3^+} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{et} \quad X = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

À l'aide d'un logiciel de calcul formel tel que **Sage** [124] nous obtenons

$$\begin{aligned} \sum_{d\in\mathbb{N}} b_{B_3^+,d} t^d &= 1 + t\frac{-2t+5}{(2t-1)(t-1)} = \frac{2t+1}{(2t-1)(t-1)} = \sum_{d\in\mathbb{N}} (2^{d+2}-3)t^d \\ &= 1 + 5t + 13t^2 + 29t^3 + 61t^4 + 125t^5 + 253t^6 + 509t^7 + \dots \end{aligned}$$

Le groupe des tresses B_3 admet un autre monoïde de Garside : le monoïde des tresses duales B_3^{+*}. Les simples de ce monoïde sont $1, a_{1,2}, a_{2,3}, a_{1,3}$ et

$$\delta_3 = a_{1,2}a_{2,3} = a_{2,3}a_{1,3} = a_{1,3}a_{1,2}.$$

Avec cette énumération des simples, nous obtenons :

$$\mathrm{Adj}_{B_3^{+*}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix},$$

ce qui en utilisant le corollaire 1.13 donne :

$$\begin{aligned} \sum_{d\in\mathbb{N}} b_{B_3^{+*},d} t^d &= 1 + t\frac{-2t+4}{(2t-1)(t-1)} = \frac{t+1}{(2t-1)(t-1)} = \sum_{d\in\mathbb{N}} (3\cdot 2^d - 2)\, t^d \\ &= 1 + 4\,t + 10\,t^2 + 22\,t^3 + 46\,t^4 + 94\,t^5 + 190\,t^6 + 382\,t^7 + \dots \end{aligned}$$

Dans [5], P. Biane et P. Dehornoy ramènent la détermination de $b_{B_n^{+*},2}$ à un calcul de cumulants libres pour un produit de variables aléatoires indépendantes pour lesquels ils donnent des formules.

1.4 Cas des groupes de Garside

Soit (M, Δ) un monoïde de Garside et G le groupe des fractions de M. La proposition 3.4 associe à chaque élément de G une unique forme normale de Garside. Si $\Delta^k \cdot s_1 \cdot \ldots \cdot s_p$ est la forme normale de Garside de $\beta \in B$, nous posons $\ell_{G,\Delta}(\beta) = k + p$. En 1992, W. P. Thurston établit dans [58] que la forme normale de Garside est bi-automatique pour le groupe des tresses B_n, impliquant que la série génératrice associée à $\ell_{B_n,\Delta}$ est rationnelle. Ce résultat a été généralisé pour tous les groupes d'Artin–Tits de type sphérique par R. Charney en 1992 dans [21]. Le défaut de la longueur $\ell_{G,\Delta}$ est qu'elle utilise l'alphabet

$$\{\text{simples non triviaux de } M\} \sqcup \{\Delta^{-1}\},$$

qui n'est pas stable par inverse.

Dans [58], W. P. Thurston introduit la version symétrique de la forme normale de Garside, aussi connue sous le nom de *forme normale de Thurston*.

Proposition 1.15. *Soit (M, Δ) un monoïde de Garside. Tout élément β de G admet une décomposition unique de la forme $\beta = t_q^{-1} \cdot \ldots \cdot t_1^{-1} \cdot s_1 \cdot \ldots \cdot s_p$, où $(s_1, \ldots, s_p)$ et $(t_1, \ldots, t_q)$ sont deux suites normales de M vérifiant* $\mathrm{pgcd}_g(s_1, t_1) = 1$.

En reprenant les notations de la proposition précédente, nous définissons une longueur sur G en notant $\ell^{\mathrm{Sym}}_{G,\Delta}(\beta)$ l'entier $p + q$ pour tout $\beta \in G$. La longueur $\ell^{\mathrm{Sym}}_{G,\Delta}$ correspond à une longueur géodésique pour l'alphabet

$$\{\text{simples non triviaux de } M\} \sqcup \{\text{inverses des simples non triviaux de } M\},$$

qui est stable par inverse. En 1995, R. Charney a montré dans [22] que la forme normale de Thurston munit tout groupe d'Artin–Tits de type sphérique d'une structure bi-automatique. Elle en déduit en particulier que la série génératrice associée à $\ell^{\mathrm{Sym}}_{G,\Delta}$ est rationnelle pour tout groupe d'Artin–Tits de type sphérique G. En 2002, P. Dehornoy a établi [29] que tout groupe de Garside peut être munis d'une structure bi-automatique.

1.5 Cas des monoïde d'Artin–Tits

Afin d'alléger les notations, nous introduisons les notations suivantes.

Notation 1.16. Soit $\mathbf{\Gamma}$ un diagramme de Dynkin de type sphérique. Nous notons $\mathrm{Adj}^+_{\mathbf{\Gamma}}$ la matrice $\mathrm{Adj}_{B^+_{\mathbf{\Gamma}}}$ et $b^+_{\mathbf{\Gamma},d}$ le nombre $b_{B^+_{\mathbf{\Gamma}},d}$.

Par le corollaire 1.13, le taux de croissance de la suite $(b^+_{\mathbf{\Gamma},d})_d$ est le rayon spectral de la matrice $\mathrm{Adj}^+_{\mathbf{\Gamma}}$ qui peut être obtenu à partir du polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{\Gamma}}$.

Notation 1.17. Soit $\mathbf{\Gamma}$ un diagramme de Dynkin de type sphérique. Nous notons $\chi_{\mathbf{\Gamma}}$ le polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{\Gamma}}$.

En 2005, P. Dehornoy étudie dans [30] la suite $(b^+_{\mathbf{A_n},d})$ à l'aide de son polynôme caractéristique $\chi_{\mathbf{A_n}}$ et conjecture que le polynôme caractéristique $\chi_{\mathbf{A_n}}$ divise $\chi_{\mathbf{A_{n+1}}}$. Cette conjecture a été démontrée par F. Hivert, J. C. Novelli et J. Y. Thibon en 2008 dans [81]. Pour cela ils interprètent la matrice d'adjacence $\mathrm{Adj}^+_{\mathbf{A_n}}$ comme la matrice d'un endomorphisme $\Phi_{\mathbf{A_n}}$ de l'algèbre de Hopf de Malvenuto-Reutenauer **FQSym** [93, 46], qui est une algèbre de Hopf connexe graduée dont la base en degré n est indexée par les éléments du groupe symétrique $\mathfrak{S}_n$, qui est isomorphe à $W_{\mathbf{A_{n-1}}}$. Ils construisent alors une dérivation surjective ∂ de degré -1 satisfaisant la relation $\partial \circ \Phi_{\mathbf{A_n}} = \Phi_{\mathbf{A_{n-1}}} \circ \partial$ puis établissent le résultat de divisibilité. Une description combinatoire de $\mathrm{Adj}^+_{\mathbf{A_n}}$ est disponible dans [30] et dans [74] avec une approche plus algorithmique.

2 Monoïde d'Artin–Tits de type B.

2.1 Permutations signées

Définition 2.1. Une *permutation signée* de rang n est une permutation σ de $[-n, n]$ satisfaisant $\sigma(-i) = -\sigma(i)$ pour tout $i \in [-n, n]$. Nous notons $\mathfrak{S}^{\pm}_n$ le *groupe des permutations signées*.

Dans la littérature, le groupe des permutations signées $\mathfrak{S}_n^{\pm}$ est aussi connu sous le nom de groupe hyperoctaédrique de rang n. Remarquons, que par définition, toute permutation signée envoie 0 sur lui-même. Ainsi une permutation signée est entièrement déterminée par ses valeurs sur $[1, n]$.

Définition 2.2. Soit σ une permutation de rang n. Le n-uplet $(\sigma(1), \ldots, \sigma(n))$, est la *notation fenêtrée* de la permutation σ.

Exemple 2.3. Les permutations signées de rang 2 sont

$$\mathfrak{S}_2^{\pm} = \{(1,2), (-1,2), (1,-2), (-1,-2), (2,1), (-2,1), (2,-1), (-2,-1)\}.$$

Nous pouvons remarquer que pour toute permutation signée σ de $\mathfrak{S}_n^{\pm}$, l'application $|\sigma|$ définie sur $[1, n]$ par $|\sigma|(i) = |\sigma(i)|$ est une permutation de $\mathfrak{S}_n$.

2.2 Groupe de Coxeter de type B

Parmi toutes les permutations signées, nous isolons une famille génératrice de permutations s_i qui muniront $\mathfrak{S}_n^{\pm}$ d'une structure de Coxeter.

Notation 2.4. Pour $n \geqslant 1$ et $i \in [0, n]$ nous notons s_i la permutation signée définie par

$$s_i = \begin{cases} (-1, 2, \ldots, n) & \text{pour } i = 0, \\ (1, \ldots, i+1, i, \ldots, n) & \text{sinon.} \end{cases}$$

et on pose $\mathscr{S}_{\mathbf{B_n}} = \{s_0, s_1, \ldots, s_n\}$.

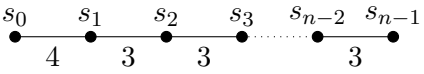
Proposition 2.5 (Proposition 8.1.3 de [9])**.** *Pour tout $n \geqslant 1$, les permutations $\mathscr{S}_{\mathbf{B_n}}$ sont soumises aux relations :*

- R_1 *: $s_i^2 = 1$ pour tout $i \in [0, n]$;*
- R_2 *: $s_0\, s_1\, s_0\, s_1 = s_1\, s_0\, s_1\, s_0$;*
- R_3 *: $s_i\, s_j = s_j\, s_i$ pour $i, j \in [0, n]$ avec $|i - j| \geqslant 2$;*
- R_4 *: $s_i\, s_j\, s_i = s_j\, s_i\, s_j$ pour $1 \leqslant i, j \leqslant n$ avec $|i - j| = 1$.*

De plus nous avons

$$\mathfrak{S}_n^{\pm} \simeq W_{\mathbf{B_n}} = \langle \mathscr{S}_{\mathbf{B_n}} \,|\, R_1, R_2, R_3, R_4 \rangle\,.$$

Nous rappelons que le diagramme de Dynkin $\mathbf{B_n}$ relativement aux générateurs $\mathscr{S}_{\mathbf{B_n}}$ est donné par



À partir de maintenant nous identifierons le groupe de Coxeter $W_{\mathbf{B}_n}$ avec le groupe des permutations signées $\mathfrak{S}_n^{\pm}$.

Exemple 2.6. Les permutations de $\mathfrak{S}_3^{\pm}$ admettent les décompositions suivantes comme produit de permutations de $\mathscr{S}_{\mathbf{B_2}}$:

$$\begin{aligned} (1,2) &= \emptyset, & (2,1) &= s_1, \\ (-1,2) &= s_0, & (-2,1) &= s_1 \cdot s_0, \\ (1,-2) &= s_1 \cdot s_0 \cdot s_1, & (2,-1) &= s_0 \cdot s_1, \\ (-1,-2) &= s_0 \cdot s_1 \cdot s_0 \cdot s_1, & (-2,-1) &= s_0 \cdot s_1 \cdot s_0. \end{aligned}$$

Toutes les expressions sont réduites. En particulier, la longueur de $(-1,-2)$ est 4, tandis que celle de $(-2,1)$ est 2.

Lemme 2.7 (Proposition 8.1.1 de [9]). *L'élément de Coxeter de $W_{\mathbf{B_n}}$ est*

$$w_{\mathbf{B_n}} = (-1,\dots,-n).$$

2.3 Suites normales et descentes

Nous rappelons que chaque tresse simple de $B^+_{\mathbf{B}_n}$ peut être exprimée de manière unique comme $r(\sigma)$, où σ est une permutation signée et r est l'application donnée à la définition 3.11 du chapitre I. À partir de la définition de paire en position normale de simples nous obtenons la notion de paire en position normale de permutations signées.

Définition 2.8. Une paire de permutations signées (σ,τ) est dite en *position normale* si et seulement si la paire de simples $(r(\sigma), r(\tau))$ l'est.

Cherchons maintenant un critère pour reconnaître si une paire de permutations signées est en position normale.

Définition 2.9. L'*ensemble des descentes* d'une permutation $\sigma \in \mathfrak{S}^{\pm}_n$ est défini par

$$\mathrm{Des}\,(\sigma) = \{i \in [0,n-1] \mid \ell(\sigma\, s_i) < \ell(\sigma)\}.$$

Exemple 2.10. Calculons l'ensemble des descentes de $\sigma = (-2,1)$. Une expression réduite de σ est $s_1\, s_0$ et donc σ est de longueur 2. L'expression $\sigma\, s_0 = s_1\, s_0\, s_0$ se réduit en s_1, qui est de longueur 1. L'expression $\sigma\, s_1 = s_1\, s_0\, s_1$ est réduite, et donc $\sigma\, s_1$ est de longueur 3. Ainsi l'ensemble des descentes de σ est $\mathrm{Des}\,(\sigma) = \{0\}$.

Lemme 2.11. *Pour toute permutation signée σ de $\mathfrak{S}^{\pm}_n$ et tout entier $i \in [0,n-1]$, la tresse $r(\sigma)r(s_i)$ est simple si et seulement si $i \notin \mathrm{Des}\,(\sigma)$.*

Démonstration. Soit σ une permutation signée de $\mathfrak{S}^{\pm}_n$ et $x_1 \cdots x_{\ell(\sigma)}$ une de ses expressions réduites. Si l'entier i n'appartient pas à $\mathrm{Des}\,(\sigma)$ alors nous avons $\ell(\sigma s_i) > \ell(\sigma)$ et donc $x_1 \cdots x_{\ell(\sigma)}\, s_i$ est une expression réduite de σs_i. Nous obtenons

$$r(\sigma s_i) = r(x_1 \cdots x_{\ell(\sigma)}) r(s_i),$$

et donc $r(\sigma)r(s_i)$ est simple car image de r. Réciproquement, supposons que $r(\sigma)r(s_i)$ soit simple. Il existe alors une permutation signée τ de longueur $\ell(\sigma)+1$ telle que nous ayons $\pi(r(\sigma)r(s_i)) = \tau$. Comme $\pi(r(\sigma)r(s_i))$ vaut σs_i, nous devons avoir $\ell(\sigma s_i) = \ell(\sigma)+1$ et donc i n'appartient pas à $\mathrm{Des}\,(\sigma)$. □

Lemme 2.12. *Pour toute permutation signée τ de $\mathfrak{S}^{\pm}_n$ et tout entier i de $[0,n-1]$, la tresse $r(s_i)$ est un diviseur à gauche de $r(\tau)$ si et seulement si $i \in \mathrm{Des}\,(\tau^{-1})$.*

Démonstration. Les tresses $r(s_i)$ et $r(\tau)$ sont simples. L'isomorphisme entre les treillis $(r(B^+_{\mathbf{B_n}}), \preccurlyeq)$ et $(\mathfrak{S}^{\pm}_n, \preccurlyeq_{\mathbf{B_n}})$, établi à la proposition 3.15 du chapitre I, montre que la tresse $r(s_i)$ est un diviseur à gauche de $r(\tau)$ si et seulement si la relation $s_i \preccurlyeq_{\mathbf{B_n}} \tau$ est satisfaite. Ainsi, par définition de $\preccurlyeq$, la tresse $r(s_i)$ est un diviseur à gauche de $r(\tau)$ si et seulement si nous avons $\ell(\tau) = \ell(s_i) + \ell(s_i\tau)$. Cette dernière relation est équivalente à $\ell(s_i\tau) < \ell(\tau)$ car nous avons nécessairement $\ell(s_i\tau) = \ell(\tau) \pm 1$. Comme la longueur d'une permutation est égale à la longueur de son inverse, nous avons $\ell(s_i\tau) < \ell(\tau) \Leftrightarrow \ell(\tau^{-1}s_i) < \ell(\tau^{-1})$ qui est équivalent à $i \in \mathrm{Des}\,(\tau^{-1})$. □

Proposition 2.13. *Une paire (σ,τ) de permutations signées de $\mathfrak{S}^{\pm}_n$ est en position normale si et seulement si l'inclusion $\mathrm{Des}\,(\tau^{-1}) \subseteq \mathrm{Des}\,(\sigma)$ est vérifiée.*

Démonstration. Soient σ et τ deux permutations signées de $\mathfrak{S}_n^{\pm}$. Supposons que la paire (σ, τ) ne soit pas en position normale. Il existe alors un multiple à droite propre z de $r(\sigma)$ qui divise à gauche $r(\sigma)r(\tau)$. En particulier, il existe $i \in [0, n]$ telle que $r(\sigma)r(s_i)$ soit simple, et telle que $r(s_i)$ divise à gauche $r(\tau)$. En notant x la tresse simple $r(\sigma)r(s_i)$ et par y la tresse positive $r(s_i)^{-1}r(\tau)$, nous obtenons $r(\sigma)r(\tau) = x\,y$. Par le lemme 2.11, l'entier i n'appartient pas à $\mathrm{Des}\,(\sigma)$, mais appartient à $\mathrm{Des}\,(\tau^{-1})$.

Nous avons ainsi montré que la paire (σ, τ) n'est pas en position normale s'il existe $i \in [0, n]$ tel qu'on ait $i \notin \mathrm{Des}\,(\sigma)$ et $i \in \mathrm{Des}\,(\tau^{-1})$. L'implication réciproque est immédiate. La paire (σ, τ) est donc en position normale si et seulement si pour tout $i \in [0, n]$, nous avons soit $i \in \mathrm{Des}\,(\sigma)$ soit $i \notin \mathrm{Des}\,(\tau^{-1})$. Comme i appartient ou n'appartient pas à $\mathrm{Des}\,(\tau^{-1})$, nous obtenons que la paire (σ, τ) est en position normale si et seulement si nous avons $\mathrm{Des}\,(\tau^{-1}) \subseteq \mathrm{Des}\,(\sigma)$. □

L'ensemble des descentes d'une permutation signée σ peut être construit directement à partir de la notation fenêtrée.

Proposition 2.14 (Proposition 8.1.2 de [9])**.** *Pour $n \geqslant 1$, $\sigma \in \mathfrak{S}_n^{\pm}$ et $i \in [0, n-1]$ nous avons $i \in \mathrm{Des}\,(\sigma)$ si et seulement si $\sigma(i) > \sigma(i+1)$.*

2.4 Matrice d'adjacence

La caractérisation des paires de simples de $B^+_{\mathbf{B_n}}$ donne immédiatement la caractérisation suivante de la matrice d'adjacence $\mathrm{Adj}^+_{\mathbf{B_n}}$ (définition 1.10).

Corollaire 2.15. *Pour $n \geqslant 1$, la matrice $\mathrm{Adj}^+_{\mathbf{B_n}} = (a_{r(\sigma),r(\tau)})$ est donnée par*

$$a_{r(\sigma),r(\tau)} = \begin{cases} 1 & \text{si } \mathrm{Des}\,(\tau^{-1}) \subseteq \mathrm{Des}\,(\sigma), \\ 0 & \text{sinon.} \end{cases}$$

Exemple 2.16. Il y a exactement 8 permutations signées dans $\mathfrak{S}_2^{\pm}$. Dans la table suivante, nous donnons des informations sur leurs inverses ainsi que sur leur ensemble de descentes.

σ	σ^{-1}	$\mathrm{Des}\,(\sigma)$	$\mathrm{Des}\,(\sigma^{-1})$
$(1,2)$	$(1,2)$	$\emptyset$	$\emptyset$
$(1,-2)$	$(1,-2)$	$\{1\}$	$\{1\}$
$(-1,2)$	$(-1,2)$	$\{0\}$	$\{0\}$
$(-1,-2)$	$(-1,-2)$	$\{0,1\}$	$\{0,1\}$
$(2,1)$	$(2,1)$	$\{1\}$	$\{1\}$
$(2,-1)$	$(-2,1)$	$\{1\}$	$\{0\}$
$(-2,1)$	$(2,-1)$	$\{0\}$	$\{1\}$
$(-2,-1)$	$(-2,-1)$	$\{0\}$	$\{0\}$

Avec l'énumération des éléments de $\mathfrak{S}_2^{\pm}$ ci-dessus, nous obtenons :

$$\mathrm{Adj}^+_{\mathbf{B_2}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Exemple 2.17. Dans $B^+_{\mathbf{B_2}}$, la seule tresse de longueur de longueur de Garside 0 est la tresse triviale, c'est-à-dire, $b^+_{\mathbf{B_2},0} = 1$. À l'exception de la tresse triviale, toutes les tresses

simples sont de longueur de Garside 1, et donc $b^+_{\mathbf{B_2},1} = 7$, correspondant à ${}^tXX$. En considérant la matrice $\mathrm{Adj}^+_{\mathbf{B_n}}$ nous obtenons les valeurs suivantes pour $b^+_{\mathbf{B_n},d}$:

d	$b^+_{\mathbf{B_2},d}$	$b^+_{\mathbf{B_3},d}$	$b^+_{\mathbf{B_4},d}$
0	1	1	1
1	7	47	383
2	25	771	35 841
3	79	10 413	2 686 591
4	241	134 581	193 501 825
5	727	1 721 467	13 837 222 655

La série génératrice $F^+_{\mathbf{B}_n}(t) = \sum_{d=0}^{+\infty} b^+_{\mathbf{B_n},d} t^d$ est donnée par ${}^tX\left(\mathrm{I} - t\,\mathrm{Adj}^+_{B_2}\right)^{-1} X$:

$$F^+_{\mathbf{B}_2}(t) = \frac{7-3t}{(3t-1)(t-1)},$$
$$F^+_{\mathbf{B}_3}(t) = \frac{-60t^4+149t^3-163t^2+169t-47}{(t-1)(3t-1)(20t^3-43t^2+16t-1)}.$$

En développant $F^+_{\mathbf{B}_2}(t)$, nous obtenons $b^+_{\mathbf{B_2},d} = 3^{d+1} - 2$.

Les valeurs propres de la matrice $\mathrm{Adj}^+_{\mathbf{B_n}}$ donnent des informations sur le taux de croissance de la suite $(b^+_{\mathbf{B_n},d})_d$. Nous pouvons, par exemple, déterminer si les valeurs propres de $\mathrm{Adj}^+_{\mathbf{B_n}}$ sont aussi des valeurs propres de $\mathrm{Adj}^+_{\mathbf{B_{n+1}}}$, c'est-à-dire, déterminer si le polynôme caractéristique $\chi_{\mathbf{B_n}}$ de la matrice $\mathrm{Adj}^+_{\mathbf{B_n}}$ divise celui de la matrice $\mathrm{Adj}^+_{\mathbf{B_{n+1}}}$.

Exemple 2.18. Nous avons

$$\begin{aligned}
\chi_{\mathbf{B}_1}(x) &= (x-1)^2,\\
\chi_{\mathbf{B}_2}(x) &= \chi_{\mathbf{B}_1}(x)\ x^4\ (x-1)\ (x-3),\\
\chi_{\mathbf{B}_3}(x) &= \chi_{\mathbf{B}_2}(x)\ x^{37}\ (x^3-16x^2+43x-20),\\
\chi_{\mathbf{B}_4}(x) &= \chi_{\mathbf{B}_3}(x)\ x^{329}\ (x-1)^3\ (x^4-85x^3+1003x^2-2291x+1260),\\
\chi_{\mathbf{B}_5}(x) &= \chi_{\mathbf{B}_4}(x)\ x^{3449}\ (x^7-574x^6+39344x^5-576174x^4+\\
&\qquad 3027663x^3-5949972x^2+4281984x-1088640).
\end{aligned}$$

Nous constatons que le polynôme $\chi_{\mathbf{B}_i}$ divise $\chi_{\mathbf{B}_{i+1}}$ pour $i \in \{1,2,3,4\}$.

Les deux prochaines sections ont pour but de démontrer le résultat suivant que nous avons établi avec L. Foissy dans [62].

Théorème 2.19. *Pour tout $n \in \mathbb{N}$, le polynôme caractéristique de la matrice $\mathrm{Adj}^+_{\mathbf{B_n}}$ divise le polynôme caractéristique de la matrice $\mathrm{Adj}^+_{\mathbf{B_{n+1}}}$.*

3 L'algèbre de Hopf BFQSym

Dans cette section nous décrivons un analogue de l'algèbre de Hopf **FQSym** pour le groupe des permutations signées $\mathfrak{S}^\pm_n$. Assez peu de connaissances sur les algèbres de Hopf sont nécessaires pour comprendre la suite de ce chapitre. Cependant le lecteur souhaitant une introduction aux algèbres de Hopf combinatoires pourra par exemple consulter les notes de L. Foissy [61].

Notation 3.1. Notons $\mathbb{Q}\mathfrak{S}_n^{\pm}$ le $\mathbb{Q}$-espace vectoriel de base $\mathfrak{S}_n^{\pm}$ et notons $\mathbb{Q}\mathfrak{S}^{\pm}$ le $\mathbb{Q}$-espace vectoriel $\bigoplus_{n=1}^{+\infty} \mathbb{Q}\mathfrak{S}_n^{\pm}$.

Les permutations de $\mathfrak{S}_n^{\pm}$ sont alors des vecteurs de $\mathbb{Q}\mathfrak{S}_n^{\pm}$. De cette façon, les expressions 2σ et $\sigma + \tau$ prennent sens pour des permutations signées σ et τ.

3.1 Les mots de permutations signées

Nous avons vu à la section 2 qu'une permutation signée peut être entièrement décrite par sa notation fenêtrée. Afin d'avoir une définition simple des notations attachées à la construction de l'algèbre de Hopf **BFQSym**, nous décrivons une bijection entre les permutations signées et certains mots associés à la notation fenêtrée.

Notation 3.2. Pour $n \geqslant 1$, nous notons $W_n^{\pm}$ l'ensemble des mots $w = w_1 \cdots w_n$ sur l'alphabet $[-n, n] \setminus \{0\}$ satisfaisant la relation $\{|w_1|, \ldots, |w_n|\} = [1, n]$.

Si w est un mot de $W_n^{\pm}$, alors $(w_1, \ldots, w_n)$ est la notation fenêtrée d'une certaine permutation signée $\mathfrak{S}_n^{\pm}$.

Définition 3.3. Pour $n \geqslant 1$, nous définissons deux applications $w : \mathfrak{S}_n^{\pm} \to W_n^{\pm}$ et $\rho : W_n^{\pm} \to \mathfrak{S}_n^{\pm}$ par $w(\sigma) = \sigma(1) \cdots \sigma(n)$ et

$$\rho(w)(i) = \begin{cases} 0 & \text{si } i = 0, \\ w_i & \text{si } i > 0, \\ -w_{-i} & \text{si } i < 0, \end{cases}$$

pour $i \in [-n, n]$.

Les définitions suivantes nous seront utiles pour décrire le produit et le co-produit de l'algèbre de Hopf **BFQSym**.

Définition 3.4. Pour $i \in \mathbb{Z} \setminus \{0\}$ et $k \in \mathbb{Z}$, nous définissons les entiers $i_{[k]}$ et $i\langle k \rangle$ (pour $i \neq \pm k$) par :

$$i_{[k]} = \begin{cases} i + k & \text{si } i > 0, \\ i - k & \text{si } i < 0, \end{cases} \qquad i\langle k \rangle = \begin{cases} i + 1 & \text{if } i < -k, \\ i & \text{if } -k < i < k, \\ i - 1 & \text{if } i > k. \end{cases}$$

Pour $w = w_1 \cdots w_\ell$ un mot en les lettres $[-n, n] \setminus \{0\}$, nous définissons $w_{[k]}$ comme étant le mot $w_{1[k]} \cdots w_{\ell[k]}$ et $w\langle k \rangle$ comme étant le mot $w_1\langle k \rangle \cdots w_\ell\langle k \rangle$ si $w_j \neq \pm k$ pour tout j. Nous étendons ces notions aux ensembles d'entiers.

Exemple 3.5. Si w est le mot $1 \cdot -5 \cdot 3 \cdot -2 \cdot 6$, nous avons $w_{[2]} = 3 \cdot -7 \cdot 5 \cdot -4 \cdot 8$ ainsi que $w\langle 4 \rangle = 1 \cdot -4 \cdot 3 \cdot -2 \cdot 5$.

3.2 Produit de battage

Construisons un produit d'algèbre de Hopf graduée sur $\mathbb{Q}\mathfrak{S}^{\pm}$.

Notation 3.6. Pour $k, \ell \geqslant 1$, nous notons $\mathrm{Sh}_{k,\ell}$ tous les sous-ensembles de $[1, k+\ell]$ de cardinalité k. Pour $X \in \mathrm{Sh}_{k,\ell}$, nous écrivons $X = \{x_1 < \cdots < x_k\}$ pour indiquer que les x_i sont des éléments de X dans l'ordre croissant.

Par exemple, nous avons :

$$\mathrm{Sh}_{2,3} = \{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\}.$$

Définition 3.7. Soient $k, \ell \geqslant 1$ deux entiers. Pour deux mots $u \in W_k^{\pm}$, $v \in W_\ell^{\pm}$ et $X = \{x_1 < \cdots < x_k\} \in \mathrm{Sh}_{k,\ell}$ nous définissons le *X-battage de u et v*, noté $u \sqcup\!\sqcup^X v$, le mot de $W_{k+\ell}^{\pm}$ donné par :

$$u \sqcup\!\sqcup^X v = v_0\, u_1\, v_1 \,\cdots\, v_{k-1}\, u_k\, v_k,$$

avec $v_0 \cdots v_k = v[k]$ et $\ell(v_i) = x_{i+1} - x_i - 1$, avec les conventions $x_0 = 0$ et $x_{k+1} = k + \ell$.

Remarquons que les lettres venant du mot u sont aux positions désignées par X dans le mot final $u \sqcup\!\sqcup^X v$.

Exemple 3.8. Soient u le mot $-2 \cdot 1$ et v le mot $3 \cdot -1 \cdot 2$. Nous avons donc $k = 2$ et $\ell = 3$. Le mot $v_{[k]}$ est $5 \cdot -3 \cdot 4$. Le $\{2,4\}$-battage de u et v est le mot $5 \cdot -2 \cdot -3 \cdot 1 \cdot 4$ tandis que le $\{4,5\}$-battage de u et v est $5 \cdot -3 \cdot 4 \cdot -2 \cdot 1$; les lettres en gris proviennent du mot u.

Définition 3.9. Pour $\sigma \in \mathfrak{S}_k^{\pm}$ et $\tau \in \mathfrak{S}_\ell^{\pm}$ deux permutations signées nous définissons le *produit de battage* de σ et τ comme étant la permutation signée $\sigma \sqcup\!\sqcup \tau$ de $\mathfrak{S}_{k+\ell}^{\pm}$ définie par :

$$\sigma \sqcup\!\sqcup \tau = \sum_{X \in \mathrm{Sh}_{k,\ell}} \rho\left(w(\sigma) \sqcup\!\sqcup^X w(\tau)\right).$$

Exemple 3.10. En considérant les permutations signées $\sigma = (-2, 1)$ et $\tau = (3, -1, 2)$, nous obtenons :

$$\begin{aligned}\sigma \sqcup\!\sqcup \tau = \ & (-2,1,5,-3,4)+(-2,5,1,-3,4)+(-2,5,-3,1,4)+(-2,5,-3,4,1)\\ & +(5,-2,1,-3,4)+(5,-2,-3,1,4)+(5,-2,-3,4,1)+(5,-3,-2,1,4)\\ & +(5,-3,-2,4,1)+(5,-3,4,-2,1).\end{aligned}$$

3.3 Co-produit

Construisons maintenant un coproduit d'algèbre de Hopf graduée pour $\mathbb{Q}\mathfrak{S}^{\pm}$.

Définition 3.11. Soient $x_1, \ldots, x_n$ des entiers distincts. Pour toute suite $\varepsilon_1, \ldots, \varepsilon_n$ de l'ensemble $\{-1, +1\}$, nous définissons $\mathrm{Std}(\varepsilon_1 x_1, \ldots, \varepsilon_n\, x_n)$ comme étant le mot

$$\varepsilon_1\, f(x_1) \,\cdots\, \varepsilon_n\, f(x_n),$$

où f est l'unique application croissante de $\{x_1, \ldots, x_n\}$ dans $[1, n]$.

Mis à part les signes ε_i, cette notion de standardisation de mots coïncide avec celle utilisée pour les permutations non signées de $\mathfrak{S}_n$.

Définition 3.12. Nous définissons un co-produit sur $\Delta : \mathbb{Q}\mathfrak{S}^{\pm} \to \mathbb{Q}\mathfrak{S}^{\pm} \otimes \mathbb{Q}\mathfrak{S}^{\pm}$ par

$$\forall \sigma \in \mathfrak{S}_n^{\pm}, \quad \Delta(\sigma) = \sum_{k=0}^{n} \rho(\mathrm{Std}(\sigma(1), \ldots, \sigma(k))) \otimes \rho(\mathrm{Std}(\sigma(k+1), \ldots, \sigma(n))).$$

Exemple 3.13. Le coproduit de $(4, -2, 3, -1)$ est :

$$\begin{aligned}\Delta(4,-2,3,1) =& 1 \otimes (4,-2,3,1) + (1) \otimes (-2,3,1) \\ &+ (2,-1) \otimes (2,1) + (3,-1,2) \otimes (1) + (4,-2,3,1) \otimes 1.\end{aligned}$$

Proposition 3.14. *Muni du produit de battage $\sqcup\!\sqcup$ et du co-produit Δ, l'espace vectoriel $\mathbb{Q}\mathfrak{S}^{\pm}$ est une algèbre de Hopf graduée et connexe, notée **BFQSym**.*

Les détails de la démonstration de la proposition 3.14 sont omis de ce mémoire et peuvent être trouvés dans les travaux de J. C. Novelli et J. Y. Thibon [97] publiés en 2010. En effet, **BFQSym** correspond à l'algèbre de Hopf des permutations décorées $\mathbf{FQSym}^D$ avec $D = \{-1, 1\}$; le groupe $\mathfrak{S}_n^{\pm}$ étant isomorphe au produit en couronne $\mathfrak{S}_n \wr \{-1, 1\}$.

3.4 La structure duale

À l'aide du crochet non dégénéré $\langle \sigma, \tau \rangle = \delta_\sigma^\tau$, nous identifions **BFQSym** avec son dual. La structure d'algèbre de Hopf du dual est donnée par le produit $*$ et le co-produit δ définis par :

$$\langle \sigma * \tau, \kappa \rangle = \langle \sigma \otimes \tau, \Delta(\kappa) \rangle \qquad \text{et} \qquad \langle \delta(\sigma), \tau \otimes \kappa \rangle = \langle \sigma, \tau \sqcup\!\sqcup \kappa \rangle .$$

L'application ι de $\mathbb{Q}\mathfrak{S}^{\pm}$ dans lui-même envoyant σ sur σ^{-1} est un isomorphisme d'algèbre de Hopf entre $(\mathbf{BFQSym}, \sqcup\!\sqcup, \Delta)$ et $(\mathbf{BFQSym}, *, \delta)$. La proposition suivante donne une description de $*$.

Proposition 3.15 (J. C. Novelli et J. Y. Thibon [97])**.** *Pour $\sigma \in \mathfrak{S}_k^{\pm}$ et $\tau \in \mathfrak{S}_\ell^{\pm}$ nous avons :*

$$\sigma * \tau \;=\; \sum_{\substack{u \in W_{k+\ell}^{\pm} \\ \mathrm{Std}(u_1,\ldots,u_k) = w(\sigma) \\ \mathrm{Std}(u_{k+1},\ldots,u_{k+\ell}) = w(\tau)}} \rho(u).$$

Exemple 3.16. Pour les permutations signées $\sigma = (2, -1)$ et $\tau = (3, -1, 2)$ nous avons :

$$\begin{aligned}\sigma * \tau = \; & (2,-1,5,-3,4) + (3,-1,5,-2,4) + (4,-1,5,-2,3) + (5,-1,4,-2,3) \\ & + (3,-2,5,-1,4) + (4,-2,5,-1,3) + (5,-2,4,-1,3) + (4,-3,5,-1,2) \\ & + (5,-3,4,-1,2) + (5,-4,3,-1,2).\end{aligned}$$

4 Le résultat de divisibilité

Rappelons, que par le corollaire 2.15, la matrice $\mathrm{Adj}_{\mathbf{B_n}} = (a_{r(\sigma),r(\tau)})$ est donnée par

$$a_{r(\sigma),r(\tau)} = \begin{cases} 1 & \text{si } \mathrm{Des}\,(\tau^{-1}) \subseteq \mathrm{Des}\,(\sigma), \\ 0 & \text{sinon.} \end{cases}$$

Définition 4.1. Pour $n \in \mathbb{N}$, nous définissons un endomorphisme $\Phi_{\mathbf{B_n}}$ de $\mathbb{Q}\mathfrak{S}_n^{\pm}$ en posant

$$\Phi_{\mathbf{B_n}}(\sigma) = \sum_{\tau \in \mathfrak{S}_n^{\pm}} a_{r(\sigma),r(\tau)}\tau = \sum_{\substack{\tau \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\tau^{-1}\right) \subseteq \mathrm{Des}(\sigma)}} \tau.$$

De plus nous notons $\Phi_{\mathbf{B}}$ l'endomorphisme $\bigoplus \Phi_{\mathbf{B_n}}$ de $\mathbb{Q}\mathfrak{S}^{\pm}$.

Lemme 4.2. *Pour $n \in \mathbb{N}$, la matrice de $\Phi_{\mathbf{B_n}}$ relativement à la base $\mathfrak{S}_n$ est ${}^t\mathrm{Adj}^{+}_{\mathbf{B_n}}$.*

Démonstration. Par bijection de l'application $r : \mathfrak{S}_n^{\pm} \to \{\text{simples de } B^{+}_{\mathbf{B_n}}\}$ et définition de $\Phi_{\mathbf{B_n}}$. □

Définition 4.3. Un endomorphisme Ψ de $\mathbb{Q}\mathfrak{S}^{\pm}$ est une *dérivation surjective* s'il vérifie :

(*i*) $\Psi(x \sqcup\!\sqcup y) = \Psi(x) \sqcup\!\sqcup y + x \sqcup\!\sqcup \Psi(y)$ pour tous x, y de $\mathbb{Q}\mathfrak{S}^{\pm}$;

(*ii*) $\Psi(\mathbb{Q}\mathfrak{S}_n^{\pm}) = \mathbb{Q}\mathfrak{S}_{n-1}^{\pm}$ pour tout $n \geqslant 1$.

Proposition 4.4. *S'il existe une dérivation surjective Ψ de $\mathbb{Q}\mathfrak{S}^{\pm}$ commutant avec $\Phi_{\mathbf{B}}$, alors, pour $n \geqslant 1$, le polynôme caractéristique de $\Phi_{\mathbf{B}_{n-1}}$ divise celui de $\Phi_{\mathbf{B}_n}$.*

Démonstration. Soit Ψ une dérivation surjective de $\mathbb{Q}\mathfrak{S}^{\pm}$ commutant avec $\Phi_{\mathbf{B}}$, et n un entier $\geqslant 1$. Notons Ψ_n la restriction de Ψ à $\mathbb{Q}\mathfrak{S}_n^{\pm}$. Nous fixons une base $\mathcal{B} = \mathcal{B}_0 \sqcup \mathcal{B}_1$ de $\mathbb{Q}\mathfrak{S}_n^{\pm}$, telle que $\mathcal{B}_0$ soit une base de $\ker(\Psi_n)$. En restreignant la relation $\Psi \circ \Phi_{\mathbf{B}} = \Phi_{\mathbf{B}} \circ \Psi$ à $\mathbb{Q}\mathfrak{S}_n^{\pm}$, nous obtenons $\Psi_n \circ \Phi_{\mathbf{B_n}} = \Phi_{\mathbf{B_{n-1}}} \circ \Psi_n$. Pour tout élément x de $\ker(\Psi_n)$, nous avons $\Psi_n(\Phi_{\mathbf{B_n}}(x)) = \Phi_{\mathbf{B_{n-1}}}(\Psi_n(x)) = \Phi_{\mathbf{B_{n-1}}}(0) = 0$. Ainsi, $\ker(\Psi_n)$ est stabilisé par l'application $\Phi_{\mathbf{B_n}}$. En particulier, la matrice représentative de Φ_n dans la base $\mathcal{B}$ est la matrice triangulaire supérieure par blocs :

$$M_n = \begin{bmatrix} A_n & B_n \\ 0 & C_n \end{bmatrix}.$$

En notant $\chi(.)$ le polynôme caractéristique d'une matrice ou d'un endomorphisme nous obtenons :

$$\chi(\Phi_{\mathbf{B_n}}) = \chi(M_n) = \chi(A_n)\chi(C_n). \tag{3.1}$$

La matrice de la restriction $\overline{\Phi}_{\mathbf{B_n}}$ de $\Phi_{\mathbf{B_n}}$ à $\mathbb{Q}\mathfrak{S}_n^{\pm}/\ker(\Psi_n)$ est C_n et donc $\chi(\overline{\Phi}_{\mathbf{B_n}}) = \chi(C_n)$. Grâce à la surjectivité de Ψ, nous obtenons le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathbb{Q}\mathfrak{S}_n^{\pm}/\ker(\Psi_n) & \xrightarrow{\overline{\Phi}_{\mathbf{B_n}}} & \mathbb{Q}\mathfrak{S}_n^{\pm}/\ker(\Psi_n) \\ \downarrow{\scriptstyle \overline{\Psi}_n} & & \downarrow{\scriptstyle \overline{\Psi}_n} \\ \mathbb{Q}\mathfrak{S}_{n-1}^{\pm} & \xrightarrow{\Phi_{\mathbf{B_{n-1}}}} & \mathbb{Q}\mathfrak{S}_{n-1}^{\pm} \end{array}$$

impliquant que l'endomorphisme $\Phi_{\mathbf{B_{n-1}}}$ est conjugué à $\overline{\Phi}_{\mathbf{B_n}}$. L'équation (3.1) devient alors $\chi(\Phi_{\mathbf{B_n}}) = \chi(A_n)\chi(\Phi_{\mathbf{B_{n-1}}})$, et donc $\chi(\Phi_{\mathbf{B_{n-1}}})$ divise $\chi(\Phi_{\mathbf{B_n}})$. □

Comme nous pouvons le constater la propriété (*i*) de la définition 4.3 n'est pas utilisée dans la démonstration précédente mais elle sera fondamentale pour établir la commutativité avec $\Phi_{\mathbf{B}}$.

Il nous reste donc à construire une dérivation surjective commutant avec Φ.

4.1 Une dérivation sur BFQSym.

Afin de décrire notre dérivation, nous introduisons quelques notations.

Définition 4.5. Pour a et b deux entiers distincts nous définissons $\varepsilon(a,b)$ par :

$$\varepsilon(a,b) = \begin{cases} 1 & \text{if } a < b, \\ -1 & \text{if } a > b. \end{cases}$$

Pour a,b,c trois entiers distincts nous posons $\varepsilon(a,b,c) = \dfrac{1}{2}\left(\varepsilon(a,b) + \varepsilon(b,c)\right) \in \{-1,0,1\}$.

Définition 4.6. Pour $u = u_1 \cdots u_n$ un mot de $W_n^{\pm}$ et i un entier de $[1,n]$, nous posons :

$$\mathrm{sign}_i(u) = \varepsilon(u_{j-1}, u_j, u_{j+1}),$$

où j est l'unique entier satisfaisant $|u_j| = i$, avec les conventions $u_0 = 0$ et $u_{n+1} = -\infty$.

Exemple 4.7. Considérons le mot $u = -1 \cdot 2 \cdot -4 \cdot -5 \cdot 3 \cdot 6$ augmenté en le mot $0 \cdot -1 \cdot 2 \cdot -4 \cdot -5 \cdot 3 \cdot 6 \cdot -\infty$. Nous obtenons :

$$\begin{aligned} \mathrm{sign}_1(u) &= \varepsilon(0,-1,2) = 0, & \mathrm{sign}_2(u) &= \varepsilon(-1,2,-4) = 0, \\ \mathrm{sign}_3(u) &= \varepsilon(-5,3,6) = 1, & \mathrm{sign}_4(u) &= \varepsilon(2,-4,-5) = -1, \\ \mathrm{sign}_5(u) &= \varepsilon(-4,-5,3) = 0, & \mathrm{sign}_6(u) &= \varepsilon(3,6,-\infty) = 0. \end{aligned}$$

Lemme 4.8. *Soient $n \geqslant 1$ et $\sigma \in \mathfrak{S}_n^{\pm}$. Pour $j \in [1,n-1]$, nous avons :*

$$\mathrm{sign}_{|\sigma(j)|}(w(\sigma)) = \begin{cases} 1 & \text{si } \{j-1,j\} \cap \mathrm{Des}\,(\sigma) = \emptyset; \\ -1 & \text{si } \{j-1,j\} \subseteq \mathrm{Des}\,(\sigma); \\ 0 & \text{sinon.} \end{cases}$$

De plus la valeur de $\mathrm{sign}_{|\sigma(n)|}(w(\sigma))$ est -1 si $n-1$ appartient à $\mathrm{Des}\,(\sigma)$ et 0 sinon.

Démonstration. Soient σ une permutation signée de $\mathfrak{S}_n^{\pm}$ et j un entier de $[1,n-1]$. Par définition de sign, nous avons $\mathrm{sign}_{|\sigma(j)|}(w(\sigma)) = 1$ si et seulement si $\sigma(j-1) < \sigma(j) < \sigma(j+1)$, ce qui est équivalent à $j-1 \notin \mathrm{Des}\,(\sigma)$ et $j \notin \mathrm{Des}\,(\sigma)$. Encore par définition de sign, nous avons $\mathrm{sign}_{|\sigma(j)|}(w(\sigma)) = -1$ si et seulement si $\sigma(j-1) > \sigma(j) > \sigma(j+1)$, c'est-à-dire, $j-1$ et j appartiennent à $\mathrm{Des}\,(\sigma)$.

Montrons le résultat pour $j = n$. Comme la relation $\sigma(n) > -\infty$ est toujours vérifiée la valeur de $\mathrm{sign}_{|\sigma(j)|}(w(\sigma))$ est -1 pour $\sigma(n-1) > \sigma(n)$ et 0 sinon, comme attendu. □

Exemple 4.9. Les descentes de $\sigma = (-1,2,-4,-5,3,6)$ sont $\{0,2,3\}$. Ainsi les valeurs non nulles de $\mathrm{sign}_{|\sigma(j)|}(w(\sigma))$ sont obtenues pour $j = 3$ et $j = 5$:

$$\begin{aligned} \mathrm{sign}_{|\sigma(3)|}(w(\sigma)) &= \mathrm{sign}_4(w(\sigma)) = -1, \\ \mathrm{sign}_{|\sigma(5)|}(w(\sigma)) &= \mathrm{sign}_3(w(\sigma)) = 1, \end{aligned}$$

Définition 4.10. Pour $u \in W_n^{\pm}$ et $i \in [1,n]$, nous notons $\mathrm{del}_i(u)$ le mot

$$\mathrm{del}_i(u) = u_1\langle i\rangle \cdots u_{j-1}\langle i\rangle\ u_{j+1}\langle i\rangle \cdots u_n\langle i\rangle$$

de $W_{n-1}^{\pm}$, où j est l'unique entier satisfaisant la relation $|u_j| = i$.

Remarquons que nous avons $\mathrm{del}_i(u) = \mathrm{Std}(u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n)$.

Exemple 4.11. En considérant le mot $u = -1 \cdot 2 \cdot -4 \cdot -5 \cdot 3 \cdot 6$, nous obtenons :

$$\begin{aligned} \mathrm{del}_1(u) &= 1 \cdot -3 \cdot -4 \cdot 2 \cdot 5, & \mathrm{del}_2(u) &= -1 \cdot -3 \cdot -4 \cdot 2 \cdot 5, \\ \mathrm{del}_3(u) &= -1 \cdot 2 \cdot -3 \cdot -4 \cdot 5, & \mathrm{del}_4(u) &= -1 \cdot 2 \cdot -4 \cdot 3 \cdot 5, \\ \mathrm{del}_5(u) &= -1 \cdot 2 \cdot -4 \cdot 3 \cdot 5, & \mathrm{del}_6(u) &= -1 \cdot 2 \cdot -4 \cdot -5 \cdot 3. \end{aligned}$$

Définition 4.12. Pour $n \in \mathbb{N}$, nous définissons une application ∂_n de $\mathbb{Q}\mathfrak{S}_n^{\pm}$ dans l'ensemble $\mathbb{Q}\mathfrak{S}_{n-1}^{\pm}$ en posant

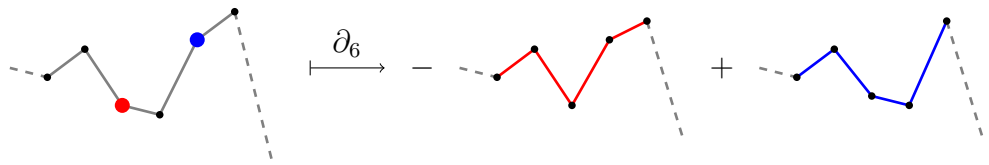
$$\partial_n(\sigma) = \sum_{k=1}^{n} \partial_n^i(\sigma) \quad \text{et} \quad \partial_n^i(\sigma) = \mathrm{sign}_i(w(\sigma))\, \rho(\mathrm{del}_i(w(\sigma))).$$

Nous notons ∂ l'application de $\mathbb{Q}\mathfrak{S}^{\pm}$ dans lui-même définie par $\partial = \bigoplus_{n=1}^{+\infty} \partial_n$.

Exemple 4.13. Considérons la permutation $\sigma = (-1, 2, -4, -5, 3, 6)$. Nous avons $\partial_6^1(\sigma) = \partial_6^2(\sigma) = \partial_6^5(\sigma) = \partial_6^6(\sigma) = 0$, ainsi que :

$$\begin{aligned} \partial_6^3(\sigma) &= \mathrm{sign}_3(w(\sigma))\rho(\mathrm{del}_3(w(\sigma))) = (-1, 2, -3, -4, 5), \\ \partial_6^4(\sigma) &= \mathrm{sign}_4(w(\sigma))\rho(\mathrm{del}_4(w(\sigma))) = -(-1, 2, -4, 3, 5). \end{aligned}$$

Finalement nous obtenons $\partial(\sigma) = (-1, 2, -3, -4, 5) - (-1, 2, -4, 3, 5)$. Géométriquement si nous représentons une permutation τ de $\mathfrak{S}_k^{\pm}$ par une ligne brisée reliant les points de coordonnées $(i, \tau(i))$ pour $i = 0, \ldots, k+1$ avec la convention $\tau(k+1) = -\infty$, nous obtenons



Le point rouge, *resp.* bleu, correspond à $\sigma(3) = -4$, *resp.* $\sigma(5) = 3$. L'application ∂ consiste donc à détruire les doubles descentes et les doubles montées tout en pondérant avec un signe : -1 pour les descentes et $+1$ pour les montées.

Exemple 4.14. L'application ∂ envoie $\mathbb{Q}\mathfrak{S}_2^{\pm}$ sur $\mathbb{Q}\mathfrak{S}_1^{\pm}$. La matrice de cette application, relativement à l'énumération de $\mathfrak{S}_2^{\pm}$ donnée à l'exemple 2.16 et l'énumération (1), (-1) de $\mathfrak{S}_1^{\pm}$, est :

$$\begin{bmatrix} 1 & -1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Nous allons maintenant montrer que l'application ∂ est une dérivation surjective de $\mathbb{Q}\mathfrak{S}^{\pm}$. Pour cela nous commençons par établir une compatibilité entre ∂ et le produit de battage $\sqcup\!\sqcup$.

Lemme 4.15. *Soient $\sigma \in \mathfrak{S}_k^{\pm}$ et $\tau \in \mathfrak{S}_\ell^{\pm}$ deux permutations signées.*

(i) Pour tout $i \in [1, k]$, nous avons $\partial_{k+\ell}^i(\sigma \sqcup\!\sqcup \tau) = \partial_k^i(\sigma) \sqcup\!\sqcup \tau$;

(ii) Pour tout $i \in [k+1, k+\ell]$, nous avons $\partial_{k+\ell}^i(\sigma \sqcup\!\sqcup \tau) = \sigma \sqcup\!\sqcup \partial_\ell^{i-k}(\tau)$.

La démonstration du lemme est technique et peut être ignorée sans impacter la compréhension du reste de ce chapitre.

Démonstration. Soient σ et τ deux permutations signées de $\mathfrak{S}_k^{\pm}$ et $\mathfrak{S}_\ell^{\pm}$. Posons $u = w(\sigma)$, $v = w(\tau)$. Soit i un entier de $[1,k]$. Il existe un unique entier j tel qu'on ait $u_j = \pm i$. Par définition de del_i, nous avons $\mathrm{del}_i(u) = u_1\langle i\rangle \cdots u_{j-1}\langle i\rangle\, u_{j+1}\langle i\rangle \cdots u_k\langle i\rangle$. Soit $Y = \{y_1 < \cdots < y_{k-1}\}$ un élément de $\mathrm{Sh}_{k-1,\ell}$. Pour tout m, on pose $u'_m = u_m\langle i\rangle$. Il existe k mots $v_0, \ldots, v_{k-1}$ satisfaisant

— $v_0 \cdots v_{k-1} = v$,

— $\ell(v_t) = y_{t+1} - y_t - 1$ avec la convention $y_k = k + \ell - 1$,

et tels que nous ayons :

$$\mathrm{del}_i(u) \sqcup\!\sqcup^Y v = v_0[k-1]\, u'_1 \cdots v_{j-2}[k-1]\, u'_{j-1} \cdot v_{j-1}[k-1] \cdot u'_{j+1}\, v_j[k-1] \cdots u'_k\, v_{k-1}[k-1]. \tag{3.2}$$

Notons $v_{j-1} = \alpha_1 \cdots \alpha_m$ où les α_t sont des lettres et m vaut $y_j - y_{j-1} - 1$. Pour $a \in [0,m]$, nous définissons $k+1$ mots $w_0^a, \ldots, w_k^a$:

$$w_t^a = \begin{cases} v_t & \text{pour } t \leqslant j-2, \\ \alpha_1 \cdots \alpha_a & \text{pour } t = j-1, \\ \alpha_{a+1} \cdots \alpha_m & \text{pour } t = j, \\ v_{t-1} & \text{pour } t \geqslant j+1. \end{cases}$$

Le mot v est donc égal à $w_0^a \cdots w_{j-1}^a\, w_j^a \cdots w_k^a$. Construisons un raffinement Y_a de Y en posant :

$$Y_a = \{y_1 < \cdots < y_{j-1} < y_{j-1} + a + 1 < y_j + 1 < \cdots < y_{k-1} + 1\}.$$

Notons que Y_a est un élément de $\mathrm{Sh}_{k,\ell}$ pour tout $a \in [0,m]$. Le produit de battage de u et v relativement à Y_a est :

$$u \sqcup\!\sqcup^{Y_a} v = w_0^a[k]\, u_1 \cdots w_{j-2}^a[k]\, u_{j-1} \cdot w_{j-1}^a[k]\, u_j\, w_j^a[k] \cdot u_{j+1}\, w_{j+1}^a[k] \ldots u_k\, w_k^a[k].$$

En appliquant del_i à la relation précédente, nous obtenons :

$$\mathrm{del}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) = w_0^a[k-1]\, u'_1 \ldots w_{j-2}^a[k-1]\, u'_{j-1} \cdot w_{j-1}^a[k-1]\, w_j^a[k-1] \cdot u'_{j+1}\, w_{j+1}^a[k-1] \ldots u'_k\, w_k^a[k-1],$$

qui, par définition des mots w_p^a, est exactement l'expression de $\mathrm{del}_i(u) \sqcup\!\sqcup^Y v$ donnée en (3.2). Nous obtenons ainsi

$$\sum_{a=0}^{m} \mathrm{sign}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) \mathrm{del}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) = \left(\sum_{a=0}^{m} \mathrm{sign}_i\left(u \sqcup\!\sqcup^{Y_a} v\right)\right) \mathrm{del}_i(u) \sqcup\!\sqcup^Y v.$$

Par définition de sign_i et ε avec les conventions $\alpha_0 = u_{j-1}$, $\alpha_{m+1} = u_{j+1}$, et les conventions $u_0 = 0$, $u_{k+1} = -\infty$ utilisées à la définition 4.6, nous obtenons :

$$\begin{aligned} \sum_{a=0}^{m} \mathrm{sign}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) &= \sum_{a=0}^{k} \varepsilon(\alpha_a, u_j, \alpha_{a+1}) = \frac{1}{2}\sum_{a=0}^{k} \varepsilon(\alpha_a, u_j) + \varepsilon(u_j, \alpha_{a+1}), \\ &= \frac{1}{2}\sum_{a=0}^{k} \big(\varepsilon(\alpha_a, u_j) - \varepsilon(\alpha_{a+1}, u_j)\big) = \varepsilon(\alpha_0, u_j, \alpha_{m+1}), \end{aligned}$$

et ce dernier vaut $\varepsilon(u_{j-1}, u_j, u_{j+1}) = \mathrm{sign}_i(u)$. Nous avons ainsi établi :

$$\sum_{a=0}^{m} \mathrm{sign}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) \mathrm{del}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) = \mathrm{sign}_i(u)\mathrm{del}_i(u) \sqcup\!\sqcup^Y v. \tag{3.3}$$

À partir de la relation $\mathrm{Sh}_{k,\ell} = \{Y_a \,|\, Y \in \mathrm{Sh}_{k-1,\ell} \,\mathrm{et}\, a \in [0,m]\}$, nous obtenons :

$$\begin{aligned} \partial_k^i(\sigma) \sqcup\!\sqcup \tau &= \sum_{Y \in \mathrm{Sh}_{k-1,\ell}} \mathrm{sign}_i(u)\ \mathrm{del}_i(u) \sqcup\!\sqcup^Y v, \\ &= \sum_{Y \in \mathrm{Sh}_{k-1,\ell}} \sum_{a=0}^{m} \mathrm{sign}_i\left(u \sqcup\!\sqcup^{Y_a} v\right) \mathrm{del}_i\left(u \sqcup\!\sqcup^{Y_a} v\right), \qquad \text{par (3.3)} \\ &= \sum_{X \in \mathrm{Sh}_{k,\ell}} \mathrm{sign}_i\left(u \sqcup\!\sqcup^X v\right) \mathrm{del}_i\left(u \sqcup\!\sqcup^X v\right), \\ &= \partial_{k+\ell}^i(\sigma \sqcup\!\sqcup \tau). \end{aligned}$$

Nous prouvons (ii) avec un argument similaire en échangeant les rôles de u et v. □

Proposition 4.16. *L'application ∂ est une dérivation de $(\boldsymbol{BFQSym}, \sqcup\!\sqcup)$.*

Démonstration. Soient σ et τ deux permutations signées de $\mathfrak{S}_k^{\pm}$ et $\mathfrak{S}_\ell^{\pm}$. Par définition de ∂, nous avons :

$$\partial(\sigma \sqcup\!\sqcup \tau) = \sum_{i=1}^{n} \partial_{k+\ell}^{i}(\sigma \sqcup\!\sqcup \tau) = \sum_{i=1}^{k} \partial_{k+\ell}^{i}(\sigma \sqcup\!\sqcup \tau) + \sum_{i=k+1}^{k+\ell} \partial_{k+\ell}^{i}(\sigma \sqcup\!\sqcup \tau).$$

Ainsi, par le lemme 4.15, nous obtenons :

$$\partial(\sigma \sqcup\!\sqcup \tau) = \sum_{i=1}^{k} \partial_{k}^{i}(\sigma) \sqcup\!\sqcup \tau + \sum_{i=1}^{\ell} \sigma \sqcup\!\sqcup \partial_{\ell}^{i}(\tau),$$

et donc $\partial(\sigma \sqcup\!\sqcup \tau) = \partial(\sigma) \sqcup\!\sqcup \tau + \sigma \sqcup\!\sqcup \partial(\tau)$. □

4.2 Surjectivité de ∂

Le but de cette sous-section est de démontrer la proposition suivante :

Proposition 4.17. *Pour tout $n \in \mathbb{N}$, l'application $\partial_{n+1} : \mathbb{Q}\mathfrak{S}_{n+1}^{\pm} \to \mathbb{Q}\mathfrak{S}_n^{\pm}$ est surjective.*

Illustrons la démonstration de la proposition 4.17 par un exemple.

Exemple 4.18. Soit $\sigma = \sigma_1$ la permutation $(2, -1, 4, 5, -3)$ de $\mathfrak{S}_5^{\pm}$. Nous cherchons la plus longue suite d'entiers successifs de la forme $k \ldots 5$ ou $-k \ldots -5$ dans le mot $w(\sigma)$. Dans notre exemple, cette suite est $4, 5$. Nous définissons τ_1 comme étant la permutation $(2, -1, 4, 5, 6, -3)$ obtenue de σ_1 en remplaçant $4, 5$ par $4, 5, 6$. Un calcul direct donne $\partial_6(\tau_1) = 2\sigma_1 - \sigma_2$ avec $\sigma_2 = (2, -1, 3, 4, 5)$, qui est le standardisé de $(2, -1, 4, 5, 6)$. Ainsi, nous obtenons :

$$\sigma_1 = \partial_6\left(\frac{1}{2}\tau_1\right) + \frac{1}{2}\sigma_2. \tag{3.4}$$

La plus longue suite de la forme souhaitée dans σ_2 est $3, 4, 5$. Nous posons alors $\tau_2 = (2, -1, 3, 4, 5, 6)$ et nous calculons $\partial_6(\tau_2) = 3\sigma_2$. Ainsi σ_2 est égale à $\partial_6\left(\frac{1}{3}\tau_2\right)$. En substituant dans (3.4), nous obtenons :

$$\sigma_1 = \partial_6\left(\frac{1}{2}\tau_1\right) + \partial_6\left(\frac{1}{6}\tau_2\right) = \partial_6\left(\frac{1}{2}(2, -1, 4, 5, 6, -3) + \frac{1}{6}(2, -1, 3, 4, 5, 6)\right),$$

établissant que σ est dans l'image de ∂_6.

Définition 4.19. Pour $n \geqslant 1$, nous notons I_n, J_n, P_n et Q_n les éléments de $\mathbb{Q}\mathfrak{S}_n^{\pm}$ définis par $I_n = (1, \ldots, n)$, $J_n = (-n, \ldots, -1)$ et :

$$P_n = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\sigma^{-1}\right) \subseteq \{0\}}} \sigma, \qquad\qquad Q_n = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}(\sigma) \subseteq \{0\}}} \sigma.$$

Exemple 4.20. Nous avons $P_2 = (1, 2) + (-1, 2) + (2, -1) + (-2, -1)$, $Q_2 = (1, 2) + (-1, 2) + (-2, 1) + (-2, -1)$ et, par exemple :

$$\begin{aligned} P_4 =& (1,2,3,4) + (-1,2,3,4) + (2,-1,3,4) + (-2,-1,3,4) + (2,3,-1,4) \\ &+ (-2,3,-1,4) + (2,3,4,-1) + (-2,3,4,-1) + (3,-2,-1,4) \\ &+ (-3,-2,-1,4) + (3,-2,4,-1) + (-3,-2,4,-1) + (3,4,-2,-1) \\ &+ (-3,4,-2,-1) + (4,-3,-2,-1) + (-4,-3,-2,-1), \\ =& J_0 \sqcup\!\sqcup I_4 + J_1 \sqcup\!\sqcup I_3 + J_2 \sqcup\!\sqcup I_2 + J_3 \sqcup\!\sqcup I_1 + J_4 \sqcup\!\sqcup I_0. \end{aligned}$$

Les vecteurs P_n et Q_n sont utilisés pour décrire les permutations de $\mathfrak{S}_n^{\pm}$ dont les ensembles des descentes sont inclus dans un sous-ensemble donné de $[0, n-1]$.

Lemme 4.21. *Soient $k_1, \dots, k_{\ell+1} \geqslant 1$ des entiers. Posons $n = k_1 + \cdots + k_{\ell+1}$ et notons D l'ensemble $\{k_1, k_1+k_2, \dots, k_1+\cdots+k_\ell\}$, nous avons les relations suivantes :*

$$Q_{k_1} * \cdots * Q_{k_{\ell+1}} = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}(\sigma) \subseteq \{0\} \cup D}} \sigma, \qquad I_{k_1} * Q_{k_2} * \cdots * Q_{k_{\ell+1}} = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}(\sigma) \subseteq D}} \sigma,$$

$$P_{k_1} \sqcup\!\sqcup \cdots \sqcup\!\sqcup P_{k_{\ell+1}} = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\sigma^{-1}\right) \subseteq \{0\} \cup D}} \sigma, \qquad I_{k_1} \sqcup\!\sqcup P_{k_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup P_{k_{\ell+1}} = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\sigma^{-1}\right) \subseteq D}} \sigma.$$

Démonstration. Pour $i \in [1, \ell]$ nous posons $d_i = k_1 + \cdots + k_i$. Comme toute permutation constituant Q_k ne peut pas avoir d'autre descente que 0, nous avons :

$$Q_k = \sum_{\substack{\sigma \in \mathfrak{S}_k^{\pm} \\ \sigma(1) < \cdots < \sigma(k)}} \sigma.$$

Alors, par la proposition 3.15, nous obtenons :

$$Q_{k_1} * \cdots * Q_{k_{\ell+1}} = \sum_{\substack{\sigma \in \mathfrak{S}_{k+\ell}^{\pm} \\ \sigma(1) < \cdots < \sigma(d_1) \\ \cdots \\ \sigma(d_\ell+1) < \cdots < \sigma(n)}} \sigma. \tag{3.5}$$

Les permutations apparaissant dans les sommes précédentes sont exactement celles ayant pour descentes un sous-ensemble de $\{0, d_1, \dots, d_\ell\}$. De même, comme I_{k_1} est la seule permutation σ de $\mathfrak{S}_{k_1}^{\pm}$ satisfaisant la relation $0 < \sigma(1) < \cdots < \sigma(k_1)$, nous avons :

$$I_{k_1} * Q_{k_2} * \cdots * Q_{k_{\ell+1}} = \sum_{\substack{\sigma \in \mathfrak{S}_{k+\ell}^{\pm} \\ 0 < \sigma(1) < \cdots < \sigma(d_1) \\ \sigma(d_1+1) < \cdots < \sigma(d_2) \\ \cdots \\ \sigma(d_\ell+1) < \cdots < \sigma(n)}} \sigma, \tag{3.6}$$

qui est la somme des permutations de $\mathfrak{S}_n^{\pm}$ ayant leur ensemble de descentes dans $\{d_1, \dots, d_\ell\}$. En appliquant l'isomorphisme ι de $(\mathbf{BFQSym}, \sqcup\!\sqcup, \Delta)$ sur $(\mathbf{BFQSym}, *, \delta)$ à l'expression de $Q_{k_1} * \cdots * Q_{k_{\ell+1}}$ donnée en (3.5) nous obtenons :

$$\iota(Q_{k_1}) \sqcup\!\sqcup \cdots \sqcup\!\sqcup \iota(Q_{k_{\ell+1}}) = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}(\sigma) \in \{0\} \cup D}} \sigma^{-1} = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\sigma^{-1}\right) \in \{0\} \cup D}} \sigma.$$

La relation désirée est alors conséquence de $\iota(Q_k) = P_k$. La seconde relation de la proposition faisant intervenir le produit de battage s'obtient de la même façon de (3.6) après avoir remarqué $\iota(I_{k_1}) = I_{k_1}$. □

Comme le suggère l'exemple 4.20, le vecteur P_n de $\mathbb{Q}\mathfrak{S}_n^{\pm}$ peut être obtenu par battage.

Lemme 4.22. *Pour tout $n \geqslant 1$, nous avons $P_n = \sum_{k=0}^{n} J_k \sqcup\!\sqcup I_{n-k}$.*

Démonstration. Par définition de Q_n, nous avons :

$$Q_n = \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm}, \\ \sigma(1) < \cdots < \sigma(n)}} \sigma = \sum_{k=0}^{n} \sum_{\substack{\sigma \in \mathfrak{S}_n^{\pm}, \\ \sigma(1) < \cdots < \sigma(k) < 0 \\ 0 < \sigma(k+1) < \cdots < \sigma(n)}} \sigma.$$

D'autre part, la proposition 3.15 donne :

$$J_k * I_{n-k} \quad = \sum_{\substack{\sigma\in\mathfrak{S}_n^{\pm} \\ \mathrm{Std}(\sigma(1),\dots,\sigma(k))=(-k,\dots,-1) \\ \mathrm{Std}(\sigma(k+1),\dots,\sigma(n))=(1,\dots,n-k)}} \sigma \quad = \sum_{\substack{\sigma\in\mathfrak{S}_n^{\pm}, \\ \sigma(1)<\cdots<\sigma(k)<0 \\ 0<\sigma(k+1)<\cdots<\sigma(n)}} \sigma.$$

Nous avons ainsi établi $Q_n = \sum_{k=0}^{n} J_k * I_{n-k}$. Comme ι envoie Q_n sur P_n et laisse invariant I_k et J_k, nous obtenons

$$P_n = \iota(Q_n) = \sum_{k=0}^{n} \iota(J_k * I_{n-k}) = \sum_{k=0}^{n} \iota(J_k) \sqcup\!\sqcup \iota(I_{n-k}) = \sum_{k=0}^{n} J_k \sqcup\!\sqcup I_{n-k}. \qquad \square$$

Grâce à la compatibilité de ∂ avec le produit de battage $\sqcup\!\sqcup$ établie au lemme 4.15, nous déterminons l'image de P_n par la dérivation ∂.

Lemme 4.23. *Pour tout $n \geqslant 1$, nous avons $\partial(I_n) = (n-1)I_{n-1}$, $\partial(J_n) = (n-2)J_{n-1}$ et $\partial(P_n) = (n-2)P_{n-1}$, avec les conventions $I_0 = J_0 = P_0 = \emptyset$.*

Démonstration. Pour $n \geqslant 1$, nous avons :

$$\partial(I_n) = \sum_{i=1}^{n} \partial_i(I_n) = \sum_{i=1}^{n} \mathrm{sign}_i(I_n) I_{n-1}.$$

Par définition de sign, nous avons $\mathrm{sign}_1(I_n) = \cdots = \mathrm{sign}_{n-1}(I_n) = 1$ et $\mathrm{sign}_n(I_n) = 0$. Ceci implique $\partial(I_n) = (n-1)I_{n-1}$. De même, on a $\mathrm{sign}_1(J_n) = -1$, $\mathrm{sign}_k(J_n) = 1$ pour $k \in [2, n-1]$, $\mathrm{sign}_n(J_n) = 0$ et $\mathrm{del}_i(J_n) = J_{n-1}$ et donc $\partial(J_n) = (n-2)J_{n-1}$ pour $n \geqslant 1$.

Montrons maintenant $\partial(P_n) = (n-2)P_{n-1}$. Par convention, nous avons $\partial(I_0) = \partial(J_0) = 0$. En utilisant le lemme 4.22 et la compatibilité de ∂ et $\sqcup\!\sqcup$ donnée au lemme 4.15, nous obtenons :

$$\begin{aligned}
\partial(P_n) &= \partial\left(\sum_{k=0}^{n} J_k \sqcup\!\sqcup I_{n-k}\right), \\
&= \sum_{k=0}^{n} \partial(J_k) \sqcup\!\sqcup I_{n-k} + \sum_{k=0}^{n} J_k \sqcup\!\sqcup \partial(I_{n-k}), \\
&= \sum_{k=1}^{n} (k-2) J_{k-1} \sqcup\!\sqcup I_{n-k} + \sum_{k=0}^{n} (n-k-1) J_k \sqcup\!\sqcup I_{n-k-1}, \\
&= \sum_{k=0}^{n-1} (k-1) J_k \sqcup\!\sqcup I_{n-1-k} + \sum_{k=0}^{n} (n-k-1) J_k \sqcup\!\sqcup I_{n-1-k}, \\
&= (n-2) \sum_{k=0}^{n-1} J_k \sqcup\!\sqcup I_{n-1-k} = (n-2) P_{n-1}. \qquad \square
\end{aligned}$$

Nous pouvons maintenant démontrer la proposition 4.17. Pour cela nous utilisons un argument triangulaire semblable à celui utilisé à l'exemple 4.18.

Démonstration de la proposition 4.17. Soit σ une permutation de $\mathfrak{S}_n^{\pm}$. Notons u le mot $w(\sigma)$. Nous traitons deux cas séparément, en fonction que n ou $-n$ apparaisse ou non dans u.

Cas où n apparaît dans u. Soit $i(\sigma)$ le plus petit entier i tel que u peut être écrit $v \cdot [i \ \cdots \ n] \cdot w$. Nous utilisons une induction sur $i(\sigma)$. Si $i(\sigma)$ vaut 1 nous avons $\sigma = I_n$. Comme le lemme 4.23 donne :

$$\partial_{n+1}(I_{n+1}) = nI_n,$$

nous obtenons $\sigma = \partial_{n+1}(\frac{1}{n} I_{n+1})$. Supposons $i = i(\sigma) > 1$. Soit u' le mot $v \cdot [i \ \cdots \ n+1] \cdot w$. Comme chaque lettre de v et de w est plus petite que $i-1$, le mot u' appartient à $W_{n+1}^{\pm}$. Pour $j \in [i, n]$ nous

avons $\mathrm{del}_j(u') = u$ et $\mathrm{sign}_j(u') = 1$. Comme la première lettre de w est inférieure à $n+1$, nous obtenons $\mathrm{sign}_{n+1}(u') = 0$, et donc :

$$\sum_{j=i}^{n+1} \partial_{n+1}^j(\rho(u')) = (n-i+1)\sigma,$$

avec $n-i+1 \neq 0$, car $i \leqslant n$. Soit j un entier de $[1, i-1]$. Comme la lettre $\pm j$ apparaît seulement dans v ou dans w et que $|j| < i$ est vérifié, nous avons :

$$\mathrm{del}_j(u') = v\langle j\rangle \cdot [i-1 \ \cdots \ n] \cdot w\langle j\rangle\,.$$

Nous obtenons ainsi que $\partial_{n+1}(\rho(u'))$ est la somme de $(n-i+1)\sigma$ et d'une combinaison linéaire de permutations $\alpha_1, \ldots, \alpha_k$ de $\mathfrak{S}_n^{\pm}$ satisfaisant $i(\alpha_j) \leqslant i-1 < i = i(\sigma)$. Par hypothèse d'induction, les permutations α_j appartiennent à $\mathrm{Im}(\partial_{n+1})$, ce qui implique $\sigma \in \mathrm{Im}(\partial_{n+1})$.

Cas où n n'apparaît pas dans u. L'entier $-n$ apparaît donc dans u. Pour $\ell \geqslant 1$, notons K_ℓ la permutation $(-1, \ldots, -\ell)$ de $\mathfrak{S}_\ell^{\pm}$. Un calcul direct donne $\partial(K_\ell) = -\ell K_{\ell-1}$ pour $\ell \geqslant 2$ et $\partial(K_1) = 0$.

Soit $i(\sigma)$ le plus petit entier i tel que u peut être écrit $v \cdot [-i \ \cdots \ -n] \cdot w$. Nous utilisons encore une induction sur $i(\sigma)$. Si $i(\sigma)$ vaut 1, alors nous avons $\sigma = K_n$ et donc $\partial_{n+1}(K_{n+1}) = -(n+1)K_n$, ce qui implique

$$\sigma = \partial_{n+1}\left(-\frac{1}{n+1}K_{n+1}\right).$$

Supposons maintenant $i = i(\sigma) > 1$. Notons u' le mot $v \cdot [-i \ \cdots \ -(n+1)] \cdot w$ of $W_{n+1}^{\pm}$ et par τ la permutation signée correspondante de $\mathfrak{S}_{n+1}^{\pm}$. Pour $j < i$, nous avons :

$$\mathrm{del}_j(u') = v\langle j\rangle \cdot [-(i-1) \ \cdots \ -n] \cdot w\langle j\rangle\,.$$

Ainsi

$$\alpha = \sum_{j=1}^{i-1} \partial_{n+1}^j(\rho(u'))$$

est une combinaison linéaire de permutations $\alpha_1, \ldots, \alpha_k \in \mathfrak{S}_n^{\pm}$ satisfaisant $i(\alpha_j) < i = i(\sigma)$ qui, par hypothèse d'induction, implique $\alpha \in \mathrm{Im}(\partial_{n+1})$. Il reste à établir que

$$\beta = \sum_{j=i}^{n+1} \partial_{n+1}^j(\rho(u'))$$

est un multiple de σ. Pour $j \in [i, n]$, nous avons $\mathrm{del}_j(u') = u$ et $\mathrm{sign}_j(u') = -1$. Si le mot w est vide alors $\mathrm{sign}_{n+1}(\rho(u'))$ vaut -1 et nous avons $\mathrm{del}_{n+1}(u') = u$. Ainsi, dans ce cas, β est égale à $-(n+2-i)\sigma$ avec $n+2-i \neq 0$, car nous avons $i \leqslant n$. Si w est non vide, alors sa première lettre est supérieure à $-(n+1)$, impliquant $\mathrm{sign}_{n+1}(\rho(u')) = 0$. Nous obtenons $\beta = -(n+1-i)\sigma$ avec $n+1-i \neq 0$, car $i \leqslant n$ est vérifiée. Dans tous les cas, nous avons obtenu que la permutation signée σ appartient à l'image de ∂_{n+1}. □

Comme conséquence directe de la proposition 4.16 et de la proposition 4.17 nous obtenons le résultat suivant :

Corollaire 4.24. *L'application ∂ est une dérivation surjective de $(\boldsymbol{BFQSym}, \sqcup\!\sqcup)$.*

4.3 Commutation de ∂ et $\Phi_{\mathbf{B}}$.

Par définition de $\mathrm{Adj}^+_{\mathbf{B_n}}$, pour tout $\sigma \in \mathfrak{S}_n^{\pm}$, nous avons :

$$\Phi_{\mathbf{B}}(\sigma) = \Phi_{\mathbf{B_n}}(\sigma) \ = \sum_{\substack{\tau \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\tau^{-1}\right) \subseteq \mathrm{Des}(\sigma)}} \tau.$$

L'image de σ par $\Phi_{\mathbf{B_n}}$ dépend de l'ensemble des descentes de σ.

Définition 4.25. Pour $n \in \mathbb{N}$, nous notons $\mathcal{D}_n$ l'ensemble de tous les sous-ensembles de l'intervalle $[0, n-1]$.

Notation 4.26. L'application Des de $\mathfrak{S}_n^{\pm}$ dans $\mathcal{D}_n$ peut être étendue comme l'unique application Des : $\mathbb{Q}\mathfrak{S}_n^{\pm} \to \mathbb{Q}\mathcal{D}_n$.

Définition 4.27. Pour $n \in \mathbb{N}$, nous définissons une application $\widetilde{\Phi}_{\mathbf{B_n}}$ de $\mathbb{Q}\mathcal{D}_n$ dans $\mathbb{Q}\mathfrak{S}_n^{\pm}$ en posant

$$\widetilde{\Phi}_{\mathbf{B_n}}(I) \;=\; \sum_{\substack{\tau \in \mathfrak{S}_n^{\pm} \\ \mathrm{Des}\left(\tau^{-1}\right) \subseteq I}} \tau,$$

pour tout élément I de $\mathcal{D}_n$.

Pour tout $\sigma \in \mathfrak{S}_n^{\pm}$, nous avons $\Phi_{\mathbf{B_n}}(\sigma) = \widetilde{\Phi}_{\mathbf{B_n}}(\mathrm{Des}\,(\sigma))$. Une conséquence directe du lemme 4.21 est :

Proposition 4.28. *Pour tout $D = \{d_1 < \cdots < d_\ell\}$ appartenant à $\mathcal{D}_n$, avec $0 < d_1$, nous avons les relations :*

$$\widetilde{\Phi}_{\mathbf{B_n}}(D) = I_{k_1} \sqcup\!\sqcup P_{k_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup P_{k_{\ell+1}},$$
$$\widetilde{\Phi}_{\mathbf{B_n}}(\{0\} \cup D) = P_{k_1} \sqcup\!\sqcup P_{k_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup P_{k_{\ell+1}},$$

où $k_i = d_i - d_{i-1}$ pour $i \in [1, \ell+1]$ avec les conventions $d_0 = 0$, $d_{\ell+1} = n$.

Montrons maintenant que les applications ∂ et $\Phi_{\mathbf{B}}$ commutent. Nous commençons par établir des résultats intermédiaires.

Lemme 4.29. *Pour tout $\sigma \in \mathfrak{S}_n^{\pm}$ et tout $j \in [1, n]$, nous avons :*

$$\mathrm{Des}\left(\mathrm{del}_{|\sigma(j)|}(w(\sigma))\right) = \begin{cases} D_j & \text{si } \sigma(j-1) < \sigma(j+1)\,; \\ D_j \cup \{j-1\} & \text{si } \sigma(j-1) > \sigma(j+1), \end{cases}$$

où $D_j = \mathrm{Des}\,(\sigma) \cap [0, j-2] \cup \{d-1 \,|\, d \in \mathrm{Des}\,(\sigma) \cap [j+1, n]\}$, et encore avec la convention $\sigma(0) = 0$.

Démonstration. Notons u le mot $w(\sigma)$ et posons $i = |\sigma(j)|$. Nous notons aussi par v le mot $\mathrm{del}_i(u)$ et par τ la permutation $\rho(v)$. Le mot $v = v_1 \cdots v_{n-1}$ est alors donné par

$$v_k = \begin{cases} u_k\langle i\rangle & \text{si } k \leqslant j-1, \\ u_{k+1}\langle i\rangle & \text{si } k \geqslant j, \end{cases}$$

où u_k et v_k sont les k-ème lettres de u et v respectivement. Pour $k \in [0, n-1]$, nous avons $u_k\langle i\rangle > u_{k+1}\langle i\rangle$ si et seulement si $u_k > u_{k+1}$. Ainsi, un entier k de $[0, j-2]$ est une descente de τ si et seulement si k est une descente de σ. De même, un entier k de $[j, n-2]$ est une descente de τ si et seulement si $k+1$ est une descente de σ. En considérant les ensemble D_j de l'énoncé, nous avons :

$$\mathrm{Des}\,(\tau) \cap ([0, n-2] \setminus \{j-1\}) = D_j.$$

Nous ne pouvons pas déterminer si $j-1$ est une descente de τ à partir de $\mathrm{Des}\,(\sigma)$. Remarquons seulement que l'entier $j-1$ est une descente de τ si et seulement si nous avons $v_{j-1} > v_j$, et donc si et seulement si $u_{j-1} > u_{j+1}$. □

Lemme 4.30. *Soient σ une permutation signée de $\mathfrak{S}_n^{\pm}$ et $\{d_1 < \cdots < d_\ell\}$ ses descentes non nulles. Pour tout i de $[1,\ell]$, nous avons :*

$$\mathrm{Des}\left(\sum_{e=d_i+1}^{d_{i+1}} \partial_n^{|\sigma(e)|}(\sigma)\right) = (d_{i+1}-d_i-2)\mathrm{Des}\,(\sigma)\langle d_{i+1}\rangle\,, \tag{3.7}$$

avec les conventions $d_{\ell+1} = n$. De plus, nous avons :

$$\mathrm{Des}\left(\sum_{e=1}^{d_1} \partial_n^{|\sigma(e)|}(\sigma)\right) = \begin{cases} (d_1-1)\mathrm{Des}\,(\sigma)\langle d_1\rangle & \text{si } 0 \notin \mathrm{Des}\,(\sigma), \\ (d_1-2)\mathrm{Des}\,(\sigma)\langle d_1\rangle & \text{si } 0 \in \mathrm{Des}\,(\sigma). \end{cases} \tag{3.8}$$

Démonstration. Soit i un entier de l'intervalle $[1,\ell]$. Comme à la définition 4.6 nous utilisons la convention $\sigma(n+1) = -\infty$. Nous commençons par établir (3.7) à partir de trois cas.

Cas $d_{i+1} > d_i + 2$. Nous avons :

$$\sigma(d_i) > \sigma(d_i+1) < \cdots < \sigma(d_{i+1}-1) < \sigma(d_{i+1}) > \sigma(d_{i+1}+1).$$

Par définition de sign, les termes $\partial_n^{|\sigma(d_i+1)|}(\sigma)$ et $\partial_n^{|\sigma(d_{i+1})|}(\sigma)$ sont nuls. Pour un entier e de $[d_i+2, d_{i+1}-1]$, la valeur de $\mathrm{sign}_{|\sigma(e)|}(w(\sigma))$ est 1. Par le lemme 4.29 et la relation $\sigma(e-1) < \sigma(e+1)$, nous avons :

$$\begin{aligned} \mathrm{Des}\left(\rho\left(\mathrm{del}_{|\sigma(e)|}(w(\sigma))\right)\right) &= \mathrm{Des}\,(\sigma) \cap [0, e-2] \cup \{d-1 \,|\, d \in \mathrm{Des}\,(\sigma) \cap [e+1, n]\} \\ &= \{d_1, \ldots, d_i, d_{i+1}-1, \ldots, d_\ell - 1\} \\ &= \mathrm{Des}\,(\sigma)\langle d_{i+1}\rangle\,. \end{aligned}$$

Nous concluons en remarquant que le cardinal de $[d_i+2, d_{i+1}-1]$ est $d_{i+1}-d_i-2$.

Cas $d_{i+1} = d_i + 2$. Nous avons :

$$\sigma(d_i) > \sigma(d_i+1) < \sigma(d_{i+1}) > \sigma(d_{i+1}+1).$$

Comme pour $e \in [d_i+1, d_{i+1}]$, nous avons $\mathrm{sign}_{|\sigma(e)|}(w(\sigma)) = 0$, le terme de gauche de (3.7) est 0.

Cas $d_{i+1} = d_i + 1$. Nous avons

$$\sigma(d_i) > \sigma(d_{i+1}) > \sigma(d_{i+1}+1).$$

Dans ce cas $\mathrm{sign}_{|\sigma(d_{i+1})|}(w(\sigma))$ vaut -1. Par le lemme 4.29, les descentes de $\mathrm{del}_{|\sigma(d_i+1)|}(w(\sigma))$ sont :

$$\{d_1, \ldots, d_{i-1}, d_{i+1}-1, \ldots, d_k - 1\} \cup \{d_i\} = \mathrm{Des}\,(\sigma)\langle d_{i+1}\rangle$$

comme $\sigma(d_i) > \sigma(d_i+2)$ est vérifiée. Nous concluons en remarquant que $d_{i+1}-d_i-2 = -1$ est vérifiée dans ce cas.

La relation (3.8) est établie de la même façon avec une attention particulière pour 0. □

Théorème 4.31. *Les endomorphismes $\Phi_{\mathbf{B}}$ et ∂ commutent.*

Démonstration. Soit σ une permutation signée de $\mathfrak{S}_n^{\pm}$. Notons $\{d_1 < \cdots < d_\ell\}$ les descentes non nulles de σ. Pour $i \in [1, \ell+1]$ nous notons par k_i les entiers $d_i - d_{i-1}$, avec la convention $d_0 = 0$ et $d_{\ell+1} = n$. Pour $k \in \mathbb{N}$, nous définissons X_k et x_k par :

$$X_k = \begin{cases} I_k & \text{pour } 0 \notin \mathrm{Des}\,(\sigma), \\ P_k & \text{pour } 0 \in \mathrm{Des}\,(\sigma)\,; \end{cases} \quad \text{et} \quad x_k = \begin{cases} k-1 & \text{pour } 0 \notin \mathrm{Des}\,(\sigma), \\ k-2 & \text{pour } 0 \in \mathrm{Des}\,(\sigma). \end{cases}$$

Par la proposition 4.28, nous avons $\Phi_{\mathbf{B}}(\sigma) = \widetilde{\Phi}_{\mathbf{B}}(\mathrm{Des}\,(\sigma)) = X_{k_1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{\ell+1}}$. Comme par le corollaire 4.24, ∂ est une dérivation, la relation précédente donne

$$\begin{aligned} (\partial \circ \Phi_{\mathbf{B}})(\sigma) =& \partial(X_{k_1}) \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{\ell+1}} \\ &+ \sum_{i=2}^{\ell+1} X_{k_1} \sqcup \cdots \sqcup P_{k_{i-1}} \sqcup \partial(P_{k_i}) \sqcup P_{k_{i+1}} \cdots \sqcup P_{k_{\ell+1}}, \end{aligned}$$

En utilisant le lemme 4.23, nous obtenons :

$$(\partial \circ \Phi_{\mathbf{B}})(\sigma) = x_{k_1} X_{k_1-1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{\ell+1}} + \sum_{i=2}^{\ell+1} (k_i - 2) X_{k_1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{i-1}} \sqcup P_{k_i - 1} \sqcup P_{k_{i+1}} \sqcup \cdots \sqcup P_{k_{\ell+1}}.$$

Par ailleurs le lemme 4.30 garantit :

$$\mathrm{Des}\,(\partial(\sigma)) = x_{k_1} \mathrm{Des}\,(\sigma)\langle d_1 \rangle + \sum_{i=2}^{\ell+1} (k_i - 2) \mathrm{Des}\,(\sigma)\langle d_i \rangle\,. \tag{3.9}$$

Par la proposition 4.28, nous obtenons :

$$\widetilde{\Phi}_{\mathbf{B_n}}(\mathrm{Des}\,(\sigma)\langle d_1 \rangle) = X_{k_1-1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{\ell+1}},$$

et pour i dans $[2, n]$ nous avons :

$$\widetilde{\Phi}_{\mathbf{B_n}}(\mathrm{Des}\,(\sigma)\langle d_i \rangle) = X_{k_1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{i-1}} \sqcup P_{k_i - 1} \sqcup P_{k_{i+1}} \sqcup \cdots \sqcup P_{k_{\ell+1}},$$

ce qui par la relation 3.9 donne

$$\widetilde{\Phi}_{\mathbf{B_n}}(\mathrm{Des}\,(\partial(\sigma))) = x_{k_1} X_{k_1-1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{\ell+1}} + \sum_{i=2}^{n} (k_i - 2) X_{k_1} \sqcup P_{k_2} \sqcup \cdots \sqcup P_{k_{i-1}} \sqcup P_{k_i - 1} \sqcup P_{k_{i+1}} \sqcup \cdots \sqcup P_{k_{\ell+1}}.$$

Grâce à $(\Phi_{\mathbf{B}} \circ \partial)(\sigma) = (\widetilde{\Phi}_{\mathbf{B_n}}(\mathrm{Des}\,(\partial(\sigma))))$, nous avons ainsi établi $(\Phi_{\mathbf{B}} \circ \partial)(\sigma) = (\partial \circ \Phi_{\mathbf{B}})(\sigma)$. □

Nous pouvons maintenant démontrer le théorème 2.19.

Démonstration du théorème 2.19. Soit n un entier. Le corollaire 4.24 donne que l'application ∂ est une dérivation surjective de $\mathbb{Q}\mathfrak{S}^{\pm}$ qui, par le théorème 4.31, commute avec Φ. La proposition 4.4 garantit que le polynôme caractéristique de Φ_n divise celui de Φ_{n+1}. Comme le polynôme caractéristique de Φ_n est celui de $\mathrm{Adj}^{+}_{\mathbf{B_n}}$, nous obtenons le résultat de divisibilité escompté. □

5 Autres types

Dans cette section, nous discutons de ce que devient le résultat de divisibilité pour les autres familles de Coxeter infinies et nous décrivons la combinatoire des suites normales pour certains types exceptionnels.

Soit $\mathbf{\Gamma}$ un diagramme de Dynkin de type sphérique. La taille de la matrice $\mathrm{Adj}^{+}_{\Gamma}$ est exactement le nombre d'éléments de $W_{\mathbf{\Gamma}}$ et a donc une croissance exponentielle en n pour les familles $\mathbf{A_n}, \mathbf{B_n}$ et $\mathbf{D_n}$.

La définition de descente donnée en 2.9 possède un analogue dans $W_{\mathbf{\Gamma}}$ pour tout $\mathbf{\Gamma}$, voir [9] par exemple.

Définition 5.1. Pour un diagramme de Dynkin de type sphérique $\mathbf{\Gamma}$, nous posons $\mathrm{Des}\,(\mathbf{\Gamma})$ l'ensemble des parties des sommets de $\mathbf{\Gamma}$.

L'ensemble $\mathrm{Des}\,(\mathbf{\Gamma})$ est aussi l'ensemble des descentes possibles pour un élément de $W_{\mathbf{\Gamma}}$.

Définition 5.2. Pour un diagramme de Dynkin de type sphérique $\mathbf{\Gamma}$ nous définissons une matrice carrée $\mathrm{Adj}'_{\mathbf{\Gamma}} = (a'_{I,J})$ indexée par $\mathrm{Des}\,(\mathbf{\Gamma})$ par :

$$a'_{I,J} = \mathrm{card}\left(w \in W_{\mathbf{\Gamma}} \mid \mathrm{Des}\left(w^{-1}\right) = I \text{ et } J \subseteq \mathrm{Des}\,(w)\right).$$

Pour $\mathbf{\Gamma}$ valant $\mathbf{A_n}, \mathbf{B_n}$ et $\mathbf{D_n}$, la matrice $\mathrm{Adj}'_{\mathbf{\Gamma}}$ est de dimension 2^n tandis que la matrice $\mathrm{Adj}^+_{\mathbf{\Gamma}}$ est de dimension $(n+1)!$, $2^n n!$ et $2^{n-1}n!$ respectivement.

Notation 5.3. Pour un diagramme de Dynkin de type sphérique $\mathbf{\Gamma}$ et $J \subseteq \mathrm{Des}\,(\mathbf{\Gamma})$ nous notons $b_{\mathbf{\Gamma},d}(J)$ le nombre de tresses positives de $B^+_{\mathbf{\Gamma}}$ dont la forme normale de Garside est $(r(w_1), \ldots, r(w_d))$ avec $\mathrm{Des}\,(w_d) \subset J$.

Une adaptation immédiate du lemme 2.12 de [30] donne :

Lemme 5.4. *Pour tout diagramme de Dynkin $\mathbf{\Gamma}$ de type sphérique, il existe un entier k tel que le polynôme caractéristique $\chi_{\mathbf{\Gamma}}(x)$ de $\mathrm{Adj}^+_{\mathbf{\Gamma}}$ soit égal à $x^k\chi'_{\mathbf{\Gamma}}(x)$ où $\chi'_{\mathbf{\Gamma}}(x)$ est le polynôme caractéristique de $\mathrm{Adj}'_{\mathbf{\Gamma}}$. De plus pour $d \geqslant 1$ et $J \subset \mathrm{Des}\,(\mathbf{\Gamma})$, nous avons :*

$$b_{\mathbf{\Gamma},d}(J) = {}^tY\,(\mathrm{Adj}'_\Gamma)^{d-1}J \quad \textit{où} \quad Y_I = \begin{cases} 0 & \textit{si } I = \emptyset, \\ 1 & \textit{sinon.} \end{cases}$$

Afin de déterminer les nombres $b_{\mathbf{\Gamma},d}$ de tresses de $B^+_{\mathbf{\Gamma}}$ dont la longueur de Garside est d à partir de $\mathrm{Adj}'_{\mathbf{\Gamma}}$, nous utilisons un principe d'inclusion exclusion.

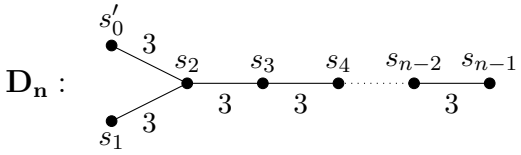
Corollaire 5.5. *Soit $\mathbf{\Gamma}$ un diagramme de Dynkin de type sphérique. Pour tout $d \geqslant 1$, nous avons :*

$$b_{\mathbf{\Gamma},d} = {}^tY\,(\mathrm{Adj}'_\Gamma)^{d-1}Z \quad \textit{où} \quad Z_I = \begin{cases} 0 & \textit{si } I = \emptyset, \\ (-1)^{\mathrm{card}(I)+1} & \textit{sinon,} \end{cases}$$

et où le vecteur Y est comme au lemme 5.4.

5.1 Tresses positives de type D.

Pour $n \geqslant 4$, le diagramme de Dynkin $\mathbf{D_n}$ est :



et le groupe de Coxeter $W_{\mathbf{D_n}}$ est isomorphe au sous-groupe de $\mathfrak{S}^{\pm}_{n+1}$ constitué des permutations signées ayant une notation fenêtrée contenant un nombre pair de valeurs négatives. Ses générateurs sont les permutations non signées s_i pour $i \in [1, n-1]$, plus la permutation signée $s'_0 = (-2, -1, 3, \ldots, n)$. Nous étendons la famille $\mathbf{D}_n$, initialement définie pour $n \geqslant 4$, en posant $\mathbf{D_1} = \mathbf{A_1}$, $\mathbf{D_2} = \mathbf{A_1} \times \mathbf{A_1}$ et $\mathbf{D_3} = \mathbf{A_3}$. Remarquons que nous considérons habituellement $n \geqslant 4$ afin d'avoir une classification des groupes de Coxeter finis irréductibles, sans doublons.

En notant $\chi_{\mathbf{D_n}}$ le polynôme caractéristique de la matrice d'adjacence $\mathrm{Adj}^+_{\mathbf{D_n}}$ des suites normales de tresses positives de type $\mathbf{D_n}$ nous obtenons

$$\begin{aligned}
\chi_{\mathbf{D_1}}(x) &= (x-1)^2, \\
\chi_{\mathbf{D_2}}(x) &= (x-1)^4, \\
\chi_{\mathbf{D_3}}(x) &= x^{19}\,(x-1)^2\,(x-2)\,(x^2-6x+3), \\
\chi_{\mathbf{D_4}}(x) &= x^{181}\,(x-1)^6\,(x^5-44x^4+402x^3-1084x^2+989x-360), \\
\chi_{\mathbf{D_5}}(x) &= x^{1906}\,(x-1)^2\,(x^{12}-302x^{11}+17070x^{10}-328426x^9+3077800x^8 \\
&\qquad -16424030x^7+4072794x^6-113921686x^5+154559655x^4 \\
&\qquad -132533636x^3+68372600x^2-18880000x+2016000).
\end{aligned}$$

Comme le lecteur peut le constater, nous ne pouvons pas espérer que le polynôme $\chi_{\mathbf{D_n}}$ divise $\chi_{\mathbf{D_{n+1}}}$, excepté pour $n = 1$. Les séries génératrices associées sont :

$$F^+_{\mathbf{D_2}}(t) = \frac{3-t}{(t-1)^2},$$
$$F^+_{\mathbf{D_3}}(t) = \frac{-6t^3+15t^2-20t+23}{(t-1)(2t-1)(3t^2-6t-1)},$$
$$F^+_{\mathbf{D_4}}(t) = \frac{-360t^5+1709t^4-2246t^3+852t^2+430t+191}{(t-1)(-1+44t-402t^2+1084t^3-989t^4+360t^5)}.$$

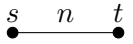
Nous obtenons ainsi les valeurs suivantes pour le nombre $b^+_{\mathbf{D_n},d}$ de tresses positives de type $\mathbf{D_n}$ et de longueur de Garside d :

d	$b^+_{\mathbf{D_2},d}$	$b^+_{\mathbf{D_3},d}$	$b^+_{\mathbf{D_4},d}$
0	1	23	191
1	3	187	9025
2	5	1169	321791
3	7	6697	10737025
4	9	37175	352664255
5	11	203971	11540908225

Question 5.6. Pour quelle raison a t-on $\chi_{\mathbf{A_n}} \mid \chi_{\mathbf{A_{n+1}}}$ et $\chi_{\mathbf{B_n}} \mid \chi_{\mathbf{B_{n+1}}}$ mais pas $\chi_{\mathbf{D_n}} \mid \chi_{\mathbf{D_{n+1}}}$?

5.2 Tresses positives de type $\mathbf{I_n}$.

Pour $n \geqslant 2$, le diagramme de Dynkin de $\mathbf{I_n}$ est :

$\mathbf{I_n}$: 

,

ce qui donne la présentation suivante du groupe de Coxeter $W_{\mathbf{I_n}}$:

$$W_{\mathbf{I_n}} = \left\langle s,t \;\middle|\; \begin{array}{c} s^2=1, t^2=1 \\ \mathrm{prod}(s,t;n) = \mathrm{prod}(t,s;n) \end{array} \right\rangle.$$

Proposition 5.7. *Pour $n \geqslant 2$, nous avons :*

$$\mathrm{Adj}'_{\mathbf{I_n}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ n-1 & b_n & a_n & 0 \\ n-1 & a_n & b_n & 0 \\ n & 1 & 1 & 1 \end{bmatrix},$$

avec $a_n = \lfloor \frac{n-1}{2} \rfloor$ et $b_n = \lfloor \frac{n}{2} \rfloor$.

Démonstration. Les éléments de $W_{\mathbf{I_n}}$ sont 1, $w_{\mathbf{I_n}} = \mathrm{prod}(s,t;n) = \mathrm{prod}(t,s;n)$ plus $\mathrm{prod}(s,t;k)$ et $\mathrm{prod}(t,s;k)$ pour k parcourant $[1, n-1]$. Pour k appartenant à $[1, n-1]$, nous avons :

$$\mathrm{prod}(s,t;k)^{-1} = \begin{cases} \mathrm{prod}(t,s;k) & \text{si } k \text{ est pair,} \\ \mathrm{prod}(s,t;k) & \text{sinon ;} \end{cases}$$
$$\mathrm{Des}\left(\mathrm{prod}(s,t;k)\right) = \begin{cases} t & \text{si } k \text{ est pair,} \\ s & \text{sinon.} \end{cases}$$

À partir des relations $\mathrm{prod}(s,t;n) = \mathrm{prod}(t,s;n)$ nous avons $w_n = \mathrm{prod}(s,t;n)^{-1} = \mathrm{prod}(s,t;n)$ et donc $\mathrm{Des}\,(w_n) = \{s,t\}$. Nous séparons les éléments de $W_{\mathbf{I_n}} \setminus \{1, w_{\mathbf{I_n}}\}$ en 4 parties :

$$X_1 = \{\mathrm{prod}(s,t;k) \text{ pour } k \text{ pair}\}, \qquad X_2 = \{\mathrm{prod}(s,t;k) \text{ pour } k \text{ impair}\},$$
$$X_3 = \{\mathrm{prod}(t,s;k) \text{ pour } k \text{ pair}\}, \qquad X_4 = \{\mathrm{prod}(t,s;k) \text{ pour } k \text{ impair}\}.$$

L'étude précédente des descentes nous donne :

$\sigma \in$	$\{1\}$	X_1	X_2	X_3	X_4	$\{w_{\mathbf{I_n}}\}$
$\mathrm{Des}\,(\sigma)$	$\emptyset$	$\{t\}$	$\{s\}$	$\{s\}$	$\{t\}$	$\{s,t\}$
$\mathrm{Des}\,(\sigma^{-1})$	$\emptyset$	$\{s\}$	$\{s\}$	$\{t\}$	$\{t\}$	$\{s,t\}$

En notant a_n et b_n les entiers $\lfloor \frac{n-1}{2} \rfloor$ et $\lfloor \frac{n}{2} \rfloor$, nous obtenons $\mathrm{card}\,(X_1) = \mathrm{card}\,(X_3) = a_n$ et $\mathrm{card}\,(X_2) = \mathrm{card}\,(X_4) = b_n$. Pour I et J des sous-ensembles de $\{s,t\}$ nous posons

$$A'_{I,J} = \{\sigma \in W_{\mathbf{I_n}} \,|\, \mathrm{Des}\,(\sigma^{-1}) = I \text{ et } J \subseteq \mathrm{Des}\,(\sigma)\}.$$

Pour tout $K \subset \{s,t\}$ nous avons $A'_{\{s,t\},K} = \{w_n\}$. On a $A'_{\emptyset,\emptyset} = \{1\}$ et $A'_{\emptyset,K} = \emptyset$ pour $K \neq \emptyset$. À partir de la définition des ensembles X_i nous obtenons :

$$A'_{\{s\},\emptyset} = X_1 \sqcup X_2, \quad A'_{\{s\},\{s\}} = X_2, \quad A'_{\{s\},\{t\}} = X_1, \quad A'_{\{s\},\{s,t\}} = \emptyset,$$
$$A'_{\{t\},\emptyset} = X_3 \sqcup X_4, \quad A'_{\{t\},\{s\}} = X_3, \quad A'_{\{t\},\{t\}} = X_4, \quad A'_{\{t\},\{s,t\}} = \emptyset.$$

En utilisant l'énumération $\{\emptyset, \{s\}, \{t\}, \{s,t\}\}$ des sous-ensembles de $\{s,t\}$ avec la relation $a_n + b_n = n-1$ nous obtenons :

$$\mathrm{Adj}'_{\mathbf{I_n}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ a_n+b_n & b_n & a_n & 0 \\ a_n+b_n & a_n & b_n & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ n-1 & b_n & a_n & 0 \\ n-1 & a_n & b_n & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \qquad \square$$

Corollaire 5.8. *Le polynôme caractéristique de* $\mathrm{Adj}^+_{\mathbf{I_n}}$ *est :*

$$\chi_{\mathbf{I_n}}(x) = \begin{cases} x^{2n-4}(x-1)^3(x-n+1) & \textit{si } x \textit{ est pair,} \\ x^{2n-3}(x-1)^2(x-n+1) & \textit{sinon,} \end{cases}$$

et la série génératrice du nombre de suites normales de tresse de type $\mathbf{I_n}$ *est :*

$$F^+_{\mathbf{I_n}}(t) = \frac{(n-1)t+1}{((n-1)t-1)(t-1)}.$$

Démonstration. La proposition 5.7 donne :

$$\begin{aligned} \chi_{\mathbf{I_n}}(x) &= (1-x)^2((b_n-x)^2 - a_n^2), \\ &= (1-x)^2(b_n+a_n-x)(b_n-a_n-x), \\ &= (x-1)^2(x-(b_n+a_n))(x-(b_n-a_n)). \end{aligned}$$

Des relations

$$a_n + b_n = n-1, \qquad b_n - a_n = \begin{cases} 1 & \text{si } n \text{ est pair,} \\ 0 & \text{sinon.} \end{cases}$$

nous obtenons :

$$\chi_{\mathbf{I_n}}(x) = \begin{cases} (x-1)^3(x-n+1) & \text{si } x \text{ est pair,} \\ x(x-1)^2(x-n+1) & \text{sinon.} \end{cases}$$

En ajoutant les puissances manquantes de x afin d'obtenir un polynôme de degré $2n$ nous obtenons la valeur annoncée pour $\chi_{\mathbf{I_n}}$. Concernant les séries génératrices, le corollaire 5.5 donne :

$$F^+_{\mathbf{I_n}}(t) = \begin{bmatrix}0 & 1 & 1 & 1\end{bmatrix} (I_4 - t\ \mathrm{Adj}'_{\mathbf{I_n}})^{-1} \begin{bmatrix}0\\1\\1\\-1\end{bmatrix}.$$

Par un calcul direct (ou en utilisant `Sage` [124] par exemple) nous obtenons :

$$F^+_{\mathbf{I_n}}(t) = \frac{(n-1)t+1}{((n-1)t-1)(t-1)}.$$ □

5.3 Tresses positives exceptionnelles

Le groupe $W_{\mathbf{F_4}}$ possède 1 152 éléments. Le polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{F_4}}$ est :

$$\begin{aligned}\chi_{\mathbf{F_4}}(x) =& x^{1140}\,(x-1)^3\,(x-4)\,(x^2-25\,x+10)\\ &(x^6-274\,x^5+9194\,x^4-77096\,x^3+250605\,x^2-324870\,x+138600),\end{aligned}$$

et la série génératrice $F^+_{\mathbf{F_4}}$ est donnée par :

$$F^+_{\mathbf{F}_4}(t) = \frac{138600\,t^6-187350\,t^5-32055\,t^4+87970\,t^3-15504\,t^2-876\,t-1}{(138600\,t^6-324870\,t^5+250605\,t^4-77096\,t^3+9194\,t^2-274\,t+1)(t-1)}.$$

Le groupe $W_{\mathbf{H_3}}$ possède 120 éléments. Le polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{H_3}}$ est :

$$\chi_{\mathbf{H_3}}(x) = x^{114}\,(x-1)^2\,(x^4-42\,x^3+229\,x^2-244\,x+72),$$

et la série génératrice $F^+_{\mathbf{H_3}}$ est donnée par :

$$F^+_{\mathbf{H_3}}(t) = -\frac{72\,t^4-196\,t^3+77\,t^2+76\,t+1}{(72\,t^4-244\,t^3+229\,t^2-42\,t+1)(t-1)}.$$

Le groupe $W_{\mathbf{H_4}}$ possèdent 14 400 éléments. Le polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{H_4}}$ est :

$$\begin{aligned}\chi_{\mathbf{H_4}}(x) = x^{14390}\,(x-1)^2\,(x^8&-3436\,x^7+565470\,x^6-11284400\,x^5+81322353\,x^4\\ &-246756500\,x^3+305430848\,x^2-157717504\,x+27929088),\end{aligned}$$

et la série génératrice $F^+_{\mathbf{H_4}}(t) = \frac{N_{\mathbf{H_4}}(t)}{D_{\mathbf{H_4}}(t)(t-1)}$ est donnée par

$$\begin{aligned}N_{\mathbf{H_4}}(t) &= 27929088\,t^8-147220480\,t^7+247258432\,t^6-138197780\,t^5\\ &\quad+465433\,t^4+10247814\,t^3-1205944\,t^2-10962\,t-1,\\ D_{\mathbf{H_4}}(t) &= 27929088\,t^8-157717504\,t^7+305430848\,t^6-246756500\,t^5\\ &\quad+81322353\,t^4-11284400\,t^3+565470\,t^2-3436\,t+1.\end{aligned}$$

Le groupe $W_{\mathbf{E_6}}$ possèdent 51 840 éléments. Le polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{E_6}}$ est :

$$\begin{aligned}\chi_{\mathbf{E_6}}(x) =& x^{51823}\,(x-1)^2\,(x^{15}-5454\,x^{14}+3391893\,x^{13}-424089882\,x^{12}+19590731031\,x^{11}\\ &-417118001254\,x^{10}+4673188683575\,x^9-29907005656510\,x^8+115900067128500\,x^7\\ &-282097630883500\,x^6+439789995997000\,x^5-441496921502000\,x^4+282303310340000\,x^3\\ &-110981554480000\,x^2+24563716800000\,x-2328480000000),\end{aligned}$$

et la série génératrice $F^+_{\mathbf{E_6}}(t) = \frac{N_{\mathbf{E_6}}(t)}{D_{\mathbf{E_6}}(t)(t-1)}$ est donnée par :

$$\begin{aligned}N_{\mathbf{E_6}}(t) =& 2328480000000\,t^{15} - 19422916800000\,t^{14} + 59384818480000\,t^{13} - 64287293380000\,t^{12}\\ &- 64835775106000\,t^{11} + 254118878161000\,t^{10} - 284082015723500\,t^9 + 148526420487700\,t^8\\ &- 32460183476310\,t^7 - 327255378405\,t^6 + 1042966224156\,t^5 - 93297805141\,t^4\\ &+ 479267710\,t^3 + 40099205\,t^2 + 46384\,t + 1,\end{aligned}$$

$$\begin{aligned}D_{\mathbf{E_6}}(t) =& 2328480000000\,t^{15} - 24563716800000\,t^{14} + 110981554480000\,t^{13} - 282303310340000\,t^{12}\\ &+ 441496921502000\,t^{11} - 439789995997000\,t^{10} + 282097630883500\,t^9 - 115900067128500\,t^8\\ &+ 29907005656510\,t^7 - 4673188683575\,t^6 + 417118001254\,t^5 - 19590731031\,t^4\\ &+ 424089882\,t^3 - 3391893\,t^2 + 5454\,t - 1.\end{aligned}$$

Le groupe $W_{\mathbf{E_7}}$ possèdent 2 903 040 éléments. Le polynôme caractéristique de $\mathrm{Adj}^+_{\mathbf{E_7}}$ est :

$$\begin{aligned}\chi_{\mathbf{E_7}}(x) =& x^{2903008}(x-1)^2(x^{30} - 214058\,x^{29} + 3482912203\,x^{28} - 7715217540884\,x^{27}\\ &+ 5551985616838969\,x^{26} - 1529651008431876022\,x^{25} + 205839509348251567567\,x^{24}\\ &- 15557852260875806821664\,x^{23} + 7254367232052618475553751\,x^{22}\\ &- 2241743675460348579037311 0\,x^{21} + 48313957974201502597741978 5\,x^{20}\\ &- 75238167128539346750702664 04\,x^{19} + 86820683327064787681782920963\,x^{18}\\ &- 75650216372822658726976335469 8\,x^{17} + 50512174505731703860038347782 29\,x^{16}\\ &- 26150530274469195713180210929096\,x^{15} + 10594459044753994216151628259972 4\,x^{14}\\ &- 33821563534649713491579548632854 4\,x^{13} + 85472361398778264669743862632496 8\,x^{12}\\ &- 17138214907835841086756876493287 36\,x^{11} + 27263536469959038120459326728167 04\,x^{10}\\ &- 34323603663342433266539151438309 12\,x^9 + 34023623337209785217770631463717 12\,x^8\\ &- 26339130087038062731267680267642 88\,x^7 + 15732751115829358419599397923942 40\,x^6\\ &- 71242787235817302290391339413913 6\,x^5 + 23829461029906713964326240239616 0\,x^4\\ &- 56571818111103214822209651671040\,x^3 + 89279598700010120762338836480 00\,x^2\\ &- 82945150879983670674063360000 0\,x + 33810888418479093841920000000)\end{aligned}$$

et la série génératrice $F^+_{\mathbf{E_7}}(t) = \frac{N_{\mathbf{E_7}}(t)}{D_{\mathbf{E_7}}(t)(t-1)}$ est donnée par :

$$\begin{aligned}N_{\mathbf{E_7}}(t) =& 33810888418479093841920000000\,t^{30} - 76889510889277871637135360000 0\,t^{29}\\ &+ 74665823019866497378135572480 00\,t^{28} - 41169708667899118886590120919040\,t^{27}\\ &+ 14322550854571647096934032261120 0\,t^{26} - 32462587163512829082107544429772 8\,t^{25}\\ &+ 45825695431408266880849504024780 8\,t^{24} - 28552484437044981554963671228108 8\,t^{23}\\ &- 30947922295640634627615138687321 6\,t^{22} + 10386237783694238408577864839919 36\,t^{21}\\ &- 14156290302790585663624026158768 00\,t^{20} + 12505007405332300853583598420838 72\,t^{19}\\ &- 78433697180639095617741391643784 8\,t^{18} + 35879462522527508540471654194913 6\,t^{17}\\ &- 11965386199057979654721081261394 0\,t^{16} + 28379013584798834803147551442288\,t^{15}\\ &- 44609009727504630063966054460 91\,t^{14} + 36039556570852125450367666907 6\,t^{13}\\ &+ 14848116603285422314577590827\,t^{12} - 80019662978831018688518170 80\,t^{11}\\ &+ 10353415397552638702592823 53\,t^{10} - 72667691774828924374585892\,t^9\\ &+ 28999216409337227556962 31\,t^8 - 57168263216921337105408\,t^7\\ &+ 19512411133774588665 5\,t^6 + 7835283652517485676\,t^5 - 70600575042276511\,t^4\\ &+ 32456066766312\,t^3 + 74706538803\,t^2 + 2688980\,t + 1\end{aligned}$$

$$
\begin{aligned}
D_{\mathbf{E_7}}(t) =& 338108884184790938419200000000\,t^{30} - 829451508799836706740633600000\,t^{29}\\
&+ 892795987000101207623388364800 0\,t^{28} - 565718181111032148222096516710 40\,t^{27}\\
&+ 238294610299067139643262402396160\,t^{26} - 712427872358173022903913394139136\,t^{25}\\
&+ 157327511158293584195993979239424 0\,t^{24} - 263391300870380627312676802676428 8\,t^{23}\\
&+ 340236233372097852177706314637171 2\,t^{22} - 343236036633424332665391514383091 2\,t^{21}\\
&+ 272635364699590381204593267281670 4\,t^{20} - 171382149078358410867568764932873 6\,t^{19}\\
&+ 854723613987782646697438626324968\,t^{18} - 338215635346497134915795486328544\,t^{17}\\
&+ 105944590447539942161516282599724\,t^{16} - 261505302744691957131802109290 96\,t^{15}\\
&+ 505121745057317038600383477822 9\,t^{14} - 756502163728226587269763354698\,t^{13}\\
&+ 868206833270647876817829209 63\,t^{12} - 752381671285393467507026640 4\,t^{11}\\
&+ 483139579742015025977419785\,t^{10} - 224174367546034857903731 10\,t^{9}\\
&+ 725436723205618475553751\,t^{8} - 15557852260875806821664\,t^{7}\\
&+ 205839509348251567567\,t^{6} - 1529651008431876022\,t^{5} + 5551985616838969\,t^{4}\\
&- 7715217540884\,t^{3} + 3482912203\,t^{2} - 214058\,t + 1.
\end{aligned}
$$

Les séries génératrices précédentes donnent les valeurs suivantes pour $b^+_{\mathbf{\Gamma},d}$, le nombre de tresses de type $\mathbf{\Gamma}$ et de longueur de Garside d :

d	$b^+_{\mathbf{F_4},d}$	$b^+_{\mathbf{H_3},d}$	$b^+_{\mathbf{H_4},d}$
0	1	1	1
1	1 151	119	14 399
2	322 561	4 923	50 126 401
3	77 804 927	179 717	164 094 364 799
4	184 41 371 521	64 49 741	535 645 654 732 801
5	4 362 177 487 103	230 926 603	1 748 252 504 973 355 199

d	$b^+_{\mathbf{E_6},d}$	$b^+_{\mathbf{E_7},d}$
0	1	1
1	51 839	2 903 039
2	319 483 603	692 645 037 843
3	1 567 574 732 717	138 195 427 545 246 957
4	7 487 770 421 878 165	27 191 736 432 214 478 848 469
5	35 655 729 684 940 971 035	5 344 613 975 019 990 021 840 686 635

Des fichiers contenant des informations sur la combinatoire des groupes exceptionnels à l'exception de $\mathbf{E_8}$ sont disponibles sur ma page internet [1].

1. `http://www.lmpa.univ-littoral.fr/~fromentin/index.php?title=Combinatorasaics_of_generalized_braids`

IV. Polynôme de Jones modulaire

Ce chapitre présente les résultats que j'ai obtenus avec S. Eliahou dans [50] sur le polynôme de Jones modulaire.

Pour tout entier $r \geqslant 1$, nous construisons une infinité de nœuds premiers dont le polynôme de Jones est trivial modulo $m = 2^r$. Notre construction est basée sur un enchevêtrement premier T_{20} à 20 croisements dont le polynôme crochet de Kauffman est trivial modulo 2.

La première section présente le contexte dans lequel nous avons obtenu nos résultats. La section 2 est consacrée aux enchevêtrements algébriques. Dans la section 3 nous décrivons l'enchevêtrement clé T_{20}, puis nous prouvons qu'il est premier. Nous construisons alors une famille de nœuds premiers K_r à partir de l'enchevêtrement M_r qui est composé de 2^{r-1} copies de l'enchevêtrement T_{20}. À la section 4, nous calculons la paire crochet de Kauffman de l'enchevêtrement M_r modulo 2^r. Finalement, à la section 5, nous prouvons que les nœuds K_r sont deux à deux distincts et que le polynôme de Jones de K_r est trivial modulo 2^r.

1 Introduction

Le polynôme de Jones est un invariant polynomial des entrelacs introduit en 1984 par V. Jones [84]. En 2001, M. B. Thistlethwaite [126] donne deux entrelacs à 2 composantes et un entrelacs à 3 composantes ayant le même polynôme de Jones que les entrelacs triviaux U^2 et U^3 à deux et trois composantes respectivement. Ce sont les premiers exemples connus d'entrelacs non triviaux indétectables par le polynôme de Jones. Peu de temps après, en 2003, S. Eliahou, L. Kauffman et M. B. Thistlethwaite [55] ont montré que, pour tout entier $k \geqslant 2$, il existe une infinité d'entrelacs à k–composantes ayant le même polynôme de Jones que l'entrelacs premiers trivial à k composantes U^k. Le problème pour les entrelacs à une composante, c'est-à-dire les nœuds, est largement ouvert :

Problème 1.1. Existe-t-il un nœud non trivial K dont le polynôme de Jones est égal à celui du nœud trivial U^1, à savoir 1 ?

Nous considérons maintenant le problème plus faible, consistant à trouver un nœud non trivial K dont le polynôme de Jones est *congruent modulo un certain entier* m à celui du nœud trivial U^1.

Problème 1.2. Etant donné un entier $m \geqslant 2$, existe-t-il un nœud non trivial K dont le polynôme de Jones $V(K)$ satisfait $V(K) \equiv 1 \mod m$?

Naturellement, pour deux polynômes de Laurent f et g de $\mathbb{Z}[t, t^{-1}]$, la notation $f \equiv g \mod m$ signifie qu'il existe un élément $h \in \mathbb{Z}[t, t^{-1}]$ tel qu'on ait $f - g = m \cdot h$. C'est équivalent à demander que, pour tout $i \in \mathbb{Z}$, les coefficients α_i et β_i de t^i dans f et g, respectivement, sont congruents modulo m comme entiers.

Un résultat de M. B. Thistlethwaite [125] de 1987 stipule que pour tout nœud K admettant un diagramme alternant avec n croisements, la largeur de $V(K)$ est exactement n et les coefficients des termes extrémaux sont tous les deux égaux à ± 1. Nous obtenons ainsi le premier résultat suivant.

Lemme 1.3. *Pour tout $m \geqslant 2$, il n'existe pas de nœud alternant non trivial ayant un polynôme de Jones trivial modulo m.*

À l'aide du paquet *Mathematica* `KnotTheory` du projet KnotAtlas, il est facile de trouver des nœuds solutions au problème 1.2 pour les modules $m = 2, 3$ et 4. La table suivante donne le nombre de nœuds premiers avec au plus 16 croisements solutions au problème 1.2 pour les modules 2 à 5.

m	$\leqslant 11$	12	13	14	15	16
2	0	4	9	35	140	582
3	0	1	0	1	2	26
4	0	0	0	0	1	0
5	0	0	0	0	0	0

2 Enchevêtrements

La notion d'enchevêtrement est au cœur de la construction de notre famille de nœuds K_r. Commençons par en donner une définition.

Définition 2.1. Un *enchevêtrement géométrique* est une paire (B, t), où B est une boule de $\mathbb{R}^3$ et t est une sous-variété propre de dimension 1 de B rencontrant le bord de B en quatre points distincts. Deux enchevêtrements géométriques sont considérés équivalents s'il existe une isotopie ambiante envoyant l'un sur l'autre mais laissant le bord de la boule fixe.

Soit (B, t) un enchevêtrement géométrique. Sans perte de généralité nous pouvons considérer que les quatre points d'intersection de la variété t avec la boule B se trouvent sur un grand cercle $\mathcal{C}$ de B. La projection de t sur le disque bordé par $\mathcal{C}$ nous donne un diagramme plan dans lequel nous veillons à bien indiquer la nature de chaque croisement : quel brin passe au-dessus de quel autre.

Définition 2.2. Un *enchevêtrement* est un diagramme plan possédant quatre extrémités marquées que nous obtenons comme projection d'un enchevêtrement géométrique.

Nous venons de voir comment obtenir un enchevêtrement à partir d'un enchevêtrement géométrique. Réciproquement, à chaque enchevêtrement T nous associons de manière naturelle un enchevêtrement géométrique (B, t) où B est une boule euclidienne de dimension 3 dont les bords rencontrent le plan de projection P sur un cercle "équatorial" circonscrivant l'enchevêtrement T et où t est obtenu de T (qui est dessiné dans P) en faisant de petites variations à proximité des croisements.

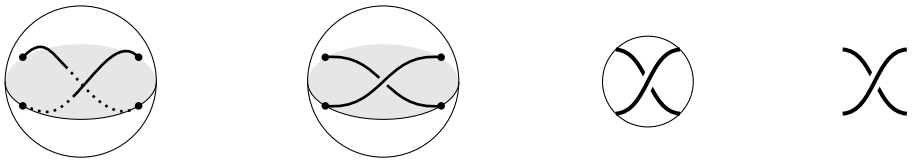


FIGURE 4.1 – Passage d'un enchevêtrement géométrique à un enchevêtrement. De la gauche vers la droite, nous avons : un enchevêtrement géométrique (B, t), projection de t sur le plan équatorial de B. Les deux dessins de droite représentent le même enchevêtrement. Le cercle permet de mieux délimiter l'enchevêtrement lorsqu'un même dessin en comporte plusieurs.

2.1 Enchevêtrements algébriques

Parmi la vaste famille des enchevêtrements nous nous intéressons en particulier à ceux dit *algébriques* qui peuvent être obtenus à partir d'enchevêtrements de base et de deux opérations.

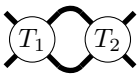
Voici les deux enchevêtrements qui vont nous servir de briques élémentaires.

Notation 2.3. Nous notons 1 et -1 les enchevêtrements

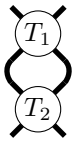
1 :  $\qquad -1$: 

Remarquons que l'on passe de 1 à -1 en inversant le signe du croisement. Plus généralement, si T est un enchevêtrement, alors $-T$ désigne l'enchevêtrement obtenu de T en échangeant les signes des croisements de T.

Définition 2.4. Soient T_1 et T_2 deux enchevêtrements. La *somme horizontale* de T_1 et T_2, notée $T_1 + T_2$, est l'enchevêtrement



La *somme verticale* de T_1 et T_2, notée $T_1 * T_2$ est l'enchevêtrement



Comme il en est l'usage nous donnons des noms à la somme de k copies (horizontale ou verticale) des enchevêtrements 1 et -1.

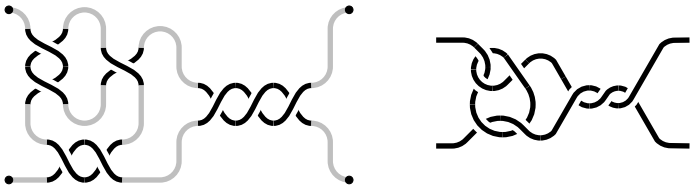
Définition 2.5. Pour $k \in \mathbb{N}_+$, nous définissons les enchevêtrements

$k = 1 + \cdots + 1$:  $\qquad -k = (-1) + \cdots + (-1)$: 

$1/k = 1 * \cdots * 1$:  $\qquad -1/k = (-1) * \cdots * (-1)$: 

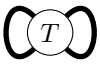
avec k termes dans chaque écriture.

Exemple 2.6. Notons $T_{8,21}$ l'enchevêtrement $(((1/2)+1)*2)+(-3)$. Un diagramme de $T_{8,21}$ est

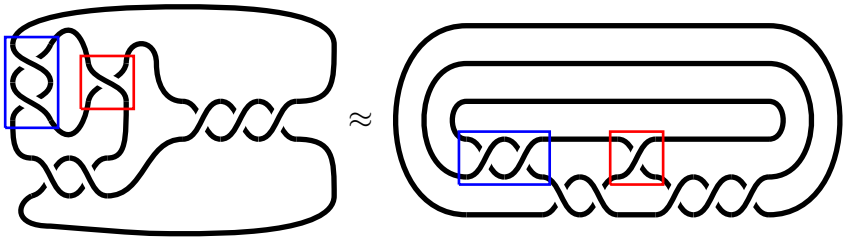


Les morceaux en noir dans le diagramme de gauche correspondent aux enchevêtrements $1/2$, 1, 2 et -3, respectivement, tandis que les arcs gris représentent les connexions entre eux. Les quatre points marqués sont les extrémités de l'enchevêtrement global. Le diagramme le plus à droite est une version "lissée" de l'enchevêtrement $T_{8,21}$.

Définition 2.7. Les *clôtures* d'un enchevêtrement T, notées $\mathrm{den}(T)$ et $\mathrm{num}(T)$, sont données par les diagrammes d'entrelacs obtenus en recollant les extrémités de T :

$\mathrm{den}(T) =$  $\qquad\qquad \mathrm{num}(T) =$ 

Exemple 2.8. Reconsidérons l'enchevêtrement $T_{8,21}$ de l'exemple 2.6. La clôture $\mathrm{num}(T_{8,21})$ admet le diagramme :



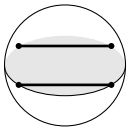
L'isotopie est obtenue à partir du diagramme de gauche en tournant dans le sens contraire des aiguilles d'une montre le bloc bleu, et dans le sens des aiguilles d'une montre celui en rouge. Le diagramme est caractérisé par la tresse à 3 brins

$$\sigma_2^{-1}\sigma_2^{-1}\sigma_1\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_1^{-1}\sigma_1^{-1}.$$

En consultant les tables de nœuds de D. Rolfsen [113], nous remarquons que $\mathrm{num}(T_{8,21})$ est un diagramme du 21ème nœud premier à 8 croisements $K_{8,21}$.

3 Théorie de Lickorish des enchevêtrements premiers

Définition 3.1. Un enchevêtrement géométrique (B,t) est *démêlé* s'il est isotopique à la paire (B,t_0), où t_0 est la réunion de deux lignes droites parallèles tracées dans le plan de projection.



Un enchevêtrement est *démêlé* s'il est la projection d'un enchevêtrement géométrique démêlé.

Définition 3.2. Un enchevêtrement géométrique (B, t) est *premier* s'il possède les propriétés suivantes :

(*i*) (B, t) est non démêlé ;

(*ii*) toute sphère de dimension 2 tracée dans B, qui rencontre t de manière transversale en deux points, délimite dans B une boule rencontrant t en un arc non noué.

Un enchevêtrement est *premier* s'il est la projection d'un enchevêtrement géométrique premier.

Comme le montrent les résultats suivants de W. B. R. Lickorish, obtenus en 1981, il est relativement aisé d'obtenir des entrelacs premiers à partir d'enchevêtrements premiers.

Théorème 3.3 (Théorème 1 de [91])**.** *Si T et U sont des enchevêtrements premiers, alors* $\mathrm{num}(T + U)$ *et* $\mathrm{den}(T * U)$ *sont des entrelacs premiers.*

Théorème 3.4 (Théorème 3 de [91])**.** *Si T est un enchevêtrement premier ou démêlé et U est un enchevêtrement premier alors $T + U$ est un enchevêtrement premier.*

Le résultat suivant, inspiré de l'exemple de la figure **2.a** de [91], nous donne un critère efficace pour établir qu'un enchevêtrement donné est premier.

Proposition 3.5. *Soit T un enchevêtrement non démêlé. Si $T +$*  *est isotope à*  *alors l'enchevêtrement T est premier.*

Démonstration. Soit T un enchevêtrement non démêlé. Notons (B, t) l'enchevêtrement géométrique non démêlé associé à T. Supposons qu'il existe une boule dans (B, t) rencontrant t en un arc noué. Cette paire *boule/arc* est toujours présente dans $T +$ puis dans $\mathrm{num}(T +$ $)$. Par hypothèse nous avons que $\mathrm{num}(T +$ $)$ est isotope à $\mathrm{num}($$)$, qui est lui-même isotope à . Comme le noeud ne possède pas de portion d'arc noué nous avons une contradiction et donc (B, t), puis T, sont premiers. □

3.1 Une famille de nœuds

Nous allons maintenant construire une famille de nœuds qui nous fournira des solutions au problème 1.2 lorsque m est une puissance de 2. Pour cela nous commençons par introduire une famille d'enchevêtrements $(M_r)_{r \geqslant 1}$.

Définition 3.6. Nous définissons des enchevêtrements T_{10}, T_{20} et M_r pour $r \geq 1$ en posant :

(*i*) $T_{10} = T_{8,21} * 2 = ((((1/2) + 1) * 2) + (-3)) * 2$;

(*ii*) $T_{20} = T_{10} + (-T_{10})$;

(*iii*) $M_1 = T_{20}$ et $M_r = M_{r-1} + M_{r-1}$ pour $r \geqslant 2$.

L'enchevêtrement M_1 est dessiné à la figure 4.2.

Pour $r \geqslant 2$, l'enchevêtrement M_r est ainsi obtenu en additionnant horizontalement 2^{r-1} copies de l'enchevêtrement T_{20}. Notons que T_{10} et T_{20} possèdent respectivement 10 et 20 croisements.

Lemme 3.7. *Les enchevêtrements T_{10} et $-T_{10}$ sont premiers.*

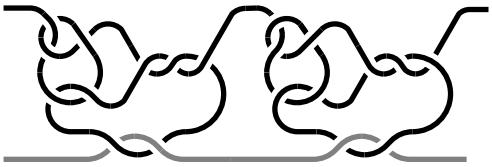
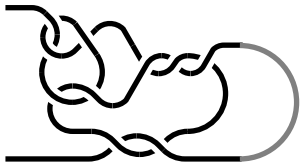
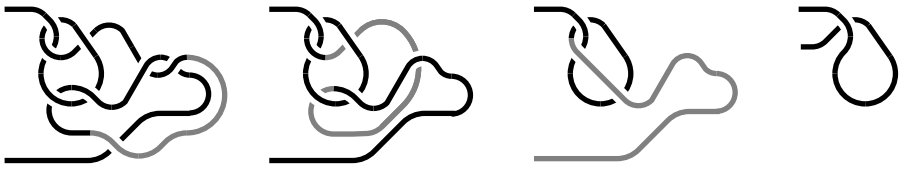


FIGURE 4.2 – L'enchevêtrement clé $M_1 = T_{20}$. Observons que les deux extrémités SW et SE sont reliées par un même arc (en gris).

Démonstration. En reliant les extrémités NE et SE de T_{10} nous obtenons le diagramme suivant :



Grâce à la suite de déformations suivante (où nous avons dessiné le fragment déformé en gris),



nous obtenons que $T_{10} +$ ❩❨ est isotope à ❩❨. L'arc joignant les extrémités nord de T_{10} ne peut pas être démêlé. Donc, par la proposition 3.5, l'enchevêtrement T_{10} est premier. Comme l'enchevêtrement $-T_{10}$ est obtenu de T_{10} en échangeant les signes des croisements, il est lui aussi premier. □

Proposition 3.8. *Pour tout $r \geqslant 1$, l'enchevêtrement M_r est premier.*

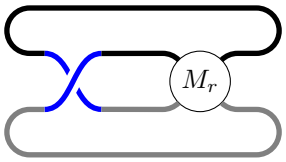
Démonstration. Comme T_{10} et $-T_{10}$ sont des enchevêtrements premiers par le lemme 3.7, le théorème 3.4 implique que l'enchevêtrement $M_1 = T_{20} = T_{10} + (-T_{10})$ est aussi premier. Par une induction directe sur r en utilisant le théorème 3.4, nous concluons que l'enchevêtrement M_r est premier pour tout $r \geqslant 1$. □

Définition 3.9. Pour tout $r \in \mathbb{N}_+$, nous définissons K_r comme étant l'entrelacs de diagramme $\mathrm{num}(1 + M_r)$.

Par construction, l'enchevêtrement M_r possède $2^{r-1} \times 20$ croisements. Ainsi l'entrelacs K_r a au plus $1 + 2^r \times 10$ croisements.

Proposition 3.10. *Pour chaque $r \geqslant 1$, l'entrelacs K_r est un nœud premier avec au plus $1 + 2^r \times 10$ croisements.*

Démonstration. Comme nous l'observons qur la figure 4.2 enchevêtrement M_1 est consitué de deux arcs, le premier allant du NW au NE et le second du SW au SE. Par construction, les enchevêtrements M_r pour $r \geqslant 1$ vérifient tous cette propriété. Comme illustré par le dessin suivant



le diagramme d'entrelacs $\mathrm{num}(1+M_r)$ a une seule composante : si nous voyageons le long de l'arc noir, passant par les points NW et NE de M_r, nous devons rencontrer celui en gris. L'entrelacs K_r est donc un nœud avec au plus $1+2^r\times 10$ croisements. Il reste à établir que K_r est premier. Pour $r=1$ nous avons

$$K_1=\mathrm{num}(1+M_1)=\mathrm{num}((1+T_{10})+(-T_{10})).$$

Par le lemme 3.7 et la proposition 3.5 les enchevêtrements T_{10} et $-T_{10}$ sont premiers. Le théorème 3.4 implique alors que $1+T_{10}$ est aussi premier. Nous concluons en utilisant le théorème 3.3. Pour $r\geqslant 2$, nous avons

$$K_r=\mathrm{num}(1+M_r)=\mathrm{num}((1+M_{r-1})+M_{r-1}).$$

En utilisant la proposition 3.8 et le théorème 3.4 nous avons que les enchevêtrements M_{r-1} et $1+M_{r-1}$ sont premiers. Le nœud K_r est donc premier par le théorème 3.3. □

Pour tout $r\geqslant 1$, un nœud mutant K'_r est obtenu de K_r en remplaçant l'enchevêtrement $-T_{10}$ de chaque sommant M_1 de M_r par son image par symétrie verticale. Les nœuds K_r et K'_r, étant mutants l'un de l'autre, ils possèdent le même polynôme de Jones [84]. Le nœud K'_1 est dessiné à la figure 4.3.

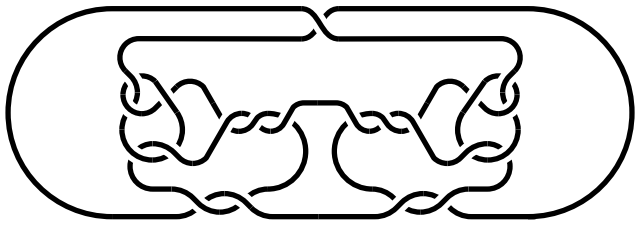


FIGURE 4.3 – Version élégante, ressemblant à un crabe, du mutant K'_1 du nœud K_1. Pour des raisons esthétiques, nous avons utilisé une isotopie pour déplacer l'enchevêtrement 1 de $1+M_1$ au dessus du dessin.

4 La paire crochet de Kauffman

Dans cette section, nous rappelons la définition de la paire crochet de Kauffman d'un enchevêtrement, qui sera utilisée pour calculer le polynôme de Jones de nos nœuds K_r.

Notation 4.1. Pour tout enchevêtrement T, nous notons $f(T)$ et $g(T)$ les uniques polynômes de $\mathbb{Z}[t,t^{-1}]$ tels que nous ayons $\langle T\rangle = f(T)\,\langle \asymp\rangle + g(T)\,\langle)(\rangle$ et où $\langle T\rangle$ est obtenu en appliquant les règles de calcul

- $\langle \bigcirc\rangle = 1$;
- $\langle \times\rangle = t^{-1}\,\langle \asymp\rangle + t\,\langle)(\rangle$;
- $\langle \bigcirc \amalg U\rangle = \delta\,\langle T\rangle$ avec $\delta=-t^{-2}-t^2$ où U est un enchevêtrement quelconque.

Définition 4.2. La *paire crochet de Kauffman* d'un enchevêtrement T, notée $\beta(T)$, est

$$\beta(T)=\begin{bmatrix} f(T)\\ g(T)\end{bmatrix}\in\mathbb{Z}[t,t^{-1}]^2, \tag{4.1}$$

où les polynômes $f(T)$ et $g(T)$ sont introduits à la notation 4.1. De plus pour tout entier $m\geqslant 2$, nous notons β_m la paire crochet de Kauffman de T modulo m.

Exemple 4.3. Nous calculons

$$\langle -1\rangle = \langle \times \rangle = t^{-1}\,\langle \asymp \rangle + t\,\langle)\,(\rangle\,,$$

ce qui implique

$$\beta(-1) = \begin{bmatrix} t^{-1} \\ t \end{bmatrix}.$$

Par définition de $-T$, nous avons $f(-T) = f(T)|_{t\leftarrow t^{-1}}$ et $g(-T) = g(T)|_{t\leftarrow t^{-1}}$ et donc nous obtenons aussi

$$\beta(1) = \begin{bmatrix} t \\ t^{-1} \end{bmatrix}.$$

Comme le montre la proposition suivante les sommes horizontales, verticales et les clôtures d'enchevêtrement possèdent un bon comportement vis-à-vis de la paire crochet de Kauffman.

Proposition 4.4 (Proposition 2.2 de [55])**.** *Pour deux enchevêtrements T et U, nous avons :*

(i) $\beta(T{+}U) = \begin{bmatrix} f(T)f(U) \\ f(T)g(U) + g(T)f(U) + \delta g(T)g(U) \end{bmatrix}$;

(ii) $\beta(T * U) = \begin{bmatrix} \delta f(T)f(U) + f(T)g(U) + g(T)f(U) \\ g(T)g(U) \end{bmatrix}$;

(iii) $\langle \mathrm{num}(T)\rangle = \delta f(T) + g(T)$ *et* $\langle \mathrm{den}(T)\rangle = f(T) + \delta g(T)$.

Exemple 4.5. Un calcul direct basé sur l'expression de $\beta(1)$ donne

$$\beta(2) = \begin{bmatrix} t^2 \\ -t^{-4}+1 \end{bmatrix}, \quad \beta(3) = \begin{bmatrix} t^3 \\ t^{-7} - t^{-3} + t \end{bmatrix} \quad \text{et} \quad \beta(1/2) = \begin{bmatrix} 1-t^4 \\ t^{-2} \end{bmatrix}.$$

En utilisant les valeurs obtenues pour $T_{8,21} = (((1/2)+1)*2)+(-3)$, nous obtenons

$$\beta(T_{8,21}) = \begin{bmatrix} -2\,t^{-6} + 2\,t^{-2} - 2\,t^2 + t^6 \\ -2\,t^{-4} + 3\; - 4\,t^4 + 3\,t^8 - 2\,t^{12} + t^{16} \end{bmatrix}, \tag{4.2}$$

qui modulo 2 donne

$$\beta_2(T_{8,21}) = \begin{bmatrix} t^6 \\ 1 + \; t^8 \; + t^{16} \end{bmatrix}.$$

4.1 L'enchevêtrement T_{20}.

Étudions la paire crochet de l'enchevêtrement T_{20} introduit à la définition 3.6.

Lemme 4.6. *La paire crochet $\beta_2(T_{20})$ est égale à $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$. De plus, le terme dominant de $f(T_{20})$ est $2\,t^{28}$ et celui de $g(T_{20})$ est $2\,t^{26}$.*

Démonstration. Par la relation (4.2), nous obtenons

$$\beta(T_{10}) = \beta(T_{8,21} * 2) = \begin{bmatrix} 2\,t^{-10} - 2\,t^{-6} + 2\,t^{-2} - 2\,t^{6} + 2\,t^{10} - 2\,t^{14} + t^{18} \\ 2\,t^{-8} - 5\,t^{-4} + 7 - 7\,t^{4} + 5\,t^{8} - 3\,t^{12} + t^{16} \end{bmatrix}.$$

En remplaçant t par t^{-1}, nous obtenons

$$\beta(-T_{10}) = \begin{bmatrix} t^{-18} - 2\,t^{-14} + 2\,t^{-10} - 2\,t^{-6} + 2\,t^{2} - 2\,t^{6} + 2\,t^{10} \\ t^{-16} - 3\,t^{-12} + 5\,t^{-8} - 7\,t^{-4} + 7 - 5\,t^{4} + 2\,t^{8} \end{bmatrix}.$$

La formule du calcul de $\beta(T_{10}+(-T_{10}))$ donnée au i) de la proposition 4.4 implique que le terme dominant de $f(T_{20})$ est $t^{18} \cdot 2\,t^{10} = 2\,t^{28}$ et que celui de $g(T_{20})$ est

$$t^{18} \cdot 2\,t^{8} + t^{16} \cdot 2\,t^{10} - t^{2} \cdot t^{16} \cdot 2\,t^{8} = 2\,t^{26}.$$

En considérant les coefficients modulo 2, nous obtenons

$$\beta_2(T_{10}) = \begin{bmatrix} t^{18} \\ t^{-4} + 1 + t^{4} + t^{8} + t^{12} + t^{16} \end{bmatrix},$$
$$\beta_2(-T_{10}) = \begin{bmatrix} t^{-18} \\ t^{-16} + t^{-12} + t^{-8} + t^{-4} + 1 + t^{4} \end{bmatrix},$$

ce qui après calcul donne $\beta_2(T_{20}) = \beta_2(T_{10} + (-T_{10})) = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$. □

4.2 Cas général de l'enchevêtrement M_r.

Nous analysons maintenant la paire crochet (4.1) de l'enchevêtrement M_r construit à la définition 3.6. Pour des raisons pratiques nous utilisons la notation suivante.

Notation 4.7. Pour $r \geqslant 1$, nous notons ℓ_r le terme dominant de $f(M_r)$.

Proposition 4.8. *Pour tout $r \geqslant 1$, nous avons $\beta_{2^r}(M_r) = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $\ell_r = \left(2\,t^{28}\right)^{2^{r-1}}$ et le terme dominant de $g(M_r)$ est égale à $t^{-2}\ell_r$.*

Démonstration. Par induction sur $r \geqslant 1$. Le cas $r = 1$ est le lemme 4.6. Supposons maintenant $r \geqslant 2$. Par hypothèse d'induction, nous avons $f(M_{r-1}) \equiv 1 \mod 2^{r-1}$ et $g(M_{r-1}) \equiv 0 \mod 2^{r-1}$. Ainsi, il existe deux polynômes de Laurent P et Q dans $\mathbb{Z}[t, t^{-1}]$ tels que les relations $f(M_{r-1}) = 1 + 2^{r-1}P$ et $g(M_{r-1}) = 2^{r-1}Q$ soient satisfaites. Par la proposition 4.4 et la formule $\beta(M_r) = \beta(M_{r-1} + M_{r-1})$ nous obtenons :

$$\begin{aligned} \beta(M_r) &= \begin{bmatrix} f(M_{r-1})^2 \\ 2g(M_{r-1})\, f(M_{r-1}) + \delta g(M_{r-1})^2 \end{bmatrix}, \\ &= \begin{bmatrix} 1 + 2^r P + 2^{2r-2}P^2 \\ 2^r Q + 2^{2r-1}PQ + \delta 2^{2r-2}Q^2 \end{bmatrix}. \end{aligned}$$

Comme $2r - 2 \geqslant r$ est vérifiée car $r \geqslant 2$ l'est, nous trouvons $\beta_{2^r}(M_r) = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$. Montrons maintenant le résultat sur les termes dominants. Comme $f(M_r)$ vaut $f(M_{r-1})^2$, l'hypothèse d'induction implique que le terme dominant de $f(M_r)$ est le carré du terme dominant de $f(M_{r-1})$, c'est-à-dire, le carré de ℓ_{r-1}. Comme ℓ_{r-1}^2 est égal à ℓ_r, nous avons le résultat escompté pour le terme dominant de $f(M_r)$. En notant $\mathrm{lt}(P)$ le terme dominant d'un polynôme de Laurent $P \in \mathbb{Z}[t, t^{-1}]$, nous avons

$$\mathrm{lt}(g(M_r)) = \mathrm{lt}\left(2g(M_{r-1})f(M_{r-1}) + \delta\, g(M_{r-1})^2\right).$$

Par l'hypothèse d'induction, nous calculons

$$\begin{aligned} \mathrm{lt}(g(M_{r-1})\, f(M_{r-1})) &= t^{-2}\ell_{r-1} \cdot \ell_{r-1} = t^{-2}\ell_{r-1}^2 = t^{-2}\ell_r \\ \mathrm{lt}(\delta\, g(M_{r-1})^2) &= -t^2 \cdot (t^{-2}\ell_{r-1})^2 = -t^{-2}\ell_{r-1}^2 = -t^{-2}\ell_r \end{aligned}$$

et donc $\mathrm{lt}(g(M_r)) = 2\left(t^{-2}\ell_r\right) - \left(t^{-2}\ell_r\right) = t^{-2}\ell_r$, comme attendu. □

5 Sur le polynôme de Jones de K_r

Pour calculer le polynôme de Jones de K_r, nous commençons par introduire l'entortillement puis le polynôme crochet de Kauffman.

Définition 5.1. L'*entortillement* d'un diagramme d'entrelacs orienté D, noté $\mathrm{wr}(D)$, est la somme des signes des croisements de D en suivant les conventions **a** et **b** de la figure 4.4.

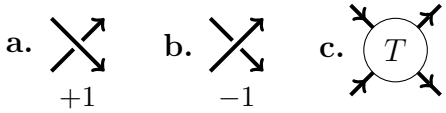


FIGURE 4.4 – **a.** Croisement avec entortillement positif. **b.** Croisement avec entortillement négatif. **c.** Enchevêtrement orienté de gauche à droite.

La notion d'entortillement peut naturellement être étendue aux enchevêtrements orientés.

Définition 5.2. Nous disons qu'un enchevêtrement T est *orienté de gauche à droite* s'il peut être muni d'une orientation comme au **c.** de la figure 4.4, dans ce cas on note $\mathrm{wr}(T)$ l'entortillement de T pour cette orientation.

Lemme 5.3. *Pour tout $r \geqslant 1$, l'enchevêtrement M_r est orientable de gauche à droite et nous avons* $\mathrm{wr}(M_r) = 0$

Démonstration. Remarquons d'abord que l'enchevêtrement T_{10} est orientable de gauche à droite. Comme $-T_{10}$ est obtenu de T_{10} en échangeant les signes des croisements, l'enchevêtrement $-T_{10}$ est aussi orientable de gauche à droite et nous avons $\mathrm{wr}(-T_{10}) = -\mathrm{wr}(T_{10})$. Comme la somme horizontale d'enchevêtrements est compatible avec l'orientation gauche-droite, pour tous enchevêtremenst orientables de gauche à droite U et V, nous avons $\mathrm{wr}(U+V) = \mathrm{wr}(U) + \mathrm{wr}(V)$. De $M_1 = T_{10} + (-T_{10})$, nous obtenons

$$\mathrm{wr}(M_1) = \mathrm{wr}(T_{10}) + \mathrm{wr}(-T_{10}) = \mathrm{wr}(T_{10}) - \mathrm{wr}(T_{10}) = 0.$$

La compatibilité de l'orientation gauche-droite avec la somme horizontale et une induction directe donnent $\mathrm{wr}(M_r) = \mathrm{wr}(M_{r-1}) + \mathrm{wr}(M_{r-1}) = 0 + 0 = 0$. □

Définition 5.4. Le *polynôme crochet de Kauffman normalisé* d'un entrelacs L dessiné par un diagramme orienté D est

$$\chi(L) = (-t^3)^{-\mathrm{wr}(D)} \langle D \rangle .$$

Le polynôme crochet de Kauffman a été introduit en 1987 par L. H. Kauffman dans [78]. Comme l'établit la proposition suivante, il est indépendant du choix du diagramme orienté D choisi pour représenter l'entrelacs L.

Proposition 5.5 (Théorème 2.6 de [78])**.** *Le polynôme crochet de Kauffman normalisé est un invariant d'entrelacs.*

À partir du polynôme crochet de Kauffman nous pouvons facilement introduire le polynôme de Jones d'un entrelacs quelconque.

Proposition 5.6 (Théorème 2.8 de [78])**.** *Le* polynôme de Jones *de l'entrelacs L est*

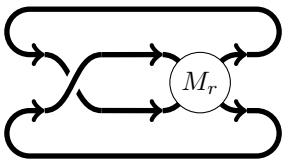
$$V(L) = \chi(L)|_{t \leftarrow t^{-1/4}}.$$

Exemple 5.7. Le polynôme crochet du nœud trivial $\bigcirc$ est $\langle \mathrm{den}(0) \rangle = 1$, qui donne $\chi(\bigcirc) = 1$ et donc $V(\bigcirc) = 1$.

Rappelons que K_r est le nœud représenté par le diagramme $\mathrm{num}(1 + M_r)$ et que ℓ_r est le terme dominant de $f(M_r)$.

Proposition 5.8. *Pour tout $r \geqslant 1$, le polynôme de Jones de K_r est congru à 1 modulo 2^r. De plus le terme dominant de $\chi(K_r)$ est ℓ_r.*

Démonstration. Soit $r \geqslant 1$ un entier. Notons D_r le diagramme $\mathrm{den}(1 * M_r)$. L'orientation gauche-droite de M_r induit l'orientation suivante sur D_r :



Comme l'entortillement de M_r est 0 par le lemme 5.3, l'entortillement de D_r pour l'orientation précédente est +1. Déterminons maintenant la paire crochet de Kauffman du diagramme D_r. Nous avons

$$\beta(1 + M_r) = \begin{bmatrix} t\, f(M_r) \\ t\, g(M_r) + t^{-1}\, f(M_r) + \delta\, t^{-1}\, g(M_r) \end{bmatrix}$$

et donc

$$\begin{aligned} \langle D_r \rangle &= \delta\, t\, f(M_r) + t\, g(M_r) + t^{-1}\, f(M_r) + \delta\, t^{-1}\, g(M_r) \\ &= (\delta\, t + t^{-1})\, f(M_r) + (t + \delta\, t^{-1})\, g(M_r) \\ &= -t^3\, f(M_r) - t^{-3}\, g(M_r). \end{aligned}$$

Ainsi le polynôme crochet de Kauffman normalisé de K_r est

$$\begin{aligned} \chi(K_r) &= (-t^3)^{-\,\mathrm{wr}(D_r)} \cdot \langle D_r \rangle = (-t^3)^{-1}\, (-t^3\, f(M_r) - t^{-3}\, g(M_r)) \\ &= f(M_r) + t^{-6} g(M_r). \end{aligned}$$

Comme $f(M_r)$ et $g(M_r)$ sont respectivement congrus à 1 et 0 modulo 2^r par la proposition 4.8, nous obtenons $\chi(K_r) \equiv 1$ modulo 2^r et donc $V(K_r)$ est trivial modulo 2^r. Le terme dominant de $g(M_r)$ étant $t^{-2}\ell_r$ par la proposition 4.8, celui de $\chi(K_r)$ est égal à ℓ_r. □

Nous pouvons maintenant établir le résultat principal de ce chapitre.

Théorème 5.9. *Pour tout $r \geqslant 1$, il existe une infinité de nœuds premiers distincts ayant un polynôme de Jones trivial modulo 2^r.*

Démonstration. Soit $r \geqslant 1$ un entier. Les nœuds K_i avec $i \geqslant r$ satisfont l'énoncé. En effet, par la proposition 5.8, pour tout $i \geqslant r$ le polynôme de Jones de K_i est trivial modulo 2^i et donc aussi modulo 2^r. Comme pour $j \geqslant 1$, le terme dominant de $\chi(K_j)$ est

$$\ell_j = \left(2\, t^{28}\right)^{2^{j-1}}$$

par la proposition 4.8, l'application $j \mapsto \chi(K_j)$ est injective. En particulier les nœuds K_i pour $i \geqslant r$ ont des polynômes de Jones distincts et sont donc deux à deux distincts. □

6 Et pour les autres modules ?

G. Pagel vient de commencer sa thèse de doctorat en octobre 2018 sour la direction de S. Eliahou et moi-même sur le thème du polynôme de Jones modulaire. Il a obtenu le résultat suivant :

Théorème 6.1 (G. Pagel [100])**.** *Soit m un entier. S'il existe un nœud non trivial ayant un polynôme de Jones trivial modulo m alors pour tout $r \in \mathbb{N}_+$ il existe un nœud non trivial ayant un polynôme de Jones trivial modulo m^r.*

Comme nous avons des exemples de nœuds non triviaux à polynôme de Jones trivial modulo 3, il existe alors des nœuds non triviaux à polynôme de Jones trivial modulo 3^r pour tout $r \in \mathbb{N}_+$.

G. Pagel a commencé à chercher des exemples de nœuds (comme clôture de tresses) à polynôme de Jones trivial modulo 5 et 6 à l'aide d'algorithmes développés en `Python` et utilisant l'algèbre de Temperley-Lieb. De tels nœuds n'ont pas encore été trouvés. C'est pourquoi nous sommes en train de développer une librairie `C++` basée sur l'algèbre de Temperley-Lieb et la structure de Garside des groupes des tresses pour, peut-être, *in-fine*, trouver de tels nœuds.

Un autre projet à moyen terme avec G. Pagel serait de faire une tabulation des nœuds premiers jusque 20 croisements ou plus en s'inspirant des travaux de J. Hoste, M. B. Thistlethwaite et J. Weeks [82] et en exploitant l'architecture des ordinateurs modernes (vectorialisation, parallélisation).

Combinatoire additive et théorie de Ramsey

V. Semigroupes numériques

Après une brève introduction aux semigroupes numériques à la section 1, nous construirons, à la section 2, l'arbre des semigroupes numériques $\mathcal{T}$ qui fût introduit par J. C. Rosales, P. A. Garcia-Sánchez, J. I. García-García et J. A. Jiménez Madrid en 2003 dans [116]. Cet arbre a permis à M. Bras-Amorós de formuler trois conjectures sur le comportement de la suite n_g du nombre de semigroupes numériques ayant un complémentaire de cardinal g dans $\mathbb{N}$. La section 3 est consacrée à l'étude d'algorithmes d'exploration efficaces de l'arbre des semigroupes numérique $\mathcal{T}$ que nous avons introduits avec F. Hivert en 2016 dans [69]. À la section 4 nous nous attarderons sur l'état de l'art autour des conjectures de M. Bras-Amorós. Finalement, à la section 5, nous introduirons la conjecture de Wilf et étudierons de rares contre-exemples de semigroupes numériques S vérifiant $W_0(S) < 0$. Le nombre W_0 a été introduit dans [47] pour résoudre la conjecture de Wilf pour les semigroupes génériques. Cette section a fait l'objet d'une publication en commun avec S. Eliahou [52].

Le lecteur souhaitant avoir une introduction complète aux semigroupes numériques pourra consulter le livre *The Diophantine Frobenius Problem* de J.L. Ramírez Alfonsín [110] ou le livre *Numerical Semigroups* de J.C. Rosales et P.A. García-Sánchez [114].

1 Introduction

Un *semigroupe numérique* est un sous-ensemble S de $\mathbb{N}$, contenant 0, stable par addition et de complémentaire fini dans $\mathbb{N}$.

Tout au long de ce chapitre nous utiliserons de nombreux paramètres rattachés aux semigroupes numériques. Nous définissons maintenant les principaux.

Définition 1.1. Soit S un semigroupe numérique.

- la *multiplicité* de S, notée $m(S)$, est le plus petit élément non nul de S ;
- le *genre* de S, noté $g(S)$, est le cardinal de $\mathbb{N} \setminus S$;
- le *nombre de Frobenius* de S, noté $F(S)$, est le plus grand élément de $\mathbb{Z} \setminus S$;
- le *conducteur* de S, noté $c(S)$, vaut $F(S) + 1$;
- la *profondeur* de S, notée $q(S)$, vaut $\left\lceil \frac{c(S)}{m(S)} \right\rceil$.

Dans la définition du Frobenius de S, nous devons utiliser $\mathbb{Z}$ et non $\mathbb{N}$ afin de pouvoir traiter le cas $S = \mathbb{N}$, qui est un semigroupe numérique de complémentaire vide dans $\mathbb{N}$. Le conducteur d'un semigroupe numérique S correspond au plus petit élément c de S tel que l'intervalle d'entiers $[c, +\infty[$ soit inclus dans S.

Exemple 1.2. L'ensemble $S_E = \{0, 3, 6, 7, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\}$ est un semigroupe numérique. Sa multiplicité $m(S_E)$ vaut 3. Son complémentaire dans $\mathbb{N}$ est l'ensemble $G_E = \{1, 2, 4, 5, 8, 11\}$, et donc son genre est $g(S_E) = 6$. De même on obtient les valeurs $F(S_E) = \max G_E = 11$ puis $c(S_E) = 12$.

Remarque 1.3. Afin de simplifier les notations et lorsque le contexte le permettra, nous utiliserons m, g, F, c et q à la place de $m(S), g(S), F(S), c(S)$ et $q(S)$ respectivement.

1.1 Ensemble générateur

Par nature les semigroupes numériques sont des objets infinis. Nous allons maintenant voir comment les décrire à l'aide d'ensembles finis.

Définition 1.4. Soient $a_1, \ldots, a_n$ des éléments de $\mathbb{N}_+$. On note $\langle a_1, \ldots, a_n \rangle$ l'ensemble des combinaisons linéaires à coefficients entiers positifs en les a_i :

$$\langle a_1, \ldots, a_n \rangle = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \,|\, \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}. \tag{5.1}$$

Par construction, le sous-ensemble $\langle a_1, \ldots, a_n \rangle$ de $\mathbb{N}$ contient 0 et est stable par addition. Cependant il n'est pas nécessairement de complément fini dans $\mathbb{N}$ comme l'illustre $\langle 2 \rangle$, qui est l'ensemble des entiers positifs pairs.

Proposition 1.5. *L'ensemble $\langle a_1, \ldots, a_n \rangle$ est un semigroupe numérique si et seulement si les entiers $a_1, \ldots, a_n$ sont premiers entre eux.*

Démonstration. De $\langle a_1, \ldots, a_n \rangle \subseteq \mathrm{pgcd}(a_1, \ldots, a_n)\mathbb{N}$, on obtient que la condition est nécessaire. Supposons maintenant que nous ayons $\mathrm{pgcd}(a_1, \ldots, a_n) = 1$. Il existe alors $\mu_1, \ldots, \mu_n$ dans $\mathbb{Z}$ vérifiant $1 = \mu_1 a_1 + \cdots + \mu_n a_n$. Posons

$$P = \sum_{i=1}^{n} \max(\mu_i, 0) a_i, \quad N = \sum_{i=1}^{n} \min(\mu_i, 0) a_i \quad \text{et} \quad Q = -N.$$

En particulier, les entiers P et Q sont des éléments de $\langle a_1, \ldots, a_n \rangle$ et vérifient $P - Q = 1$. Soit x un entier supérieur ou égal à $(a_1 - 1)Q$. Montrons que x est un élément de $\langle a_1, \ldots, a_n \rangle$. On pose $x = (a_1 - 1)Q + y$ puis $y = q\, a_1 + r$ avec $q \geqslant 0$ et $0 \leqslant r < a_1$. On obtient alors

$$x = (a_1 - 1)Q + q a_1 + r(P - Q) = q a_1 + (a_1 - 1 - r)Q + rP,$$

avec $a_1 - 1 - r \geqslant 0$ et donc x appartient à $\langle a_1, \ldots, a_n \rangle$. □

1.2 Éléments primitifs

Nous avons vu comment obtenir un semigroupe numérique à partir d'un ensemble fini générateur. Voyons maintenant comment obtenir un ensemble générateur à partir d'un semigroupe numérique donné. Un ensemble fini X d'un semigroupe numérique S est dit *générateur* si tout élément de S peut être écrit comme combinaison linéaire à coefficients entiers positifs d'éléments de X, c'est-à-dire, $S = \langle X \rangle$.

Définition 1.6. Soit S un semigroupe numérique. On dit qu'un élément x de S est *primitif* s'il ne peut pas être écrit comme la somme de deux éléments non nuls de S. On note $P(S)$ l'*ensemble des éléments primitifs* de S. Un élément non nul de S qui n'est pas primitif est dit *décomposable*. On note $D(S)$ l'*ensemble des éléments décomposables* de S. Lorsque le contexte le permettra on utilisera P et D à la place de $P(S)$ et $D(S)$.

En particulier, nous avons $S \setminus \{0\} = P \sqcup D$. Un élément primitif d'un semigroupe numérique S ne pouvant pas s'écrire comme combinaison linéaire à coefficients entiers d'autres éléments de S, tout ensemble générateur X de S doit nécessairement contenir l'ensemble $P(S)$.

Proposition 1.7. *L'ensemble des élément primitifs d'un semigroupe numérique S est un ensemble générateur de S.*

Démonstration. On montre par récurrence sur n qu'on a $S \cap [0, n] \subseteq \langle P \rangle$. Soit x un élément de S. Si x est primitif, on a immédiatement $x \in \langle P \rangle$. Sinon il existe y et z dans S non nuls tels que $x = y + z$. En particulier on a $y, z < x$ et donc y et z sont des éléments de $\langle P \rangle$. La stabilité par addition de $\langle P \rangle$ permet alors de conclure. □

Proposition 1.8. *L'ensemble des éléments primitifs d'un semigroupe numérique est inclus dans $[m, m + F]$ et contient au plus m éléments.*

Démonstration. Soit x un élément de S vérifiant $x \geqslant F + m + 1$. De $x - m \geqslant F + 1$ et $x = m + (x - m)$, nous obtenons $x \in D$. Ainsi P est inclus dans $[0, F + m]$. Comme m est le plus petit élément non nul de S, nous avons $P \subseteq [m, F + m]$. Soient x et y deux éléments distincts de P. Comme on ne peut pas passer de l'un à l'autre en ajoutant un multiple de m, les entiers x et y sont distincts modulo m et donc $\operatorname{card}(P) \leqslant m$. □

L'ensemble P est ainsi le plus petit ensemble générateur de S. Nous pouvons alors décrire un semigroupe numérique avec au plus m entiers.

Exemple 1.9. Les éléments primitifs du semigroupe numérique S_E définit à l'exemple 1.2 sont 3 et 7. Ainsi nous avons $S_E = \langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\}$.

Nous avons montré à la proposition 1.8 que les éléments primitifs d'un semigroupe numérique sont inclus dans l'intervalle $[m, m + F]$. Nous pouvons être plus précis.

Définition 1.10. L'ensemble des *éléments d'Apéry* d'un semigroupe numérique S est :

$$\operatorname{Ap}(S) = \{s \in S \mid s - m \notin S\}.$$

Deux éléments d'Apéry distincts de S ne pouvant pas être congrus modulo m, l'ensemble $\operatorname{Ap}(S)$ est de cardinalité m et peut être défini par

$$\operatorname{Ap}(S) = \{\min(S \cap (i + m\mathbb{N})) \mid 0 \leqslant i \leqslant m - 1\}.$$

Remarquons que 0 est toujours un élément d'Apéry.

Proposition 1.11. *Tous les éléments primitifs d'un semigroupe numérique S, à l'exception de m, sont des éléments d'Apéry de S.*

Démonstration. Soit x un élément primitif de S différent de m. Par définition des primitifs, la relation $x = (x - m) + m$ implique que $x - m$ n'appartient pas à S et donc x est un élément d'Apéry. □

1.3 Problème du nombre de Frobenius

Bien que relativement élémentaires, les semigroupes numériques sont au cœur de nombreux problèmes difficiles. Le plus connu est sans aucun doute celui du calcul du nombre de Frobenius d'un semigroupe numérique à partir d'un ensemble générateur.

Problème 1.12. Soit $A = \{a_1, \ldots, a_n\}$ un ensemble fini d'éléments de $\mathbb{N}$ premiers entre eux, déterminer $F(a_1, \ldots, a_n) := F(\langle a_1, \ldots, a_n \rangle)$.

Ce problème est aussi connu sous le nom de *problème de rendu de monnaie*, les entiers $a_1, \ldots, a_n$ correspondant alors à la valeur des pièces disponibles dans une certaine devise. Le nombre de Frobenius correspond dans ce cas à la plus grosse somme d'argent qui ne peut pas être atteinte dans cette devise.

Une première approche pour le cas $n = 2$ est attribuée à J.J. Sylvester pour un problème proposé dans *The education times* [121] consistant à montrer que $g(\langle a, b\rangle) = \frac{1}{2}(a-1)(b-1)$. Bien que le problème qu'il propose ne mentionne pas explicitement $F(a, b)$ on peut en déduire le résultat suivant :

Proposition 1.13. *Pour a et b des entiers premiers entre eux, on a $F(a, b) = ab - a - b$.*

Démonstration. Soit x un entier naturel. Si l'équation diophantienne $au + bv = x$ admet une solution particulière (u_0, v_0) alors la solution générale est de la forme $(u_0 - kb, v_0 + ka)$ avec k parcourant $\mathbb{Z}$. De $a(b-1) + b(-1) = ab - a - b$ on obtient que $au + bv = ab - a - b$ n'a pas de solution positive et donc $ab - a - b \notin \langle a, b\rangle$. Maintenant considérons la bijection ψ de l'intervalle $I = [0, ab - a - b]$ dans lui-même envoyant x sur $\psi(x) = ab - a - b - x$. Comme nous avons $\psi(x) + x = ab - a - b \notin \langle a, b\rangle$, l'application ψ envoie $I \cap S$ dans $I \cap (\mathbb{N} \setminus S)$. Ainsi on a

$$\operatorname{card}(I \cap S) \leqslant \operatorname{card}(I \cap (\mathbb{N} \setminus S)) \leqslant g(S) = \frac{1}{2}(a-1)(b-1).$$

Le cardinal de I étant $(a-1)(b-1) = 1 + ab - a - b$ on obtient

$$\operatorname{card}(I \cap S) = \operatorname{card}(I \cap (\mathbb{N} \setminus S)) = \frac{1}{2}(a-1)(b-1).$$

Finalement nous avons $\mathbb{N} \setminus S = I \cap (\mathbb{N} \setminus S)$ et donc $F(S) = \max(\mathbb{N} \setminus S) = \max(I \setminus S) = ab - a - b$. □

Pour le cas $n \geqslant 3$, il n'existe pas de formule polynomiale en $a_1, \ldots, a_n$ permettant de calculer $F(a_1, \ldots, a_n)$. C'est une conséquence du résultat suivant donné par F. Curtis en 1990.

Théorème 1.14 (F. Curtis [25])**.** *Il n'existe pas de famille finie de polynômes non nuls $\{P_1, \ldots, P_N\}$ telle que, pour n'importe quel triplet a, b, c d'entiers premiers entre eux, il existe $k \in \{1, \ldots, N\}$ vérifiant $P_k(a, b, c, F(a, b, c)) = 0$.*

Interprétant le problème de Frobenius comme le calcul du rayon de couverture d'un certain polytope, R. Kannan obtient en 1992 la complexité du problème de Frobenius lorsque le nombre de générateurs n est fixé.

Théorème 1.15 (R. Kannan [86])**.** *Pour tout n fixé, il existe un algorithme polynomial permettant de déterminer $F(a_1, \ldots, a_n)$.*

Dans le cas où le nombre de générateurs n'est pas fixé, J.L. Ramírez Alfonsín a utilisé en 1996 une réduction du problème du sac à dos à variables entières pour obtenir le résultat suivant.

Théorème 1.16 (J. L. Ramírez Alfonsín [109])**.** *Le problème de Frobenius est NP-dur.*

2 L'arbre des semigroupes numériques

L'arbre $\mathcal{T}$ des semigroupes numériques est considéré pour la première fois en 2003 par J. C. Rosales, P. A. Garcia-Sánchez, J.I. García-García et J.A. Jiménez Madrid dans [116]. Cet arbre permet, entre autre, d'énumérer les semigroupes numériques par genre croissant.

2.1 Construction

Soit S un semigroupe numérique de genre non nul. L'ensemble $S' = S \cup \{F(S)\}$ est alors un semigroupe numérique de genre $g(S) - 1$. En effet pour tout x non nul dans S, on a $y = x + F(S) > F(S)$ et donc y appartient à S'. Ainsi tout semigroupe numérique S de genre $g(S) > 0$ peut être obtenu à partir d'un semigroupe S' de genre $g(S') = g(S) - 1$ en retirant un élément de S'. Le semigroupe numérique S est un *fils* de S' dans l'arbre $\mathcal{T}$ des semigroupes numériques, nous disons aussi que S' est le *père* de S. La racine de $\mathcal{T}$ est donc l'unique semigroupe numérique de genre 0, à savoir $\mathbb{N}$.

Proposition 2.1. *Pour tout semigroupe numérique S et tout élément x de S, l'ensemble $S^x = S \setminus \{x\}$ est un semigroupe numérique si et seulement si x est un élément primitif de S.*

Démonstration. Si x n'appartient pas à $P(S)$, il existe des éléments non nuls y et z de S vérifiant $x = y + z$. Comme y et z sont alors encore dans S^x contrairement à x, l'ensemble S^x ne peut pas être un semigroupe numérique. Supposons maintenant que x soit un élément primitif de S. Comme 0 n'est pas primitif, on a $x \neq 0$ et donc 0 appartient à S^x. De $\mathbb{N} \setminus S^x = (\mathbb{N} \setminus S) \cup \{x\}$ nous obtenons que S^x est de complémentaire fini dans $\mathbb{N}$. Soient y, z des éléments de $S^x \subseteq S$. Dans S la somme $y+z$ est nécessairement différente de x car x est un élément primitif de S, ce qui implique $y + z \in S^x$. □

Exemple 2.2. Reconsidérons le semigroupe numérique $S_E = \langle 3, 7\rangle$ de l'exemple 1.9. Ses éléments primitifs sont 3 et 7. On obtient ainsi :

$$S_E^3 = \{0, 6, 7, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\} = \langle 6, 7, 9, 10\rangle\,,$$
$$S_E^7 = \{0, 3, 6, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\} = \langle 3, 10, 14\rangle\,.$$

Le Frobenius de S_E^7 étant 11, on a que

$$S' = S_E^7 \cup \{11\} = \{0, 3, 6\} \cup \{x \in \mathbb{N}, x \geqslant 10\} = \langle 3, 10, 11\rangle$$

est le père de S_E^7 dans $\mathcal{T}$. Le semigroupe S_E^7 est donc le fils de S' et non celui de S_E.

Comme l'illustre l'exemple 2.2, les semigroupes numériques S^x, avec x élément primitif de S, ne sont pas nécessairement des fils de S. En effet si S' est le père de S alors nous avons $S' = S \cup \{F(S)\}$ et donc $F(S') < F(S)$. Le Frobenius du semigroupe numérique S^x valant $\max(x, F(S))$ par construction, nous obtenons que S^x est un fils de S dans $\mathcal{T}$ si et seulement si $x \geqslant F(S) + 1 = c(S)$.

Corollaire 2.3. *Pour tout semigroupe numérique S et tout élément x de S, l'ensemble S^x est un fils de S dans l'arbre des semigroupes numériques $\mathcal{T}$ si et seulement si x est primitif et vérifie $x \geqslant c(S)$.*

Remarquons que grâce à la proposition 1.8 la condition $x \geqslant c(S)$ du corollaire précédent peut être remplacée par $x \in [c(S), c(S) + m(S) - 1]$.

Nous construisons l'arbre des semigroupes numériques $\mathcal{T}$ de la manière suivante. La racine de l'arbre est l'unique semigroupe de genre 0, à savoir, $\langle 1\rangle$ qui est $\mathbb{N}$ tout entier. Si S est un semigroupe de l'arbre, ses fils sont les semigroupes numériques S^x avec x parcourant l'ensemble $P(S) \cap [c(S), c(S) + m(S) - 1]$. Par convention, lorsque nous dessinerons $\mathcal{T}$, le semigroupe numérique S^x sera à gauche de S^y si x est plus petit que y.

Si S est un nœud de $\mathcal{T}$ alors les fils de S sont de genre $g(S) + 1$. L'ensemble des semigroupes numériques de profondeur g dans l'arbre $\mathcal{T}$ correspond alors exactement à l'ensemble des semigroupes numériques de genre g.

Notation 2.4. On désigne par $\mathcal{T}_g$ la restriction de $\mathcal{T}$ aux semigroupes numériques de genre inférieur ou égal à g.

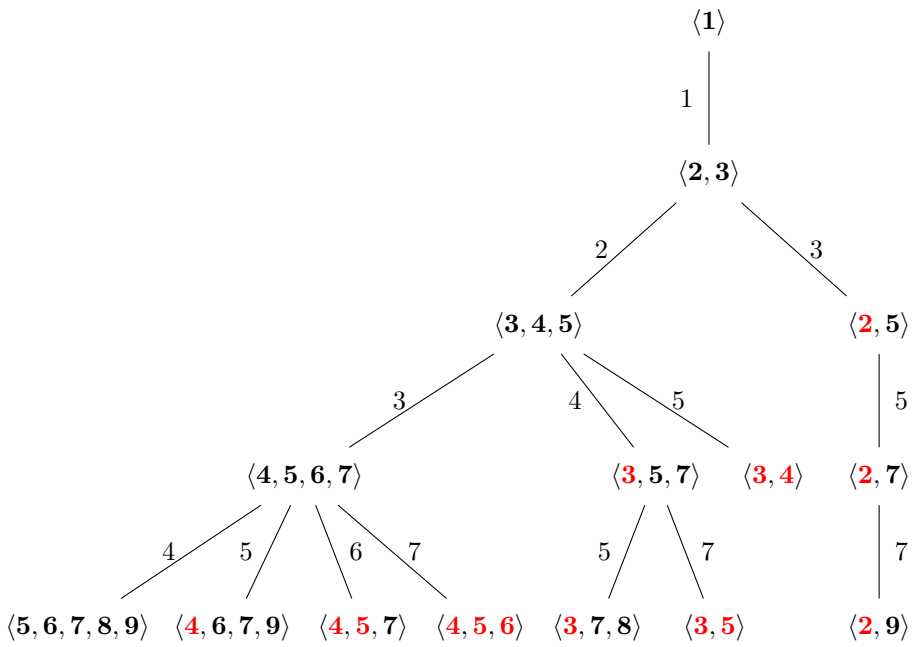


FIGURE 5.1 – Les quatre premiers niveaux de l'arbre $\mathcal{T}$ des semigroupes numériques, correspondant à $\mathcal{T}_4$. Un générateur d'un semigroupe numérique S est en rouge s'il est inférieur au conducteur $c(S)$. Une arête entre un semigroupe numérique S et son fils S' est étiquetée x si S' est obtenu de S en retirant x, c'est-à-dire, si on a $S' = S^x$.

2.2 Nombre de semigroupes numériques de genre donné

Le principal intérêt de l'arbre des semigroupes numériques $\mathcal{T}_g$ est de pouvoir engendrer tous les semigroupes numériques de genre $\leqslant g$.

Notation 2.5. Pour tout $g \in \mathbb{N}$, on note N_g l'ensemble des semigroupes numériques de genre g et par n_g son cardinal.

Sur sa page personnelle [96], N. Medeiros liste tous les semigroupes numériques de genre $g \leqslant 12$. En 2007, M. Bras-Amorós [13] détermine l'arbre $\mathcal{T}_{50}$ à l'aide d'une exploration en largeur. Le calcul de l'ensemble N_{50} de tous les semigroupes numériques de genre 50 à partir de celui des semigroupes numériques de genre 49 a demandé 19 jours de calcul sur un ordinateur équipé d'un `Pentium D` cadencé à `3Ghz` et disposant d'`1Go` de mémoire vive. Le fichier compressé décrivant N_{50} a une taille de `3.6Go`. Cette exploration lui a permis de déterminer les valeurs de n_g pour $g \leqslant 50$ et de formuler trois conjectures :

Conjecture 2.6 (M. Bras-Amorós [13])**.** *Pour tout $g \in \mathbb{N}$, nous avons*

$$n_{g+2} \geqslant n_{g+1} + n_g.$$

Conjecture 2.7 (M. Bras-Amorós [13])**.** *Nous avons*

$$\lim_{g \to +\infty} \frac{n_{g+1} + n_g}{n_{g+2}} = 1.$$

Conjecture 2.8 (M. Bras-Amorós [13]). *Nous avons*

$$\lim_{g\to+\infty} \frac{n_{g+1}}{n_g} = \phi = \frac{1+\sqrt{5}}{2}.$$

Par la suite M. Bras-Amorós a obtenu n_{51} puis n_{52}. Sur sa page personnelle [40], M. Delgado annonce la valeur de n_{55}. Une version faible de la conjecture 2.6 a été énoncée par N. Kaplan en 2011.

Conjecture 2.9 (N. Kaplan [87]). *Pour tout $g \in \mathbb{N}$, on a $n_{g+1} \geqslant n_g$.*

3 Exploration de l'arbre des semigroupes numériques

Cette section est consacrée aux résultats que nous avons obtenus avec F. Hivert dans [69]. Nous présentons de nouvelles idées afin d'explorer efficacement l'arbre des semigroupes numériques $\mathcal{T}$. Nous avons tout d'abord commencé par introduire une nouvelle façon de représenter les semigroupes numériques afin d'exploiter efficacement les capacités vectorielles des processeurs actuels. Finalement grâce à cette approche, la parallélisation de notre exploration et l'optimisation du code, nous avons obtenu un algorithme très efficace pour parcourir l'arbre $\mathcal{T}$ des semigroupes numériques.

3.1 Nombre de S-décompositions

Afin de décrire notre nouvelle représentation des semigroupes numériques nous commençons par introduire le nombre de S-décompositions.

Définition 3.1. Pour tout semigroupe numérique S et tout $x \in \mathbb{N}$, on définit :

$$D_S(x) = \{y \in S \,|\, x - y \in S \text{ et } 2y \leqslant x\},$$

et $d_S(x) = \operatorname{card}(D_S(x))$. L'entier $d_S(x)$ est le *nombre de S-décompositions de x*. L'application $d_S : \mathbb{N} \to \mathbb{N}$ est la *fonction de décomposition* de S.

Supposons que y soit un élément de $D_S(x)$. Par définition, l'entier $z = x - y$ appartient aussi à S. Ainsi x peut être décomposé en $x = y + z$ avec y et z dans S. De plus la condition $2y \leqslant x$ implique $y \leqslant z$. En d'autres mots si nous définissons $D'_S(x)$ comme étant l'ensemble de tous les couples $(y, z) \in S \times S$ vérifiant $x = y + z$ et $y \leqslant z$ alors l'ensemble $D_S(x)$ est l'image de $D'_S(x)$ par la projection sur la première coordonnée. Ainsi $D_S(x)$ décrit comment l'entier x peut être décomposé en la somme de deux éléments de S.

Exemple 3.2. Reprenons le semigroupe numérique

$$S_E = \langle 3, 7\rangle = \{0, 3, 6, 7, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\}$$

de l'exemple 1.9. L'entier 14 admet deux décompositions comme somme de deux éléments de S_E, à savoir : $14 = 0 + 14$ et $14 = 7 + 7$. Ainsi $D_{S_E}(14)$ est l'ensemble $\{0, 7\}$ et le nombre de S_E-décompositions de 14 est $d_{S_E}(14) = 2$.

Lemme 3.3. *Pour tout semigroupe numérique S et tout $x \in \mathbb{N}$, nous avons*

$$d_S(x) \leqslant 1 + \left\lfloor \frac{x}{2} \right\rfloor,$$

et l'égalité est obtenue pour $S = \mathbb{N}$.

Démonstration. L'ensemble $D_S(x)$ est inclus dans $\{0, \ldots, \lfloor \frac{x}{2} \rfloor\}$ avec égalité pour $S = \mathbb{N}$. □

Proposition 3.4. *Pour tout semigroupe numérique S et tout entier $x \in \mathbb{N}_+$ nous avons :*

(i) x appartient à S si et seulement si $d_S(x) > 0$;

(ii) x est un élément primitif de S si et seulement si $d_S(x) = 1$.

Démonstration. Un entier x appartient à S si et seulement si $x = 0 + x$ est une S-décomposition de x, si et seulement si $0 \in D_S(x)$. Si de plus x est primitif alors c'est la seule S-décomposition de x et nous avons alors $D_S(x) = \{0\}$. □

Dans la proposition précédente nous avons dû supprimer le cas $x = 0$ car on a $0 = 0+0$ et donc $d_S(0) = 1$ alors que 0 n'est pas un élément primitif de S.

Le résultat suivant montre comment obtenir la fonction de décomposition d'un semigroupe numérique à partir de celle de son père.

Proposition 3.5. *Soit S un semigroupe numérique et x un élément primitif de S. Pour tout $y \in \mathbb{N} \setminus \{0\}$ nous avons :*

$$d_{S^x}(y) = \begin{cases} d_S(y) - 1 & \text{si } y \geqslant x \text{ et } d_S(y-x) > 0, \\ d_S(y) & \text{sinon.} \end{cases}$$

Démonstration. Dans S^x la décomposition $y = x + (y - x)$ est impossible. Or c'est une S-décomposition de y si et seulement si $y - x$ appartient à S et donc si et seulement si $y \geqslant x$ et $d_S(y - x) > 0$. □

3.2 Une nouvelle représentation

Pour le reste de cette section nous fixons un entier G de $\mathbb{N}_+$. Nous décrivons maintenant notre façon de représenter les semigroupes numériques, qui est adaptée à l'exploration de l'arbre $\mathcal{T}_G$ et permet d'exploiter les capacités de calcul vectoriel des processeurs modernes.

Lemme 3.6. *Tout semigroupe numérique S vérifie*

(i) $x \in P$ implique $x \leqslant c + m - 1$;

(ii) $m \leqslant g + 1$;

(iii) $c \leqslant 2g$.

Démonstration. Le (i) est une conséquence de la Proposition 1.8. Le (ii) est une conséquence de l'inclusion de l'intervalle $[1, m-1]$ dans $\mathbb{N} \setminus S$. Pour le (iii), on considère la bijection ψ de l'intervalle $I = [0, F]$ dans lui même envoyant x sur $F - x$. Comme la somme de x et $\psi(x)$ vaut F, l'entier $\psi(x)$ appartient nécessairement à $I \cap (\mathbb{N} \setminus S)$ dès que x est un élément de $I \cap S$. Nous obtenons ainsi

$$\operatorname{card}(I \cap S) \leqslant \operatorname{card}(I \cap (\mathbb{N} \setminus S)) \leqslant g.$$

Finalement, la relation

$$\operatorname{card}(I) = \operatorname{card}(I \cap S) + \operatorname{card}(I \cap (\mathbb{N} \setminus S)) \leqslant 2g,$$

implique $c = F + 1 = \operatorname{card}(I) \leqslant 2g$. □

Proposition 3.7. *Tout semigroupe numérique S de genre $g \leqslant G$ est entièrement déterminé par le vecteur*

$$\delta_S = (d_S(0), \ldots, d_S(3\,G)) \in \mathbb{N}^{3G+1}.$$

En particulier, nous pouvons retrouver c, g, m et P à partir de δ_S.

Démonstration. Le lemme 3.6 garantit que les entiers c, m ainsi que les éléments primitifs de S sont inférieurs à $3g \leqslant 3G$. Par la proposition 3.4 l'entier x est un élément de S si et seulement si $d_S(x)$ est non nul. Le nombre de Frobenius F de S est donc le plus grand entier x tel que $d_S(x) = 0$, d'où :

$$c = 1 + F = 1 + \max\{x \in \{0, \dots, 2G\},\ d_S(x) = 0\}.$$

L'entier g correspond au nombre d'entiers x inférieurs à c vérifiant $d_S(x) = 0$:

$$g = \operatorname{card}(\{x \in \{0, \dots, 2G\},\ d_S(x) = 0\}).$$

L'entier m est le plus petit entier $x > 0$ vérifiant $d_S(x) \neq 0$:

$$m = \min\{x \in \{1, \dots, G+1\},\ d_S(x) \neq 0\}.$$

Toujours par la proposition 3.4, on obtient

$$P = \{x \in \{1, \dots, 3G\},\ d_S(x) = 1\}.$$ □

La représentation du semigroupe numérique S par le vecteur δ_S est similaire mais légèrement différente de celle utilisée dans [12].

3.3 Algorithmes

Dans [13], M. Bras-Amorós explore l'arbre $\mathcal{T}_G$ à l'aide d'un parcours en largeur. C'est aussi l'approche qu'utilisent M. Delgado, P.A. Garciá-Sánchez et J. Morais dans leur paquet `NumericalSgps` [43] pour `Gap` [71]. Le principal inconvénient de cette approche est sa consommation mémoire. Pour explorer l'ensemble N_g des semigroupes numériques de genre g elle nécessite d'avoir accès à l'ensemble N_{g-1} des semigroupes numériques de genre $g-1$. Ainsi pour déterminer n_{50}, il faut avoir accès aux $n_{49} = 62\ 200\ 036\ 752$ semigroupes de genre 49. Afin de limiter la consommation mémoire, nous utilisons un parcours en profondeur de l'arbre $\mathcal{T}_G$:

Algorithme 1 Exploration en profondeur et récursive de l'arbre $\mathcal{T}_G$.

```
1: procedure ExploreRec(S, G)
2:     si g(S) < G alors
3:         pour x de c(S) à c(S) + m(S) faire
4:             si x ∈ P(S) alors
5:                 ExploreRec(S^x, G)
6:             fin si
7:         fin pour
8:     fin si
9: fin procedure
```

Nous pouvons aussi écrire une version itérative à l'aide d'une pile (voir algorithme 2).

Dans les algorithmes 1 et 2 nous n'avons pas spécifié comment étaient représentés les semigroupes numériques. Pour cela nous allons utiliser le vecteur δ_S introduit à la proposition 3.7. En pratique, déterminer c, g et m à partir de δ_S a un coût non-négligeable. Nous représentons donc les semigroupes numériques S de genre $g \leqslant G$ par (c, g, m, δ_S). Dans un contexte algorithmique, si la variable `S` désigne un semigroupe numérique, nous utiliserons :

– `S.c`, `S.g` et `S.m` pour les entiers $c(S)$, $g(S)$ et $m(S)$;
– `S.d[i]` pour l'entier $d_S(i)$.

Algorithme 2 Exploration en profondeur et itérative de l'arbre $\mathcal{T}_G$.

```
1: procedure EXPLORE(G)
2:     Pile pile                                              ▷ la pile vide
3:     pile.empile(ℕ)
4:     tant que pile est non vide faire
5:         S ← pile.dessus()
6:         pile.dépile()
7:         si g(S) < G alors
8:             pour x de c(S) à c(S) + m(S) faire
9:                 si x ∈ P(S) alors
10:                    pile.empile(S^x)
11:                fin si
12:            fin pour
13:        fin si
14:    fin tant que
15: fin procedure
```

Il est important de noter que le vecteur δ_S et donc la représentation de S dépend du genre cible G. L'algorithme suivant initialise la racine $\mathbb{N}$ de l'arbre $\mathcal{T}_G$ des semigroupes numériques de genre au plus G.

Algorithme 3 Renvoie la racine de l'arbre $\mathcal{T}_G$

```
1: fonction RACINE(G)
2:     R.c ← 0                                  ▷ R désigne le semigroupe numérique ℕ
3:     R.g ← 0
4:     R.m ← 1
5:     pour x de 0 à 3G faire
6:         R.d[x] ← 1 + ⌊x/2⌋
7:     fin pour
8:     renvoie R
9: fin fonction
```

L'algorithme 4 renvoie la représentation du semigroupe numérique S^x à partir de celle de son père S lorsque x est un élément primitif de S plus grand que $c(S)$.

Algorithme 4 Renvoie le fils S^x de S où $x \in P(S) \cap [c(S), c(S) + m(S)[$.

```
1: fonction FILS(S,x,G)
2:     S^x.c ← x + 1
3:     S^x.g ← S.g + 1
4:     si x > S.m alors
5:         S^x.m ← S.m
6:     sinon
7:         S^x.m ← S.m + 1
8:     fin si
9:     S^x.d ← S.d                              ▷ copie les nombres de S-décompositions
10:    pour y de x à 3G faire
11:        si S.d[y − x] > 0 alors
12:            S^x.d[y] ← S.d[y] − 1            ▷ retire 1 au nombre de S-décompositions
13:        fin si
14:    fin pour
15:    renvoie S^x
16: fin fonction
```

Proposition 3.8. *Appliqué à (S, x, G) avec $g \leqslant G$, $x \in P$ et $x \geqslant c$, l'algorithme 4 renvoie le semigroupe S^x en temps $O(\log(G) \times G)$.*

Démonstration. Vérifions d'abord la correction de l'algorithme. Par construction on a $S^x = S \setminus \{x\}$. Ainsi le genre de S^x est $g(S) + 1$ (ligne `3`). L'entier x étant supérieur à c, l'intervalle $I = [x + 1, +\infty[$ est inclus dans S puis dans S^x. Comme x n'appartient pas à S^x, le conducteur de S^x est $x + 1$ (ligne `2`). Concernant la multiplicité de S^x nous avons deux cas. Si $x > m(S)$ est vérifiée alors $m(S)$ appartient aussi S^x et donc $m(S^x)$ vaut $m(S)$. Supposons $x = m(S)$. La relation $x(S) \geqslant c(S)$ et la caractérisation de $m(S)$ impliquent $x = m(S) = c(S)$. Ainsi S^x contient $m(S)+1$ et donc $m(S^x) = m(S)+1$. L'affectation de $m(S^x)$ est faite entre les lignes `4` à `8`. La correction du calcul de δ_{S^x} effectué entre les lignes `9` et `15` est une conséquence directe de la proposition 3.5.

Déterminons maintenant la complexité de l'algorithme. Comme par le lemme 3.6 nous avons la relation$x \leqslant 3G$ ainsi que $m(S) \leqslant G + 1$, les lignes `2` à `8` sont chacune exécutées en temps $O(\log(G))$. La boucle **pour** nécessite $O(G)$ étapes et chaque étape est exécutée en temps $O(\log(G))$. Nous obtenons ainsi que l'algorithme est exécuté en temps $O(\log(G) \times G)$. □

En modifiant les algorithmes 1 et 2 pour y remplacer `S^x` par Fils(`S`,`x`,`G`) ligne `10` et `12` respectivement nous pouvons maintenant explorer en profondeur (récursivement ou itérativement), l'arbre des semigroupes numériques. Déterminons maintenant la complexité en temps et en espace de l'algorithme 2 ainsi obtenu.

Lemme 3.9. *Stocker la représentation (c, g, m, δ_S) d'un semigroupe numérique S de genre $g \leqslant G$ requiert un espace mémoire en $O(G \times \log(G))$.*

Démonstration. Les points *ii*) et *iii*) du lemme 3.6 impliquent $c \leqslant 2g(S) \leqslant 2G$ et $m \leqslant g(S)+1 \leqslant G+1$. Les entiers c, g et m nécessitent donc un espace mémoire en $O(\log(G))$ pour être stockés. Chaque entrée de δ_S étant le nombre de S-décompositions d'un entier inférieur à $3G$, c'est un entier inférieur à $1+\frac{3}{2}G$ par le lemme 3.3. Le vecteur δ_S, qui est de taille $3G+1$, requiert donc un espace mémoire en $O(G \times \log(G))$. Il en est donc de même pour (c, g, m, δ_S). □

Proposition 3.10. *Appliqué à $G \in \mathbb{N}$ l'algorithme 2 explore l'arbre $\mathcal{T}_G$ en temps*

$$O\left(\log(G) \times G \times \sum_{g=0}^{G} n_g\right)$$

avec une consommation mémoire en $O(\log(G) \times G^3)$.

Démonstration. La correction de l'algorithme est une conséquence de la proposition 3.8 et de la construction de l'arbre $\mathcal{T}$ des semigroupes numériques. Pour la complexité en temps, on constate que l'algorithme Fils est appelé pour tous les semigroupes de l'arbre $\mathcal{T}_G$. Comme il y a exactement $N = \sum_{g=0}^{G} n_g$ semigroupes de genre $g \leqslant G$, la complexité en temps de l'algorithme 4 établi à la proposition 3.8 garantit que la complexité en temps de l'algorithme 2 est en $O(\log(G) \times G \times N)$.

Montrons maintenant le résultat sur la consommation mémoire. Pour cela nous avons besoin de décrire le comportement de la pile tout au long de l'exécution de l'algorithme. Comme elle est remplie à l'aide d'un parcours en profondeur, elle possède deux propriétés. La première est que le genre des semigroupes contenus dans la pile est croissant lorsque nous parcourons la pile du bas vers le haut. La seconde propriété, est que pour tout genre $g \in [0, G]$, tous les semigroupes de genre g stockés dans la pile possèdent le même père. Comme le nombre de fils d'un semigroupe numérique S est le nombre d'éléments primitifs de S dans l'intervalle $[c(S), c(S) + m(S) - 1]$, le semigroupe S a au plus $m(S)$ fils. Par le lemme 3.6 *ii*) on obtient ainsi qu'un semigroupe numérique de genre g a au plus $g+1$ fils. Ainsi la pile contient au plus g semigroupes de genre g pour tout $1 \leqslant g \leqslant G$. La taille de la pile est donc majorée par

$$M = \sum_{g=0}^{G} g = \frac{G(G+1)}{2}.$$

Finalement à l'aide du lemme 3.9 nous obtenons que la consommation mémoire de l'algorithme Explore est en

$$O(\log(G) \times G \times M) = O(\log(G) \times G^3).$$ □

3.4 Vectorialisation

Supposons que nous souhaitions explorer l'arbre $\mathcal{T}_G$ des semigroupes numériques de genre au plus G. Il est alors nécessaire de considérer les nombres de décompositions d'entiers jusque $3G$. Grâce au lemme 3.3, nous savons que ces nombres sont inférieurs à $\left\lfloor \frac{3G}{2} \right\rfloor + 1$. En particulier pour $G \leqslant 169$, chaque entrée de δ_S est majorée par 254 et peut donc être codée sur un octet, qui permet de stocker des entiers entre 0 et 255. À partir de maintenant nous nous plaçons dans ce cas.

À chaque pas de la boucle **pour** de l'algorithme 4, le processeur travaille sur un seul octet. En exploitant les capacités de calcul vectoriel des processeurs il y a donc certainement possibilité de travailler directement avec 8, 16 ou 32 nombres de décompositions en fonction de la technologie (`MMX`, `SSE`, `AVX`) utilisée. C'est dans ce but que nous avons choisi de représenter les semigroupes numériques à l'aide du vecteur δ_S.

Nous présentons maintenant une version `MMX` de notre algorithme. Bien que la technologie `MMX` soit à priori moins performante que le `SSE` ou l'`AVX`, sa mise en place est techniquement plus simple.

Pour aller plus loin, nous devons préciser que le tableau `S.d` contenant les nombres de `S`-décompositions des entiers de 0 à $3G$ est stocké en mémoire sur des octets consécutifs. Dans la boucle **pour** de l'algorithme 4 nous pouvons imaginer deux curseurs : le premier, noté `src`, pointe en mémoire sur l'octet `S.d[0]` et le second, noté `dst`, pointe en mémoire sur l'octet `T.d[]`. En utilisant ces deux curseurs, les lignes `10` à `14` de l'algorithme 4 peuvent être réécrites de la façon suivante :

```
src ← addresse(S.d[0])
dst ← addresse(T.d[x])
i ← 0
tant que i ⩽ 3G − x faire
    si contenu(src) > 0 alors
        décrémente contenu(dst) de 1
    fin si
    incrémente src,dst,i de 1
fin tant que
```

Dans cette version nous constatons que les curseurs `src` et `dst` se déplacent en même temps et que la modification de la valeur pointée par `dst` nécessite seulement un accès à celles pointées par `src` et `dst`. Nous pouvons donc travailler sur plusieurs entrées de `S.d` sans craindre de collisions. Voyons maintenant comment exploiter la technologie `MMX` permettant au processeur de travailler nativement avec des vecteurs de 8 octets. Nous utiliserons trois instructions `MMX` : `_m_pcmpeqb`, `_m_pandn` et `_m_psubb`. Ces commandes prennent en paramètres deux vecteurs de 8 octets (de type `__m64`) et en renvoie un troisième. Voici le fonctionnement de ces instructions :

— `_m_pcmpeqb(a,b)` teste l'égalité terme à terme entre les vecteurs `a` et `b` :

$$\texttt{\_m\_pcmpeqb(a,b)[i]} = \begin{cases} 255 & \text{si } \texttt{a[i]} = \texttt{b[i]} \\ 0 & \text{sinon.} \end{cases}$$

— `_m_psubb(a,b)` effectue une soustraction terme à terme :

$$\texttt{\_m\_psubb(a,b)[i]} = (\texttt{a[i]} - \texttt{b[i]}).$$

— `_m_pandn(a,b)` effectue l'opération logique `et non` terme à terme :

$$\texttt{\_m\_pandn(a,b)[i]} = (\texttt{a[i]}\ \texttt{and}\ (\texttt{not}\ \texttt{b[i]})).$$

Nous obtenons alors une version MMX de l'algorithme FILS :

```
1: src ← adresse(S.d[0])
2: dst ← adresse(T.d[x])
3: i ← 0
4: tant que i ⩽ 3G − x faire
5:     t ← [0,0,0,0,0,0,0,0]
6:     t ← _m_pcmpeqb(src,t)
7:     t ← _m_pandn([1,1,1,1,1,1,1,1],t)
8:     dst ← _m_psubb(dst,t)
9:     incrémente src,dst,i de 8
10: fin tant que
```

Regardons en détail le fonctionnement de cette nouvelle version. Soit `i` un entier compris entre 0 et 7. La ligne `5` affecte la valeur de `0` à `t[i]`. Après la ligne `6`, nous avons

$$\texttt{t[i]} = \begin{cases} \texttt{255} & \text{si } \texttt{src[i]} = \texttt{0} \\ \texttt{0} & \text{sinon} \end{cases}$$

La ligne `7` effectue un `et` logique entre `1` et `non t[i]`. Les écritures binaires respectives de `0`, `1` et `255` étant $\texttt{[00000000]}_2$, $\texttt{[00000001]}_2$ et $\texttt{[11111111]}_2$ nous obtenons

$$\texttt{t[i]} = \begin{cases} \texttt{0} & \text{si } \texttt{src[i]} = \texttt{0} \\ \texttt{1} & \text{sinon} \end{cases}$$

La ligne `8` effectue la soustraction de `dst[i]` par `t[i]` ainsi `dst[i]` est inchangé pour `src[i]=0` et est diminué d'une unité dans le cas contraire. Finalement les curseurs `src` et `dst` sont décalés de 8 octets pour pointer sur le bloc d'entiers à traiter.

Dans [69], nous avons utilisé les instructions `SSE` qui donnent de meilleurs performances que celles du jeu `MMX` mais l'utilisation de cette technologie nécessite des contraintes techniques fortes, c'est pourquoi nous la détaillons pas dans ce mémoire. L'utilisation de la nouvelle technologie `AVX` permetterait sans aucun doute d'améliorer encore les performances de notre algorithme.

3.5 Parallélisation

En plus de la vectorialisation nous pouvons utiliser la parallélisation afin d'augmenter l'efficacité de notre algorithme. En effet, aujourd'hui les processeurs sont équipés de plusieurs cœurs (2, 4 ou plus). La version actuelle de notre algorithme d'exploration de l'arbre $\mathcal{T}_G$ utilise un seul cœur et donc seulement une fraction de la puissance d'un processeur. L'idée est de faire explorer différentes branches de l'arbre $\mathcal{T}_G$ en parallèle par différents cœurs. Le point clé est de s'assurer que chacun soit occupé en lui donnant une nouvelle branche à explorer dès qu'il en a fini avec une précédente.

L'arbre des semigroupes numériques étant fortement déséquilibré il est difficile de prévoir avant son exploration comment effectuer une distribution équilibrée des branches à explorer. Une solution consiste donc à utiliser des algorithmes de parallélisation basés sur le vol de tâches comme proposé par la librairie `Cilk` [120]. L'algorithme 1 devient alors :

Algorithme 5 Exploration parallèle et récursive de l'arbre $\mathcal{T}_G$.

```
1: procedure ExploreParalleleRecursive(S, G)
2:     si g(S) < G alors
3:         pour x de c(S) à c(S) + m(S) faire
4:             si x ∈ P(S) alors
5:                 cilk_spawn ExploreRec(S^x, G)
6:             fin si
7:         fin pour
8:     fin si
9: fin procedure
```

La seule différence avec la version précédente est l'ajout de l'instruction **cilk_spawn** au début de la ligne 5, signalant à `Cilk` que les sous-arbres de $\mathcal{T}_G$ enracinés en différents fils peuvent être exécutés en parallèle.

Les choses sont en fait un peu plus compliquées. Par exemple si nous souhaitons compter les semigroupes numériques visités durant l'exploration de $\mathcal{T}_G$ alors nous devons fusionner les résultats obtenus durant l'exploration des différents sous-arbres et nous sommes alors en situation de concurrence. En effet la mise à jour d'une variable `v` en parallèle par deux processus différents peut mettre la variable `v` dans un état non-déterministe en fonction de l'ordre d'exécution des diverses primitives atomiques constituant la mise à jour de la variable [131]. Un autre problème est que le coût d'appel récursif d'une fonction à l'aide de **cilk_spawn** est non-négligeable. Une solution consiste à passer de la version récursive utilisant `Cilk` à une exploration itérative à l'aide de pile lorsque le genre du semigroupe considéré est *proche* du genre cible G (par exemple $G - 10$) :

Algorithme 6 Exploration parallèle mixte de l'arbre $\mathcal{T}_G$.

```
1: procedure ExploreParalleleMixte(S, G)
2:     si g(S) < G − 10 alors
3:         pour x de c(S) à c(S) + m(S) faire
4:             si x ∈ P(S) alors
5:                 cilk_spawn ExploreRec(S^x, G)
6:             fin si
7:         fin pour
8:     sinon
9:         ExplorePile(S^x, G)
10:    fin si
11: fin procedure
```

Nous utilisons la valeur de $G - 10$ car c'est celle qui a donné les meilleurs temps pour un genre cible G entre 45 et 67. Avec cette borne l'appel à ExplorePile est effectué dans plus de 99% des cas. Le surcoût de l'appel récursif à l'aide de **cilk_spawn** est ainsi maîtrisé.

3.6 Résultats et temps de calculs

Grâce aux algorithmes que nous avons développés avec F. Hivert nous avons pu déterminer [69] les nombres n_g de semigroupes numériques de genre g pour $g \leqslant 67$. Depuis la publication de notre article nous avons déterminé les valeurs de n_g pour $g \leqslant 70$.

g	n_g	g	n_g	g	n_g
0	1	24	282 828	48	38 260 496 374
1	1	25	467 224	49	62 200 036 752
2	2	26	770 832	50	101 090 300 128
3	4	27	1 270 267	51	164 253 200 784
4	7	28	2 091 030	52	266 815 155 103
5	12	29	3 437 839	53	433 317 458 741
6	23	30	5 646 773	54	703 569 992 121
7	39	31	9 266 788	55	1 142 140 736 859
8	67	32	15 195 070	56	1 853 737 832 107
9	118	33	24 896 206	57	3 008 140 981 820
10	204	34	40 761 087	58	4 880 606 790 010
11	343	35	66 687 201	59	7 917 344 087 695
12	592	36	109 032 500	60	12 841 603 251 351
13	1 001	37	178 158 289	61	20 825 558 002 053
14	1 693	38	290 939 807	62	33 768 763 536 686
15	2 857	39	474 851 445	63	54 749 244 915 730
16	4 806	40	774 614 284	64	88 754 191 073 328
17	8 045	41	1 262 992 840	65	143 863 484 925 550
18	13 467	42	2 058 356 522	66	233 166 577 125 714
19	22 464	43	3 353 191 846	67	377 866 907 506 273
20	37 396	44	5 460 401 576	68	612 309 308 257 800
21	62 194	45	8 888 486 816	69	992 121 118 414 851
22	103 246	46	14 463 633 648	70	1 607 394 814 170 158
23	170 963	47	23 527 845 502		

FIGURE 5.2 – Les 71 premières valeurs de la suite n_g.

Dans cette section nous comparons les différentes améliorations algorithmiques que nous avons développées à la section précédente afin de mesurer le gain que chacune d'entre elles apporte.

La table suivante contient les temps d'exécution en secondes mis par différents algorithmes pour calculer les valeurs de n_g pour $g \leqslant G$ avec $30 \leqslant G \leqslant 40$ sur un ordinateur équipé d'un processeur `Intel™ i5-3570K` cadencé à `3.4GHz` et possédant `8Go` de mémoire.

`Algorithmz`	30	31	32	33	34	35	36	37	38	39	40
`largeur`	5.0	8.3	14	23	38	1251					
`profondeur`	3.4	5.8	9.2	16	27	45	75	125	204	346	557
`profondeur+`δ	0.3	0.6	1.0	1.7	2.7	4.2	7.4	12	20	32	74
δ`+sse`	0.1	0.2	0.3	0.4	0.8	1.2	2.0	3.1	5.1	9.0	14

Tous les algorithmes sont exécutés sur un seul cœur. L'algorithme `largeur` utilise une exploration en largeur de l'arbre tandis que l'algorithme `profondeur` utilise une exploration en profondeur. Ces deux algorithmes utilisent la même représentation naïve pour les semigroupes numériques. L'algorithme `profondeur+`δ est un raffinement de `depth` utilisant la représentation des semigroupes numériques développée à la section précédente. Les algorithmes δ`+sse` sont des optimisations de la version précédente exploitant les jeux d'instructions vectoriels `SSE`.

Les calculs de n_g pour $g \leqslant 35$ avec l'algorithme `largeur` sont très longs car il consomment plus que les `8Go` de mémoire vive disponible : le système d'exploitation doit donc recourir à la mémoire d'*échange* disponible sur le disque dur de l'ordinateur pour pouvoir poursuivre le calcul. Cet algorithme n'a pas été lancé pour $G \geqslant 36$.

La table suivante illustre l'impact de la parallélisation avec `Cilk++` [83] de l'algorithme δ`+SSE` sur une machine équipée d'un processeur `Intel™ i5-3570K` muni de 4

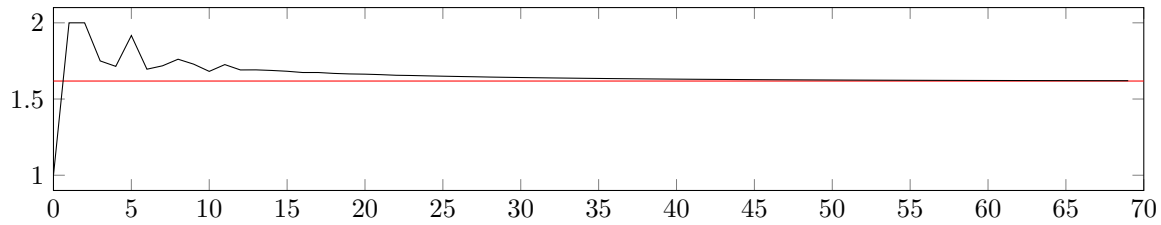


FIGURE 5.5 – Quotient $\frac{n_{g+1}}{n_g}$ pour $g \in [0, 69]$. La ligne rouge a pour équation $y = \phi = \frac{1+\sqrt{5}}{2}$.

cœurs physiques.

Cœurs	30	35	40	45	50
1	0.11	1.26	14.9	182	2201
2	0.06	0.65	7.50	92	1110
3	0.05	0.44	5.14	63	747
4	0.04	0.34	4.02	48	489

Le temps obtenu pour un seul coeur doit être comparé avec la version δ+`SSE` de la table précédente : elle illustre le surcoût occasionné par l'utilisation de la technologie `Cilk++`. Par exemple pour $G = 40$ la version sans `Cilk++` met 14s tandis que celle avec `Cilk++` met 14.9s : le surcoût est donc négligeable surtout à la vue des gains sur les versions utilisant plusieurs cœurs. Il est aussi utile de noter que la technologie `TurboBoost` [130] est présente sur le processeur de test. La fréquence d'horloge du processeur est donc légèrement supérieure quand le nombre de cœurs utilisés est petit. Le gain lors de l'utilisation de plusieurs cœurs serait donc un peu plus grand sans cette technologie.

Avec les valeurs obtenues nous avons pu tester les conjectures 2.6, 2.7 et 2.8 de M. Bras-Amorós pour $g \leqslant 68$, 68 et 69 respectivement.

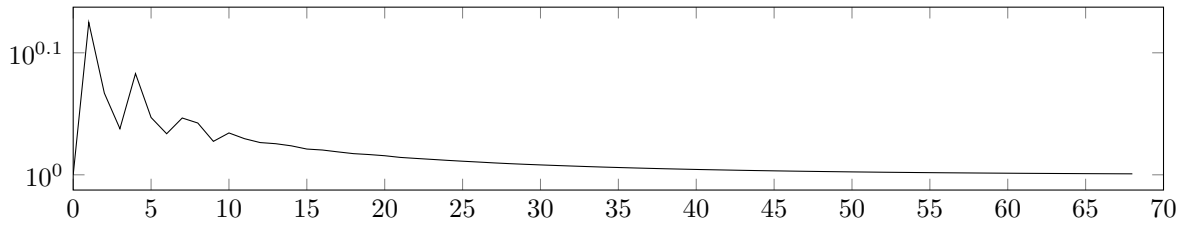


FIGURE 5.3 – Différence $n_{g+2} - n_{g+1} - n_g$ pour $g \in [1, 68]$. L'ordonnée est en échelle logarithmique.

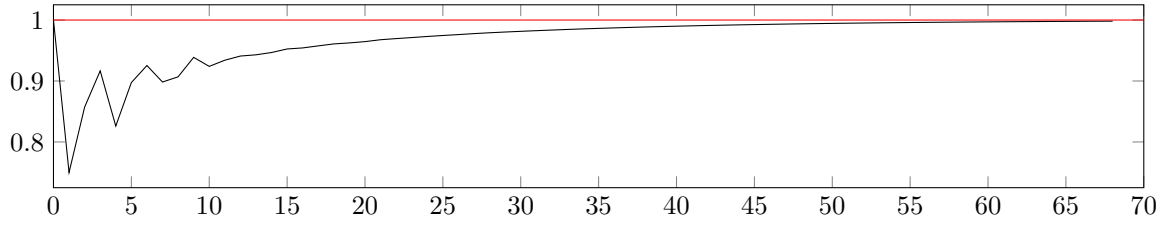


FIGURE 5.4 – Quotient $\frac{n_g+n_{g+1}}{n_{g+2}}$ pour $g \in [0, 68]$. La ligne rouge a pour équation $y = 1$.

4 Conjectures de M. Bras-Amorós

Une façon d'attaquer les conjectures de M. Bras-Amorós est de trouver un bon encadrement de la suite n_g. Les meilleures bornes connues à ce jour sont celles obtenues par S. Elizalde en 2010.

Théorème 4.1 (S. Elizalde, [57]). *Pour tout $g \in \mathbb{N}_+$, on a*

$$a_g \leqslant n_g \leqslant b_g$$

où les suites $(a_g)_g$ et $(b_g)_g$ sont données par leurs séries génératrices respectives

$$\sum_{g\geqslant 1} a_g t^g = t\frac{1-t^2-2t^3-3t^4+t^5+2t^6+3t^7+3t^8+t^9}{(1+t)(1-t)(1-t-t^2)(1-t-t^3)(1-t^3-2t^4-2t^5-t^6)},$$

$$\sum_{g\geqslant 1} b_g t^g = t\frac{2-3t+t^2-4t^3+3t^4-2t^5+t(1-t-t^3)\sqrt{\frac{1+2t}{1-2t}}}{2(1-3t+3t^2-3t^3+4t^4-3t^5+2t^6)}.$$

Ce résultat a été obtenu à l'aide d'une analyse fine de l'arbre des semigroupes numériques.

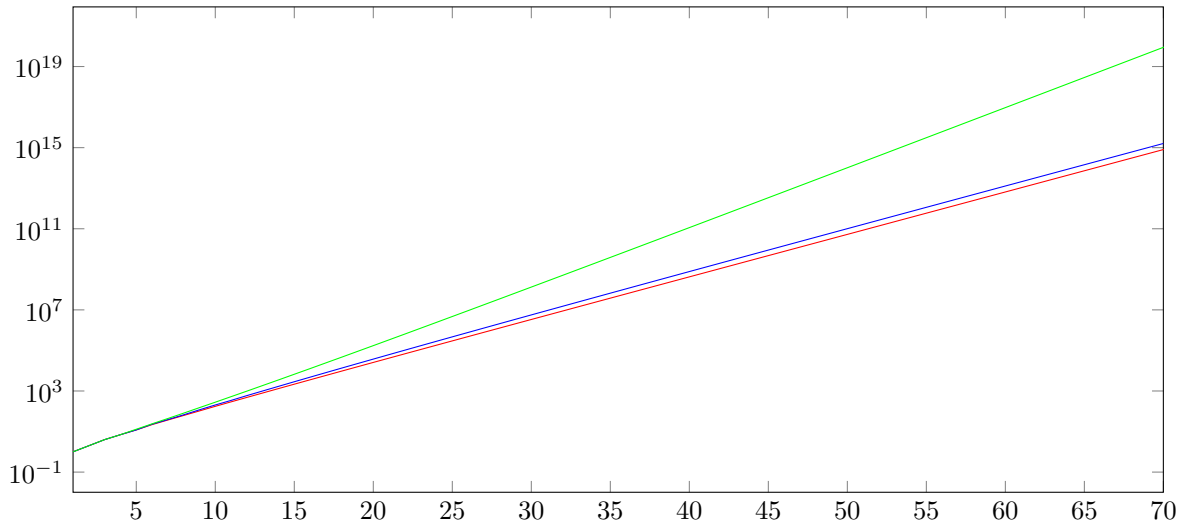


FIGURE 5.6 – Comparaison des suite a_g (en rouge), n_g (en bleu) et b_g (en vert) pour $g \in [1, 70]$. L'axe des ordonnées est en échelle logarithmique.

Nous constatons sur la figure précédente que la minoration de n_g par a_g est assez bonne tandis que la majoration par b_g est assez grossière. Pouvons-nous espérer résoudre les conjectures de M. Bras-Amorós à partir des bornes précédentes ? Par le résultat de S. Elizalde, nous avons

$$n_{g+2} \geqslant a_{g+2} \quad \text{et} \quad n_{g+1} + n_g \geqslant b_{g+1} + b_g.$$

Pour $g \geqslant 6$ nous avons $a_{g+2} < b_{g+1} + b_g$ et nous ne pouvons donc pas espérer obtenir une preuve de la conjecture 2.6 à partir du théorème 4.1. De même pour la conjecture plus faible 2.9 car $a_{g+1} < b_g$ est vérifiée pour $g \geqslant 11$.

En 2009, Y. Zhao [135] tente d'obtenir un encadrement de la suite n_g sans avoir recours à l'analyse de l'arbre des semigroupes numériques $\mathcal{T}_g$. Pour cela il considère une famille particulière de semigroupes numériques.

Définition 4.2. Un semigroupe numérique est dit *générique* s'il vérifie $F(S) < 3m(S)$. Le nombre de semigroupes génériques de genre g est noté n'_g.

Il obtient alors le résultat suivant.

Théorème 4.3 (Y. Zhao, [135] Théorème 3.11)**.** *Il existe $\theta \in]3.32, +\infty]$ tel que*

$$\lim_{g\to+\infty} \frac{n'_g}{\phi^g} = \theta.$$

Dans [135], Y. Zhao n'arrive pas à montrer que la constante θ est finie mais il conjecture que c'est le cas. Il conjecture aussi que la proportion de semigroupes numériques génériques parmi tous ceux de genre g tend vers 1 lorsque g tend vers $+\infty$. Les deux conjectures précédentes impliqueraient en particulier que la rapport $\frac{n'_g}{\phi^g}$ posséderait une limite finie. Notons par exemple que le quotient n_{70} par ϕ^{70} vaut $3.77561\ldots$

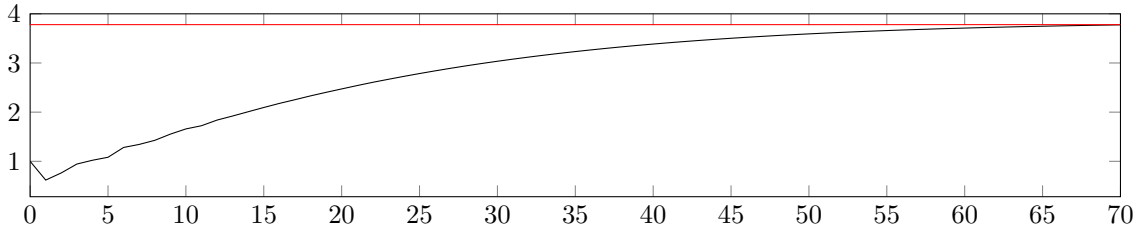


FIGURE 5.7 – Quotient $\frac{n_g}{\phi^g}$ pour $g \in [0, 70]$. La droite rouge a pour équation $y = 3.78$.

Remarque 4.4. Avec les notations de la définition 1.1, nous remarquons que les semigroupes numériques génériques sont exactement ceux de profondeur au plus 3.

Les conjectures précédentes énoncées par Y. Zhao sont démontrées par A. Zhai en 2012 :

Théorème 4.5 (A. Zhai, [134])**.** *Il existe un réel θ tel que*

$$\lim_{g\to+\infty} \frac{n_g}{\phi^g} = \theta.$$

De plus on a

$$\lim_{g\to+\infty} \frac{n'_g}{n_g} = 1.$$

En minorant le nombre de semigroupes numériques génériques qui possèdent une combinatoire assez simple il est facile d'obtenir de bonnes minorations de n_g. Ce n'est malheureusement pas le cas pour les bornes supérieures. Le théorème 4.5 explique donc la différence de qualité entre la minoration et la majoration de n_g donnée par S. Elizalde au théorème 4.1.

La figure 5.8 "illustre" le fait que la proportion de semigroupes numériques tend vers 1 lorsque g tend vers l'infini. Le ligne du bas possède $n_{11} = 343$ points dont 287 noirs correspondant aux semigroupes génériques.

Comme par le théorème 4.5 la suite n_g possède un comportement asymptotique similaire à la suite de Fibonacci, A. Zhai obtient facilement le résultat suivant.

Corollaire 4.6 (A. Zhai, [134])**.** *Les conjectures 2.8 et 2.7 sont vraies.*

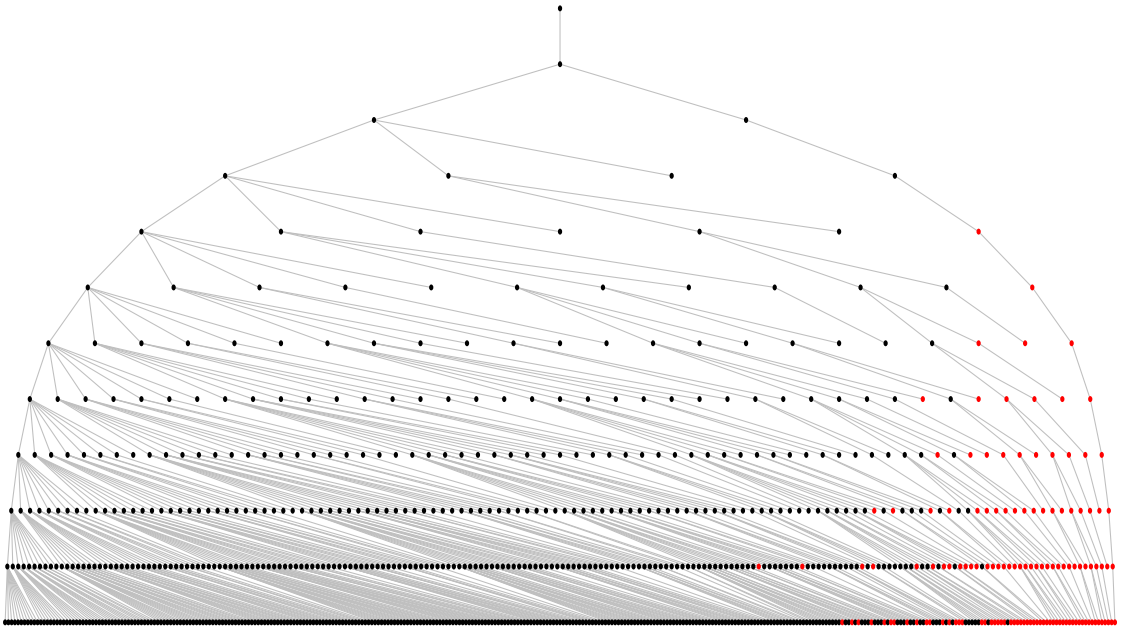


FIGURE 5.8 – Les 12 premiers niveaux de l'arbre $\mathcal{T}_{12}$. Les points noirs correspondent aux semigroupes numériques génériques, c'est-à-dire vérifiant $q \leq 3$.

Malgré le formidable progrès obtenu sur les conjectures de M. Bras-Amorós, la conjecture 2.6 est toujours ouverte. Pire la conjecture 2.9 l'est toujours aussi. Cependant les résultats de A. Zhai, montrent qu'il existe un rang à partir duquel la conjecture précédente est vraie. La conjecture 2.6 sur la croissance forte de la suite n_g semble hors de portée de l'approche développée par Y. Zhao et A. Zhai.

Avec l'algorithme développé à la section 3 nous obtenons, figure 5.9, les valeurs de n'_g pour $g \leqslant 65$.

5 Conjecture de Wilf

La conjecture de Wilf a été formulée par H. Wilf en 1978 et porte sur la positivité d'un certain paramètre $W(S)$ attaché au semigroupe numérique S. Une des dernières avancées sur cette conjecture est sans doute celle de S. Eliahou [47] qui a établi la conjecture de Wilf pour les semigroupes numériques génériques. Pour cela il introduit un paramètre $W_0(S)$ et prouve que celui-ci est positif lorsque S est générique. Dans [52] nous construisons des semigroupes numériques pour lesquels W_0 est négatif et aussi petit que l'on souhaite. Notre construction repose sur l'analyse des 5 semigroupes numériques, parmi les environs 10^{13} de genre au plus 60, possédant un W_0 négatif et que nous avons trouvés grâce aux algorithmes développés dans la section 3.

Nous commençons cette section par une présentation de la conjecture de Wilf, puis par une introduction au nombre W_0 donné dans [47]. Finalement nous redonnerons les résultats obtenus dans [52] sur la construction de semigroupes numériques à W_0 négatif et aussi petit que l'on souhaite. À la fin de cette section nous présentons des travaux en cours, en commun avec M. Delgado, sur la vérification algorithmique de la conjecture de Wilf pour des semigroupes de genre au plus 100.

Définition 5.1. Pour tout semigroupe numérique S, *le nombre de Wilf* de S, noté $W(S)$

g	n'_g	g	n'_g	g	n'_g
0	0	24	237 936	48	35 227 607 540
1	1	25	394 532	49	57 443 335 681
2	2	26	653 420	50	93 635 242 237
3	4	27	1 080 981	51	152 577 300 884
4	6	28	1 786 328	52	248 541 429 293
5	11	29	2 948 836	53	404 736 945 777
6	20	30	4 863 266	54	658 898 299 876
7	33	31	8 013 802	55	1 072 361 202 701
8	57	32	13 194 529	56	1 744 802 234 628
9	99	33	21 707 242	57	2 838 171 714 880
10	168	34	35 684 639	58	4 615 547 228 454
11	287	35	58 618 136	59	7 504 199 621 406
12	487	36	96 221 845	60	12 197 944 701 688
13	824	37	157 840 886	61	19 823 231 255 210
14	1 395	38	258 749 944	62	32 208 621 575 008
15	2 351	39	423 906 805	63	52 321 970 917 845
16	3 954	40	694 076 610	64	84 979 572 462 842
17	6 636	41	1 135 816 798	65	137 996 307 278 819
18	11 116	42	1 857 750 672		
19	18 593	43	3 037 078 893		
20	31 042	44	4 962 738 376		
21	57 180	45	8 105 674 930		
22	86 223	46	13 233 250 642		
23	143 317	47	21 595 419 304		

FIGURE 5.9 – Les 65 premières valeurs de la suite n'_g.

est défini par

$$W(S) = \operatorname{card}(P(S)) \operatorname{card}(L(S)) - c(S)$$

où $L(S) = S \cap [0, c(S) - 1]$.

Comme exactement $g(S)$ éléments de S ne sont pas dans $[0, c(S) - 1]$, nous avons $\operatorname{card}(L(S)) = c(S) - g(S)$ et donc $W(S) = \operatorname{card}(P(S))(c(S) - g(S)) - c(S)$.

Exemple 5.2. Reprenons le semigroupe numérique

$$S_E = \langle 3, 7 \rangle = \{0, 3, 6, 7, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\}$$

de l'exemple 1.9. Nous obtenons $P(S_E) = \{3, 7\}$, $c(S_E) = 12$, $L(S_E) = \{0, 3, 6, 7, 9, 10\}$ et donc $W(S_E) = 2 \times 6 - 12{=}0$.

En 1978, H. Wilf [133] formule la conjecture suivante.

Conjecture 5.3. *Tout semigroupe numérique S vérifie $W(S) \geqslant 0$.*

Depuis sa formulation, la conjecture de Wilf a été vérifiée dans de nombreux cas :

Condition sur S	Auteurs	Année	Référence
$\text{card}\,(P(S)) \leqslant 3$	R. Fröberg, C. Gottlieb et R. Häggkvist	1987	[64]
$\text{card}\,(L(S)) \leqslant 4$	D. Dobbs et G. Matthews	2006	[45]
$f(S) \leqslant 20$	D. Dobbs et G. Matthews	2006	[45]
$g(S) \leqslant 50$	M. Bras-Amorós	2008	[13]
$c(S) \leqslant 2m(S)$	N. Kaplan	2012	[87]
$\text{card}\,(P(S)) \geqslant m(S)/2$	A. Sammartano	2012	[118]
$m(S) \leqslant 8$	A. Sammartano	2012	[118]
$g(S) \leqslant 60$	J. Fromentin et F. Hivert	2016	[69]
$c(S) \leqslant 3m(S)$	S. Eliahou	2018	[47]
$\text{card}\,(L(S)) \leqslant 6$	S. Eliahou	2018	[47]
$\text{card}\,(P(S)) \geqslant m(S)/3$	S. Eliahou	2019	[48]

Les vérifications de la conjecture de Wilf pour $g(S) \leqslant 50$ par M. Bras-Amorós et $g(S) \leqslant 60$ en commun avec F. Hivert ont été faites à l'aide de l'exploration de l'arbre des semigroupes numériques $\mathcal{T}_{50}$ et $\mathcal{T}_{60}$ respectivement. Plus récemment S. Eliahou [47] a montré que la conjecture de Wilf était satisfaite par tous les semigroupes génériques, c'est-à-dire ceux vérifiant $c(S) \leqslant 3m(S)$. Pour cela il introduit un nouveau paramètre $W_0(S)$ plus petit que $W(S)$ et il montre que si S est générique alors $W_0(S)$ est positif, ce qui implique la conjecture de Wilf dans ce cas. Avec la même approche il obtient aussi que la conjecture de Wilf est satisfaite pour $\text{card}\,(L(S)) \leqslant 6$.

5.1 Le nombre $W_0(S)$.

Le nombre de Wilf fait intervenir les primitifs d'un semigroupe numérique ainsi que ses éléments inférieurs au conducteur. Il est alors naturel de séparer les primitifs en deux ensembles, ceux qui sont inférieurs au conducteur et ceux qui ne le sont pas. C'est à partir de cette observation que S. Eliahou à considéré le nombre $W_0(S)$.

Pour pouvoir définir W_0 nous devons introduire quelques notations. Nous rappelons que la profondeur q d'un semigroupe numérique S est la partie entière supérieure de c/m. Nous avons donc la relation

$$c \in [qm - m + 1, qm]. \tag{5.2}$$

Notation 5.4. Pour tout semigroupe numérique S nous notons $\rho(S)$ l'entier vérifiant

$$c(S) = q(S)m(S) - \rho(S). \tag{5.3}$$

Lorsque le contexte le permettra, on notera ρ à la place de $\rho(S)$.

Par la relation (5.2) nous avons immédiatement $0 \leqslant \rho \leqslant m - 1$.

Notation 5.5. Pour tout semigroupe numérique S de profondeur q, nous notons

$$I_q = [c, c + m - 1] \tag{5.4}$$

l'intervalle entier le plus à gauche de longueur m inclus dans S. De manière générale, pour tout $j \in \mathbb{N}$, on note I_j le translaté de I_q par $(j - q)m$. De plus pour tout $j \in \mathbb{N}$, on pose

$$S_j = S \cap I_j. \tag{5.5}$$

Pour tout j de $\mathbb{N}$, nous avons donc

$$\begin{aligned} I_j &= (j-q)m + [c, c+m-1] \\ &= [c-qm+jm, c-qm+(j+1)m-1] \\ &= [jm-\rho, (j+1)m-\rho-1]. \end{aligned}$$

Observons que nous avons $S_j = I_j$ si et seulement si $j \geqslant q$ et que $S_0 = \{0\}$. Finalement, parmi les éléments de S_j, nous isolons ceux qui sont primitifs de ceux qui ne le sont pas : les décomposables.

Notation 5.6. Pour tout semigroupe numérique S et tout $j \in \mathbb{N}$ nous posons

$$P_j = S_j \cap P, \qquad D_j = S_j \cap D = S_j \setminus P_j.$$

Nous avons maintenant les notations nécessaires pour introduire le nombre $W_0(S)$.

Définition 5.7. Pour tout semigroupe numérique S nous posons

$$W_0(S) = \operatorname{card}(P \cap L)\operatorname{card}(L) - q\operatorname{card}(D_q) + \rho.$$

Établissons maintenant le lien existant entre $W_0(S)$ et $W(S)$.

Proposition 5.8. *Pour tout semigroupe numérique S nous avons $W(S) = W_0(S) + \operatorname{card}(P_q)(\operatorname{card}(L) - q)$.*

Démonstration. Comme P est inclus dans $[m, c+m-1]$, nous avons

$$P = P_1 \sqcup \cdots \sqcup P_q.$$

En particulier de $L = S_0 \sqcup \cdots \sqcup S_{q-1}$, nous obtenons $P \cap L = P_1 \sqcup \cdots \sqcup P_{q-1} = P \setminus P_q$. Ainsi nous avons

$$\begin{aligned} W(S) &= \operatorname{card}(P)\operatorname{card}(L) - c \\ &= \operatorname{card}(P \cap L)\operatorname{card}(L) + \operatorname{card}(P_q)\operatorname{card}(L) - qm + \rho. \end{aligned}$$

Par ailleurs l'ensemble S_q est de cardinal m et donc $\operatorname{card}(P_q) + \operatorname{card}(D_q)$ vaut m puis

$$\begin{aligned} W(S) &= \operatorname{card}(P \cap L)\operatorname{card}(L) + \operatorname{card}(P_q)\operatorname{card}(L) - q\operatorname{card}(P_q) - q\operatorname{card}(D_q) + \rho \\ &= W_0(S) + \operatorname{card}(P_q)\operatorname{card}(L) - q\operatorname{card}(P_q) \\ &= W_0(S) + \operatorname{card}(P_q)(\operatorname{card}(L) - q). \end{aligned}$$

□

Corollaire 5.9. *Tout semigroupe numérique S vérifiant $W_0(S) \geqslant 0$ satisfait la conjecture de Wilf.*

Démonstration. Les entiers $0, m, \ldots, (q-1)m$ étant inclus dans L nous avons $\operatorname{card}(L) \geqslant q$. Ainsi la proposition 5.8 implique $W(S) \geqslant W_0(S)$. □

Théorème 5.10 (S. Eliahou [47])**.** *Tout semigroupe numérique générique S vérifie la relation $W_0(S) \geqslant 0$ et donc satisfait la conjecture de Wilf.*

Rappelons que A. Zhai a montré que la proportion de semigroupes numériques génériques de genre g tend vers 1 lorsque g tends vers $+\infty$. S. Eliahou a ainsi établi que la proportion de semigroupes numériques vérifiant la conjecture de Wilf tend aussi vers 1 avec le genre. S'il existe des contre-exemples à la conjecture de Wilf, ils seront donc extrêmement rares.

S	m	$\mathrm{card}\,(P)$	$\mathrm{card}\,(L)$	g	$W_0(S)$	$W(S)$
$\langle 14, 22, 23\rangle_{56}$	14	7	13	43	-1	35
$\langle 16, 25, 26\rangle_{64}$	16	9	13	51	-1	53
$\langle 17, 26, 28\rangle_{68}$	17	10	13	55	-1	62
$\langle 17, 27, 28\rangle_{68}$	17	10	13	55	-1	62
$\langle 18, 28, 29\rangle_{72}$	18	11	13	59	-1	71

FIGURE 5.10 – Les 5 semigroupes de genre $g \leqslant 60$ vérifiant $W_0(S) < 0$.

Remarque 5.11. Si S est une feuille dans l'arbre $\mathcal{T}$ des semigroupes numériques alors S ne possède pas de primitifs supérieurs à c. L'ensemble P_q est donc vide et nous avons alors $W(S) = W_0(S)$ par la proposition 5.8.

Nous pouvons nous demander s'il existe des semigroupes numériques S vérifiant la relation $W_0(S) < 0$. Par le théorème 5.10 de tels semigroupes sont forcément non génériques et donc rares. En utilisant les algorithmes d'exploration de l'arbre $\mathcal{T}_g$ introduit à la section 3 nous avons trouvé seulement 5 semigroupes vérifiant $W_0(S) < 0$ parmi les plus de 10^{13} de genre inférieur à 60. Ces cinq semigroupes vérifient tous $W_0(S) = -1$ et $W(S) \geqslant 0$.

Dans l'article [52] en commun avec S. Eliahou nous exploitons la structure de nos cinq exemples pour construire une famille infinie de semigroupes numériques possédant des valeurs de W_0 aussi petites que souhaitées dans $\mathbb{Z}$:

Théorème 5.12. *Pour tout $n \geqslant 3$ il existe un semigroupe numérique S de profondeur 4 vérifiant $W_0(S) = -\binom{n}{3}$.*

M. Delgado a aussi construit une telle famille de semigroupes en 2016 dans [41] :

Théorème 5.13 (M. Delgado [41])**.** *Pour tout $z \in \mathbb{Z}$, il existe une infinité de semigroupes numériques S vérifiant $W_0(S) = z$.*

La différence principale est que dans [41], l'ensemble $P \cap L$ est de cardinal constant 3 et q tend vers l'infini, tandis que pour le théorème 5.12 la profondeur q est constante à 4 et le cardinal $\mathrm{card}\,(P \cap L)$ tend vers l'infini.

5.2 Obtenir $W_0(S) = -1$

Pour pouvoir facilement décrire les 5 semigroupes de genre $\leqslant 60$ vérifiant $W_0(S) < 0$ nous introduisons la notation suivante.

Notation 5.14. Étant donnés des entiers positifs $a_1, \ldots, a_n$ et t, nous posons

$$\langle a_1, \ldots, a_n\rangle_t = \langle a_1, \ldots, a_n\rangle \cup [t, +\infty[.$$

L'ensemble $\langle a_1, \ldots, a_n\rangle_t$ est toujours un semigroupe numérique même si $a_1, \ldots, a_n$ ne sont pas premiers entre eux. Son conducteur vérifie $c \leqslant t$ et vaut t si et seulement si $t-1$ n'appartient pas à $\langle a_1, \ldots, a_n\rangle$.

Notation 5.15. Pour tout semigroupe numérique S nous posons $X = \mathrm{Ap}(S)$ ainsi que $X_i = \mathrm{Ap}(S) \cap S_i$ pour $i \geqslant 0$ ($\mathrm{Ap}(S)$ désigne les éléments d'Apéry de S et est donné à la définition 1.10).

Remarquons que X_0 est toujours égale à $\{0\}$.

Proposition 5.16. *Pour tout semigroupe numérique S de profondeur $q \geqslant 2$, nous avons*

$$\operatorname{card}(L) = q\operatorname{card}(X_0) + (q-1)\operatorname{card}(X_1) + \cdots + 2\operatorname{card}(X_{q-2}) + \operatorname{card}(X_{q-1}), \quad (5.6)$$
$$\operatorname{card}(D_q) = \operatorname{card}(X_0) + \operatorname{card}(X_1) + \cdots + \operatorname{card}(X_{q-1}) + \operatorname{card}(X_q \cap D). \quad (5.7)$$

Démonstration. Soit $0 \leqslant i \leqslant q-1$. Pour tout $j \geqslant 0$, on a $jm + X_i \subseteq S_{i+j}$. Ainsi de $L = S_0 \sqcup \cdots \sqcup S_{q-1}$ nous obtenons $jm + X_i \subseteq L$ si et seulement $i + j \leqslant q-1$ et donc si et seulement si $j \leqslant q-i-1$. Comme les éléments de $X = X_0 \sqcup \cdots \sqcup X_{q-1}$ sont distincts modulo m, nous avons

$$\bigsqcup_{i=0}^{q-1} ([0, q-i-1]m + X_i) \subseteq L.$$

Réciproquement, soit a un élément de L. Notons x le plus petit élément de L tel que a et x soient équivalents modulo m. Nous avons alors $x \in X = \operatorname{Ap}(S)$ et donc

$$L = \bigsqcup_{i=0}^{q-1} [0, q-i-1]m + X_i \quad \text{puis} \quad \operatorname{card}(L) = \sum_{i=0}^{q-1} (q-i)\operatorname{card}(X_i).$$

Traitons maintenant le cas de D_q. Par construction, on a

$$D_q = S_q \cap D = (X_q \cap D) \sqcup ((S_q \setminus X_q) \cap D).$$

Soit a un élément de $S_q \setminus X_q$. Il existe alors x dans X tel qu'on ait $a = x + km$ avec $k \geqslant 1$. Comme km est un élément non nul de S, l'entier a est un élément décomposable sauf pour $x = 0$ et $k = 1$, ce qui correspond au cas $a = m$. Nous aurions alors $m \in [c, c+m-1] = [qm - \rho, (q+1)m - \rho + 1]$ et donc $q = 1$, ce qui est contraire aux hypothèses. Nous avons donc $a \in D$. Soit i l'unique entier tel que $x \in X_i$. On a alors $k = (q-i)$ et donc $a \in (q-i)m + X_i$. Tout élément de $(q-i)m + X_i$ étant dans $S_q \setminus X_q$ nous obtenons

$$((S_q \setminus X_q) \cap D) = S_q \setminus X_q = \bigsqcup_{i=0}^{q-1} (q-i)m + X_i,$$

et donc

$$D_q = (X_q \cap D) \sqcup \bigsqcup_{i=0}^{q-1} (q-i)m + X_i \quad \text{puis} \quad \operatorname{card}(D_q) = \sum_{i=0}^{q-1} \operatorname{card}(X_i) + \operatorname{card}(X_q \cap D). \quad (5.8)$$

□

Nous avons dû exclure les semigroupes de profondeur $q = 1$ du résultat précédent car si le semigroupe numérique S est de profondeur 1 alors il est de la forme $\{0\} \cup [m, +\infty[$. Nous obtenons donc $S_1 = [m, 2m-1] = P_1$ et $D_1 = \emptyset$. L'ensemble d'Apéry de S étant $X = \{0, m+1, \ldots, 2m-2\}$, nous avons $X_0 = \{0\}$ et $X_1 \cap D = \emptyset$ et donc $\operatorname{card}(X_0) + \operatorname{card}(X_1 \cap D) = 1$ qui est différent du cardinal de D_1.

Proposition 5.17. *Soient m, a, b des entiers de $\mathbb{N}_+$ satisfaisant*

$$(3m+1)/2 \leqslant a < b \leqslant (5m-1)/3. \quad (5.9)$$

Posons $A = \{a, b\}$ et supposons que les éléments

$$A \cup 2A \cup 3A = \{a, b, 2a, a+b, 2b, 3a, 2a+b, a+2b, 3b\}$$

soient deux à deux distincts modulo m. Alors le semigroupe numérique $S = \langle m, a, b\rangle_{4m}$ vérifie $W_0(S) = -1$.

Démonstration. Remarquons que l'inégalité $(3m+1)/2 < (5m-1)/3$ implique $m \leqslant 6$ et que l'hypothèse faite sur $A \cup 2A \cup 3A$ implique $m \geqslant 9$. Nous décomposons le calcul de $W_0(S)$ en plusieurs étapes.
Fait 1 *Nous avons*

$$\begin{aligned} m+1 \leqslant a < b \leqslant 2m-2, \\ 3m+1 \leqslant 2a < 2b \leqslant 4m-2 \\ 4m+1 \leqslant 3a < 3b \leqslant 5m-1 \end{aligned}$$

En effet, c'est une conséquence de (5.9). Ainsi nous avons $A \subseteq [m+1, 2m-2]$, $2A \subseteq [3m+1, 4m-2]$ et $3A \subseteq [4m+1, 5m-1]$.
Fait 2 *Soit c le conducteur de S. Alors $c = 4m$, $q = 4$ et $\rho = 0$.* En effet, à partir du Fait 1 nous obtenons

$$S \cap [3m+1, 4m-1] = (A + 2m) \cup 2A \subseteq [3m+1, 4m-2]$$

et donc $4m-1$ n'appartient pas à S. Le conducteur de S est donc $c = 4m$.
Fait 3 *Les éléments de $\{0\} \cup A \cup 2A \cup 3A$ sont deux à deux distincts modulo m.* Par hypothèse c'est déjà le cas pour les éléments de $A \cup 2A \cup 3A$ et grâce au Fait 1 nous savons qu'ils sont non nuls modulo m.
Fait 4 Nous avons

$$X_1 = A, \quad X_2 = \emptyset, \quad X_3 = 2A, \quad X_4 = X_4 \cap D = 3A.$$

En effet par le Fait 3, nous avons

$$\{0\} \cup A \cup 2A \cup 3A \subseteq X. \tag{5.10}$$

Comme ρ vaut 0 par le Fait 2, nous avons $I_j = [jm, jm+m-1]$ pour tout $j \geqslant 0$. Nous obtenons $S_1 = S \cap [m, 2m-1]$, $S_2 = S \cap [2m, 3m-1]$, $S_3 = S \cap [3m, 4m-1]$ et $S_4 = [4m, 5m-1]$. Le Fait 1 implique alors $A \subseteq S_1$, $2A \subseteq S_3$ et $3A \subseteq S_4$. Comme $X \cap (m+S)$ est vide, nous avons $X \subseteq \langle a, b\rangle$. Les éléments de X étant majorés par $c + m = 5m$, le Fait 1 implique que X est un sous-ensemble de $\{0\} \cup A \cup 2A \cup 3A$. Nous obtenons ainsi $X_1 = X \cap S_1 \subseteq A$, $X_2 = X \cap S_2 = \emptyset$, $X_3 = X \cap S_2 \subseteq 2A$ et $X_4 = X \cap S_4 \subseteq 3A$. Comme tous les éléments de $3A$ sont décomposables on a $X_4 = X_4 \cap D$. L'équation (5.10) nous permet alors de conclure.

Nous pouvons maintenant calculer $W_0(S) = \operatorname{card}(P \cap L)\operatorname{card}(L) - q\operatorname{card}(D_q) + \rho$. Nous avons $P \cap L = \{m, a, b\}$, $q = 4$ et $\rho = 0$. Ainsi $W_0(S)$ est égal à $3\operatorname{card}(L) - 4\operatorname{card}(D_4)$. La proposition 5.17 implique

$$\begin{aligned} \operatorname{card}(L) &= 4\operatorname{card}(X_0) + 3\operatorname{card}(X_1) + 2\operatorname{card}(X_2) + \operatorname{card}(X_3), \\ \operatorname{card}(D_4) &= \operatorname{card}(X_0) + \operatorname{card}(X_1) + \operatorname{card}(X_2) + \operatorname{card}(X_4 \cap D). \end{aligned}$$

De $\operatorname{card}(X_0) = 1$, $\operatorname{card}(X_1) = \operatorname{card}(A) = \operatorname{card}(\{a, b\}) = 2$, $\operatorname{card}(X_2) = 0$, $\operatorname{card}(X_3) = \operatorname{card}(2A) = \operatorname{card}(\{2a, a+b, 2b\}) = 3$ et

$$\operatorname{card}(X_4 \cap D) = \operatorname{card}(3A) = \operatorname{card}(\{3a, 2a+b, a+2b, 3b\}) = 4,$$

nous trouvons

$$\operatorname{card}(L) = 4 \times 1 + 3 \times 2 + 2 \times 0 + 1 \times 3 = 13,$$

ainsi que

$$\operatorname{card}(D_4) = 1 + 2 + 0 + 3 + 4 = 10.$$

Finalement nous avons $W_0(S) = 3\operatorname{card}(L) - 4\operatorname{card}(D_4) = 39 - 40 = -1$. □

Nous vérifions immédiatement que les 5 semigroupes de genre $\leqslant 60$ vérifiant $W_0(S) < 0$ sont tous de la forme $\langle m, a, b\rangle_{4m}$ où m, a, b vérifient les conditions de la proposition 5.17. Nous allons maintenant voir comment construire une infinité de semigroupes numériques S vérifiant $W_0(S) = -1$.

Corollaire 5.18. *Soient k et m des entiers vérifiant $k \geqslant 2$, $m \leqslant 3k+8$ et $m \equiv k \mod 2$. En posant $a = (3m+k)/2$ et $S = \langle m, a, a+1\rangle_{4m}$ nous avons $W_0(S) = -1$.*

Démonstration. Posons $b = a + 1$ et $A = \{a, b\}$ et montrons que les conditions de la proposition 5.17 sont vérifiées. Les inégalités (5.9) sont des conséquences directes de $k \leqslant 2$ et $m \geqslant 3k+8$. Il reste à établir que les éléments de $A \cup 2A \cup 3A$ sont deux-à-deux distincts modulo m. Ce qui est équivalent à établir que les éléments de $(3m + A) \cup (m + 2A) \cup 3A$ sont deux-à-deux distincts modulo m, qui est une conséquence de la chaîne d'inégalités

$$\begin{aligned} 4m + 1 &\leqslant 2a + m < a + b + m < 2b + m && (5.11)\\ &< a + 3m < b + 3m && (5.12)\\ &< 3a < 2a + b < a + 2b < 3b && (5.13)\\ &\leqslant 5m - 1, && (5.14) \end{aligned}$$

qui sont toutes des conséquences immédiates des hypothèses et des inégalités (5.9). □

Parmi les 5 semigroupes de genre $\leqslant 60$ vérifiant $W_0(S) < 0$, quatre peuvent être obtenus à partir du corollaire 5.18 :

m	k	a	$\langle m, a, a+1\rangle$
14	2	22	$\langle 14, 22, 23\rangle_{56}$
16	2	25	$\langle 16, 25, 26\rangle_{64}$
17	3	27	$\langle 17, 27, 28\rangle_{68}$
18	2	28	$\langle 18, 28, 29\rangle_{72}$

Seul le semigroupe $\langle 17, 26, 28\rangle_{68}$ de genre $g \leqslant 60$ n'est pas couvert par le corollaire 5.18.

Dans le but de généraliser la construction précédente et obtenir des semigroupes numériques S avec $W_0(S)$ négatif aussi petit que souhaité nous avons besoin d'introduire la notion d'ensemble B_h utilisé en combinatoire additive et en particulier pour $h = 3$.

5.3 Les ensembles B_h

Soit G un groupe abélien. Soit $A \subseteq G$ un sous-ensemble fini non vide, et $h \geqslant 1$ un entier. Alors nous avons

$$\operatorname{card}(hA) \leqslant \binom{\operatorname{card}(A) + h - 1}{h}. \tag{5.15}$$

Voir [123, section 2.1] pour plus de détails. Cette borne supérieure est mieux comprise en remarquant qu'elle compte le nombre de monômes de degré h en $\operatorname{card}(A)$ variables commutatives.

Définition 5.19. Un sous-ensemble non vide fini A de G est un *ensemble B_h* si $\operatorname{card}(hA)$ atteint la borne supérieure donnée en (5.15).

La proposition suivante permet de caractériser autrement les ensembles B_h.

Proposition 5.20 ([123], section 4.5)**.** *Un sous-ensemble non vide fini A de G est un ensemble B_h si et seulement si, pour tous $a_1, \ldots, a_h, b_1, \ldots, b_h \in A$, nous avons*

$$a_1 + \cdots + a_h = b_1 + \cdots + b_h$$

si et seulement si $(a_1, \ldots, a_h)$ est une permutation de $(b_1, \ldots, b_h)$.

La famille des ensembles B_h de G est stable par translation par un élément de G. Tout ensemble non vide de G est un ensemble B_1 et pour tout $h \geqslant 2$ un ensemble B_h est un ensemble B_{h-1}.

Pour $G = \mathbb{Z}$, tout sous-ensemble $A = \{a, b\}$ de cardinalité 2 est un ensemble B_h pour tout $h \geqslant 1$. En effet nous avons $hA = \{i\,a^i + (h-i)\,b \,|\, i = 0, \ldots, h\}$ et donc

$$\operatorname{card}(hA) = h + 1 = \binom{h+1}{h} = \binom{\operatorname{card}(A) + h - 1}{h}.$$

Par ailleurs l'ensemble $A = \{3, 4, 5\}$ n'est pas un ensemble B_2 car $3 + 5 = 4 + 4$ est dans $2A$.

Pour tout entier $h \geqslant 2$, il existe des ensembles B_h dans $\mathbb{Z}$ arbitrairement grands. Il suffit, par exemple, de prendre $A = \{1, h, h^2, \ldots, h^t\}$ pour $t \geqslant 1$ arbitraire.

Remarque 5.21. Remarquons qu'un ensemble B_h de $\mathbb{Z}$ n'induit par nécessairement un ensemble B_h de $\mathbb{Z}/m\mathbb{Z}$. Cependant, pour tout sous-ensemble A de $\mathbb{Z}$ et tout entier $m \geqslant \operatorname{card}(A)$ si A induit un ensemble B_h de cardinalité $\operatorname{card}(A)$ dans $\mathbb{Z}/m\mathbb{Z}$ alors A est lui-même un ensemble B_h de $\mathbb{Z}$.

Théorème 5.22. *Soient $m, a, b, n \in \mathbb{N}_+$ satisfaisant $n \geqslant 3$ et*

$$(3m+1)/2 \leqslant a < b \leqslant (5m-1)/3. \tag{5.16}$$

Soit $A \subset \mathbb{N}_+$ un sous-ensemble de cardinalité $n-1$ avec $\min A = a$, $\max A = b$ induisant un ensemble B_3 de $\mathbb{Z}/m\mathbb{Z}$. Alors le semigroupe $S = \langle \{m\} \cup A \rangle_{4m}$ vérifie $W_0(S) = -\binom{n}{3}$.

Pour $n = 3$, le théorème 5.22 est exactement la proposition 5.17

Démonstration. La démonstration est une généralisation de celle de la proposition 5.17.
Fait 1 *Nous avons*

$$\begin{aligned} m+1 \leqslant a < b \leqslant 2m-2, \\ 3m+1 \leqslant 2a < 2b \leqslant 4m-2 \\ 4m+1 \leqslant 3a < 3b \leqslant 5m-1 \end{aligned}$$

Ce sont des conséquences directes des hypothèses faites sur a et b. Il en suit $A \subseteq [m+1, 2m-2]$, $2A \subseteq [3m+1, 4m-2]$ et $3A \subseteq [4m+1, 5m-1]$.
Fait 2 *Le conducteur c de S est $4m$ et donc $q = 4$ et $\rho = 0$.* En effet, de $S = \langle \{m\} \cup A \rangle_{4m}$, nous obtenons $c \leqslant 4m$ et donc $c = 4m$ car $4m - 1$ n'appartient pas à S par le Fait 1.
Fait 3 *Les éléments de $\{0\} \cup A \cup 2A \cup 3A$ sont deux à deux distincts modulo m.* Le Fait 1 implique l'inégalité $\operatorname{card}(A) \leqslant m - 2$. Notons $\overline{A}$ l'ensemble induit par A dans $\mathbb{Z}/m\mathbb{Z}$. Par hypothèse $\overline{A}$ est un ensemble B_3 de $\mathbb{Z}/m\mathbb{Z}$ et donc, par la remarque 5.21, A est un ensemble B_3 de $\mathbb{Z}$. Toujours par le Fait 1, les éléments de A sont distincts deux à deux modulo m, et donc $\operatorname{card}(\overline{A}) = \operatorname{card}(A) = n - 1$. Un ensemble B_3 étant en particulier un ensemble B_2, la définition 5.19 donne

$$\begin{aligned} \operatorname{card}(2A) = \operatorname{card}(2\overline{A}) &= \binom{\operatorname{card}(A)+1}{2} = \binom{n}{2}, \\ \operatorname{card}(3A) = \operatorname{card}(3\overline{A}) &= \binom{\operatorname{card}(A)+2}{3} = \binom{n+1}{3}. \end{aligned} \tag{5.17}$$

Les éléments de $2A$ puis de $3A$ sont donc deux à deux distincts modulo m. Si un élément de A est congru à un élément de $2A$ modulo m alors A contiendrait un multiple de m. Le Fait 1 impliquant que les ensembles A, $2A$ et $3A$ ne contiennent pas de multiple de m, nous obtenons que les éléments de $\{0\} \cup A \cup 2A \cup 3A$ sont donc deux à deux distincts modulo m.
Fait 4 *Nous avons*

$$X_1 = A, \quad X_2 = \emptyset, \quad X_3 = 2A, \quad X_4 \cap D = 3A.$$

C'est exactement le même argument que celui utilisé dans la démonstration du fait 4 de la proposition 5.17.

Nous avons $P \cap L = \{m\} \cup A$, et $q = 4$, $\rho = 0$ par le Fait 2. Nous obtenons ainsi $\operatorname{card}(P \cap L) = \operatorname{card}(A) + 1 = n$ puis $W_0(S) = n \operatorname{card}(L) - 4 \operatorname{card}(D4)$. Par le Fait 4, nous avons $\operatorname{card}(X_0) = 1$, $\operatorname{card}(X_1) = \operatorname{card}(A) = n-1$, $\operatorname{card}(X_2) = 0$, $\operatorname{card}(X_3) = \operatorname{card}(2A)$ et $\operatorname{card}(X_4 \cap D) = \operatorname{card}(3A)$. Par les formules (5.6) et (5.7) avec les valeurs de $\operatorname{card}(2A)$ et $\operatorname{card}(3A)$ données en (5.17), nous obtenons

$$\operatorname{card}(L) = 4 + 3(n-1) + \binom{n}{2} = \binom{n}{2} + 3n + 1, \tag{5.18}$$

$$\begin{aligned} \operatorname{card}(D_4) &= 1 + (n-1) + \binom{n}{2} + \binom{n+1}{3} \\ &= \binom{n-2}{0} + \binom{n-1}{1} + \binom{n}{2} + \binom{n+1}{3} = \binom{n+2}{3}. \end{aligned} \tag{5.19}$$

Un dernier calcul donne finalement $W_0(S) = n \operatorname{card}(L) - 4 \operatorname{card}(D_4) = -\binom{n}{3}$. □

Le résultat suivant permet, à l'aide du théorème 5.22, de construire un semigroupe numérique S vérifiant $W_0(S) = -\binom{n}{3}$ à partir d'un ensemble B_3 de $\mathbb{N}$ et de cardinal $n-1$

Corollaire 5.23. *Soit $n \geqslant 3$ un entier. Soit $A' \subset \mathbb{N}$ un ensemble B_3 de cardinal $n-1$ contenant 0. Soit $r = \max A'$ et $k, m \in \mathbb{N}_+$ satisfaisant $k \geqslant r+1$, $m \geqslant 3k+6r+2$ et $m \equiv k \mod 2$. Nous posons $a = (3m+k)/2$ et $A = a + A'$. Le semigroupe numérique $S = \langle \{m\} \cup A \rangle_{4m}$ vérifie $W_0(S) = -\binom{n}{3}$.*

Démonstration. Il suffit de montrer que A satisfait les hypothèses du théorème 5.22. Nous avons $a = \min A$. Posons $b = \max A = a + r$. Les inégalités (5.16) sont des conséquences directes des hypothèses $k \geqslant 2$ et $m \geqslant 3k+8$. Comme A est un translaté de A', qui est un ensemble B_3, c'est aussi un ensemble B_3. Il reste à montrer que A induit un ensemble B_3 de même cardinalité dans $\mathbb{Z}/m\mathbb{Z}$. Posons

$$\begin{aligned} C &= A \cup 2A \cup 3A, \\ C' &= (A + 3m) \cup (2A + m) \cup 3A. \end{aligned}$$

Fait *$C' \subseteq [4m+1, 5m-1]$ et $A+3m, 2A+m, 3A$ sont deux-à-deux disjoints.* C'est une conséquence des inégalités (5.11), (5.12), (5.13) et (5.14) de la démonstration du corollaire 5.18 qui sont elles-mêmes conséquences des hypothèses et des inégalités (5.16). Comme A est un ensemble B_3, les éléments de C sont deux à deux distincts dans $\mathbb{Z}$. C'est donc aussi le cas pour ceux de C'. De plus, comme C' est inclus dans $[4m+1, 5m-1]$ ses éléments sont aussi deux à deux distincts modulo m. Ainsi A est un ensemble B_3 de $\mathbb{Z}/m\mathbb{Z}$. □

Construisons maintenant une famille infinie de semigroupes numériques S vérifiant $W_0(S) = -\binom{n}{3}$ pour n donné. Posons $A' = \{3^0 - 1, 3^1 - 1, \ldots, 3^{n-2} - 1\}$. Alors A' est un ensemble B_3 de cardinalité $n-1$ contenant 0 et peut donc être utilisé avec le corollaire précédent. Posons $r = \max A' = 3^{n-2} - 1$. Soit k un entier tel que $k \geqslant r+1$. Posons $m = 3k + 6r + 2$, $a_k = (3m+k)/2$, $A_k = a_k + A'$ et $S_k = \langle \{m\} \cup A_k \rangle_{4m}$. Alors $W_0(S_k) = -\binom{n}{3}$ pour tout $k \geqslant r+1$.

Ceci termine la démonstration du théorème 5.12.

5.4 Vérification de la conjecture de Wilf

Montrons maintenant que les semigroupes numériques S vérifiant $W_0(S) < 0$ que nous venons de construire satisfont la conjecture de Wilf.

Proposition 5.24. *Tout semigroupe numérique S du théorème 5.22 vérifie $W(S) \geqslant 9$.*

Démonstration. Nous réutilisons les différents résultats établis durant le démonstration du théorème 5.22. Par le Fait 2 nous avons $q = 4$ et donc la proposition 5.8 implique

$$W(S) = W_0(S) + \operatorname{card}(P_4)(\operatorname{card}(L) - 4). \tag{5.20}$$

Fait 5 Nous avons $\operatorname{card}(P_4) \geqslant m/6 \geqslant \operatorname{card}(D_4)/6$. En effet, de $S_4 = P_4 \sqcup D_4$ et $\operatorname{card}(S_4) = m$ nous obtenons $m = \operatorname{card}(P_4) + \operatorname{card}(D_4)$. Par (5.8) nous avons

$$D_4 = (X_4 \cap D) \sqcup \bigsqcup_{i=0}^{3} (X_i + (4-i)m).$$

Le Fait 4 du théorème 5.22 implique alors

$$D_4 = \{4m\} \sqcup (A + 3m) \sqcup (2A + m) \sqcup 3A. \tag{5.21}$$

Par (5.16) et le fait que a et b soient des entiers, nous avons

$$\lceil (3m+1)/2 \rceil \leqslant a < b \leqslant \lfloor (5m-1)/3 \rfloor,$$

ce qui nous donne facilement

$$\begin{aligned} m + \lceil (m+1)/2 \rceil \leqslant a < b &\leqslant m + \lfloor (2m-1)/3 \rfloor, \\ 3m + 1 \leqslant 2a < 2b &\leqslant 3m + 1 + \lfloor (m-2)/3 \rfloor, \\ 4m + \lceil (m+3)/2 \rceil \leqslant 3a < 3b &\leqslant 4m + (m-4). \end{aligned}$$

Il en suit

$$\begin{aligned} A + 3m &\subseteq 4m + [\lceil (m+1)/2 \rceil, \lfloor (2m-1)/3 \rfloor], \\ 2A + m &\subseteq 4m + [1, \lfloor (m-2)/3 \rfloor], \\ 3A &\subseteq 4m + [\lceil (m+3)/2 \rceil, m-1]. \end{aligned}$$

Tous ces sous-ensembles de $S_4 = 4m + [0, m-1]$ sont donc d'intersection vide avec le sous-intervalle J de S_4 donné par

$$\begin{aligned} J &= 4m + [\lfloor (m-2)/3 \rfloor + 1, \lceil (m+1)/2 \rceil - 1] \\ &= 4m + [\lfloor (m+1)/3 \rfloor, \lceil (m-1)/2 \rceil]. \end{aligned}$$

Ainsi, par (5.21), nous obtenons $D_4 \cap J = \emptyset$. Comme J_4 est une partie de $S_4 = D_4 \sqcup P_4$, nous avons nécessairement $J \subseteq P_4$. En considérant les six classes possibles de m modulo 6 nous obtenons

$$\operatorname{card}(J) = \lceil (m-1)/2 \rceil - \lfloor (m+1)/3 \rfloor + 1 \geqslant m/6$$

pour tout $m \in \mathbb{N}_+$. Nous obtenons ainsi $\operatorname{card}(P_4) \geqslant m/6$ et puis $\operatorname{card}(P_4) \geqslant \operatorname{card}(D_4)/6$ car nous avons $m \geqslant \operatorname{card}(D_4)$. La relation (5.20) devient alors

$$W(S) \geqslant \operatorname{card}(D_4)(\operatorname{card}(L) - 4)/6 + W_0(S). \tag{5.22}$$

La relation (5.18) donne $\operatorname{card}(L) - 4 = \binom{n}{2} + 3(n-1)$, où $n = \operatorname{card}(P \cap L) = \operatorname{card}(A) + 1$. Nous avons donc $(\operatorname{card}(L) - 4)/6 \geqslant 1$ car $n \geqslant 3$ par hypothèse. La relation (5.22) implique alors

$$W(S) \geqslant \operatorname{card}(D_4) + W_0(S).$$

Par la formule de D_4 donnée en (5.19) et le théorème 5.22 nous avons

$$\operatorname{card}(D_4) = \binom{n+2}{3}, \quad W_0(S) = -\binom{n}{3},$$

et donc $W(S)$ est croissant en n puis $W(S) \geqslant \binom{5}{3} - \binom{3}{3} = 9$ car $n \geqslant 3$. □

Avec S. Eliahou nous pensons que le borne inférieure de $W_0(S)$ en terme de $\operatorname{card}(P \cap L)$ donnée au théorème 5.22 est certainement optimale pour la profondeur $q = 4$.

Conjecture 5.25. *Soit S un semigroupe numérique avec $q = 4$ et $\operatorname{card}(P \cap L) = n$. Alors $W_0(S) \geqslant -\binom{n}{3}$.*

5.5 Vérification algorithmique de la conjecture de Wilf

M. Delgado a remarqué [42] qu'on pouvait faire des coupes importantes dans l'arbre des semigroupes numériques $\mathcal{T}_g$ lorsque nous cherchons un contre-exemple de genre $g \leqslant G$ à la conjecture de Wilf. Typiquement, depuis les travaux de S. Eliahou dans [48] nous savons que les semigroupes numériques satisfaisant $3 \times \mathrm{card}\,(P(S)) \geqslant m(S)$ vérifient la conjecture de Wilf. Comme les éléments primitifs plus petits que le conducteur d'un semigroupe numérique S sont toujours présents dans le fils S' de S dans l'arbre $\mathcal{T}$, nous obtenons que tous les descendants d'un semigroupe S vérifiant $3 \times \mathrm{card}\,(P(S) \cap [1, c(S) - 1]) \geqslant m(S)$ vérifient la conjecture de Wilf.

En utilisant les algorithmes d'exploration de l'arbre $\mathcal{T}_g$ introduits à la section 3 et en coupant l'arbre dès que possible nous avons vérifié, avec M. Delgado, la conjecture de Wilf jusqu'au genre 80. Ces calculs ont été faits sur la plateforme Calculco [128]. Les calculs en cours suggèrent que nous seront bientôt capables de valider la conjecture de Wilf jusqu'au genre 100.

VI. Filtration de gouffres

Ce chapitre, qui est une suite du chapitre V, présente mes travaux en commun avec S. Eliahou sur les semigroupes numériques réalisés en exploitant la notion de filtration de gouffre.

La première section est une introduction à la notion de filtration de gouffres. La section 2 présente les résultats que j'ai obtenus avec S. Eliahou dans [53] sur la croissance de la suite $(n'_g)_g$ de nombre de semigroupes génériques de genre g. Au cours de la section 3 nous verrons comment, avec S. Eliahou [51] nous avons employé les outils de la section 1 pour redémontrer un résultat de P.A. García-Sánchez, D. Marín-Aragón et A.M. Robles-Pérez [72] portant sur les semigroupes de petites multiplicités.

1 Gouffres et filtrations

La notion de gouffre n'est pas inconnue des spécialistes des semigroupes numériques mais la considérer explicitement nous a permis avec S. Eliahou, d'obtenir des résultats prometteurs sur les semigroupes numériques. Dans cette section nous présentons les outils utilisés dans nos publications communes [53, 51].

Nous avons vu à la section 1 du chapitre 5 que nous pouvions décrire tout semigroupe numérique S à l'aide de son ensemble fini d'éléments primitifs $P(S)$. Une autre idée est d'utiliser un ensemble fini naturellement attaché à tout semigroupe numérique, à savoir son complémentaire dans $\mathbb{N}$, qui est fini par définition.

Nous commençons par déterminer quelle(s) propriété(s) doit vérifier un sous ensemble de $\mathbb{N}$ pour qu'il soit le complémentaire d'un semigroupe numérique.

Définition 1.1. Un *gouffre* est un sous-ensemble fini G de $\mathbb{N}_+$ satisfaisant la propriété suivante : pour tout z dans G, si $z = x + y$ avec $x, y \in \mathbb{N}_+$ alors $x \in G$ ou $y \in G$.

Nous pouvons noter la similarité entre la définition précédente et celle d'idéal premier non nul d'un anneau commutatif : un idéal P non nul d'un anneau commutatif A est premier si pour tout $z = xy \in P$ avec $x \in A$ et $y \in A$ alors $x \in P$ ou $y \in P$.

Proposition 1.2. *Un sous-ensemble G de $\mathbb{N}$ est un gouffre si et seulement si $\mathbb{N} \setminus G$ est un semigroupe numérique.*

Démonstration. Soit G un gouffre. Posons $S = \mathbb{N} \setminus G$. Comme G est fini et ne contient pas 0, nous avons $0 \in S$ et $\operatorname{card}(\mathbb{N} \setminus S) = \operatorname{card}(G) < +\infty$. Montrons que S est stable par addition. Soient x et y deux éléments de $\mathbb{N}_+$. Si $x + y$ n'appartient pas à S alors nous devons avoir $x + y \in G$ et donc, par définition de gouffre, $\{x, y\} \cap G$ est non vide et donc soit x soit y n'appartient à S. Réciproquement on montre que si S est un semigroupe alors $\mathbb{N} \setminus G$ est un gouffre. □

Définition 1.3. Pour tout semigroupe S, on appelle *gouffre* de S l'ensemble $G(S) = \mathbb{N} \setminus S$.

La proposition 1.2 implique que la définition 1.3 est cohérente avec la définition 1.1.

Remarquons qu'il peut être très avantageux de considérer un semigroupe numérique à l'aide de son gouffre $G(S) = \mathbb{N} \setminus S$ plutôt que par ses éléments primitifs $P(S)$. Par exemple le calcul du nombre de Frobenius de S est immédiat à partir de $G(S)$ car on a alors $F(S) = \max(G(S))$. Cependant, les résultats de complexité du problème de Frobenius implique qu'il est, par exemple, difficile d'obtenir les primitifs de S à partir du gouffre $G(S)$ de S. Il y a donc un choix à faire entre représenter un semigroupe S numérique par ses éléments primitifs $P(S)$ ou par son gouffre $G(S)$.

Nous transférons maintenant les paramètres attachés aux semigroupes numériques aux gouffres.

Définition 1.4. Soit G un gouffre.

- la *multiplicité* de G, notée $m(G)$, est le plus petit entier $m \in \mathbb{N}_+$ tel que $m \notin G$;
- le *genre* de G, noté $g(G)$, est le cardinal de G ;
- le *Frobenius* de G, noté $F(G)$, est le plus grand élément de G ;
- le *conducteur* de G, noté $c(G)$, vaut $1 + F(G)$;
- la *profondeur* de G, notée $q(G)$, vaut $\left\lceil \frac{c(S)}{m(S)} \right\rceil$.

Comme pour le cas des semigroupes numériques, on utilisera m, g, F, c et q à la place de $m(G)$, $g(G)$, $F(G)$, $c(G)$ et $q(G)$ lorsque le contexte le permetera.

Exemple 1.5. Reprenons le semigroupe $S_E = \{0, 3, 6, 7, 9, 10\} \cup \{x \in \mathbb{N}, x \geqslant 12\}$ de l'exemple 1.2 du chapitre 5. On a $G_E = G(S_E) = \mathbb{N} \setminus S_E = \{1, 2, 4, 5, 8, 11\}$ et donc $m(G_E) = 3$, $g(G_E) = 6$, $F(G_E) = 11$, $c(G_E) = 12$ et $q(G_E) = \left\lceil \frac{12}{3} \right\rceil = 4$.

1.1 L'arbre des gouffres

L'arbre des semigroupes numériques $\mathcal{T}$ a été dessiné à la figure 5.1 du chapitre V en représentant les semigroupes numériques par leurs éléments primitifs. Dans cette sous-section, nous allons construire cet arbre à l'aide d'une représentation des semigroupes numériques par gouffre. Pour éviter toute confusion l'arbre obtenu sera noté $\mathcal{T}^G$.

Nous commençons par un résultat de stabilité portant sur les gouffres.

Lemme 1.6. *Tout segment initial d'un gouffre est un gouffre.*

Démonstration. Soient G un gouffre et t un entier de $\mathbb{N}_+$. Posons $G' = G \cap [1, t]$. Soit z un élément de G'. Supposons $z = x + y$ avec $x, y \in \mathbb{N}_+$. En particulier x et y appartiennent à $[1, t]$. Comme G est un gouffre on a $\{x, y\} \cap G \neq \emptyset$ et puis $\{x, y\} \cap G' \neq \emptyset$, donc G' est bien un gouffre. □

En particulier, si G est un gouffre non vide, alors l'ensemble $G' = G \setminus \{\max(G)\}$ est aussi un gouffre. Si on note respectivement S et S' les semigroupes numériques associés respectifs, on obtient $S' = S \cup \{F(S)\}$ et donc S' est le père de S dans l'arbre des semigroupes numériques $\mathcal{T}$. Ainsi le gouffre $G' = G \setminus \{\max(G)\}$ sera le père du gouffre G dans l'arbre des gouffres.

Notation 1.7. On note $\mathcal{T}^G$ l'arbre de tous les gouffres et $\mathcal{T}_g^G$ le sous-arbre de $\mathcal{T}^G$ des gouffres de genre au plus g.

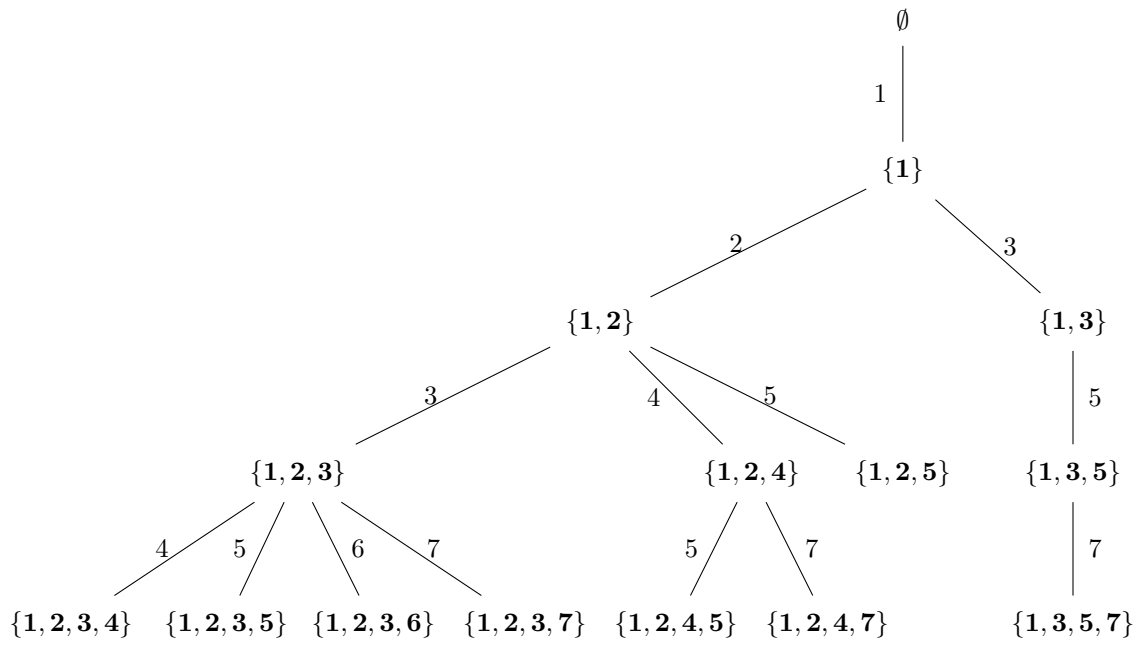


FIGURE 6.1 – Les quatre premiers niveaux de l'arbre $\mathcal{T}^G$ des gouffres, correspondant à $\mathcal{T}_4^G$.

Dans $\mathcal{T}^G$ les fils d'un gouffre G sont exactement les gouffres de la forme $G \sqcup \{a\}$ avec $a > \max(G)$. Les fils de G sont en nombre fini car l'entier a doit nécessairement être inférieur à $\max(G) + m(G)$ pour que $G \sqcup \{a\}$ soit un gouffre. En effet pour $a > \max(G) + m(G)$ l'ensemble $G \sqcup \{a\}$ n'est pas un gouffre car nous avons $a = m(G) + (a - m(G))$ tandis que ni $m(G)$ ni $a - m(G)$ ne sont dans l'ensemble $G \sqcup \{a\}$.

Contrairement à ce qui se passe pour l'arbre $\mathcal{T}$, le passage d'un nœud à son fils dans $\mathcal{T}^G$ est clair : on ajoute un élément au gouffre. Évidemment les deux arbres équivalents sont aussi complexes l'un que l'autre mais cette vision épurée peut permettre de mieux en comprendre la structure.

1.2 Partition canonique

Lemme 1.8. *Tout gouffre G de multiplicité m vérifie $[1, m-1] \subseteq G$ et $G \cap m\mathbb{N} = \emptyset$.*

Démonstration. Par définition de multiplicité, le gouffre G contient l'intervalle $[1, m-1]$ mais pas l'entier m. Soit $k \geqslant 2$. Si km appartient à G alors la formule $km = m + (k-1)m$ implique qu'il en est de même pour $(k-1)m$. Par induction on obtiendrait alors $m \in G$, ce qui est impossible. □

Grâce au lemme précédent nous pouvons couper un gouffre en tranches. Chaque tranche sera contenue entre deux multiples consécutifs de m.

Notation 1.9. Pour tout gouffre G de multiplicité m, on pose $G_0 = [1, m-1]$ et

$$G_i = G \cap [im + 1, (i+1)m - 1] \quad \text{pour tout } i \geqslant 0. \tag{6.1}$$

Comme il en est l'usage, pour $m \in \mathbb{N}$ et $A \subset \mathbb{N}$, on pose $m + A = \{m + a \,|\, a \in A\}$.

Proposition 1.10. *Pour tout gouffre G de multiplicité m et profondeur q nous avons*

$$G = G_0 \sqcup G_1 \sqcup \cdots \sqcup G_{q-1} \tag{6.2}$$

avec $G_{q-1} \neq \emptyset$. De plus nous avons $G_{i+1} \subseteq m + G_i$ pour tout $i \geqslant 0$.

Démonstration. Comme $m\mathbb{N}$ n'est pas inclus dans G, l'ensemble G est la réunion disjointe des G_i pour $i \geqslant 0$. Par définition du Frobenius, de la profondeur et de G, on a $G \subseteq [1, F]$ ainsi que $(q-1)m \leqslant F < qm$. L'entier F appartient donc à G_{q-1} puis G_i est vide pour $i \geqslant q$, ce qui donne (6.2). Il reste à montrer l'inclusion $G_{i+1} \subseteq m + G_i$ pour tout $i \geqslant 0$. Soit x un élément de G_{i+1}. Comme G_{i+1} est inclus dans l'intervalle $[(i+1)m+1, (i+2)m-1]$, on a

$$x - m \in [im+1, (i+1)m-1].$$

Comme m n'appartient pas au gouffre G, la relation $x = m + (x-m)$ implique que $x-m$ appartient à G et donc à l'ensemble $G_i = G \cap [im+1, (i+1)m-1]$. □

Définition 1.11. La *partition canonique* d'un gouffre G est la partition donnée en (6.2).

La multiplicité, le genre et la profondeur d'un gouffre peuvent s'obtenir directement de sa partition canonique. Nous avons par exemple $m = 1 + \max(G_0)$, $g = \sum_i \operatorname{card}(G_i)$ et q est le nombre de tranches de la partition.

Exemple 1.12. Reprenons le gouffre $G_E = \{1, 2, 4, 5, 8, 11\}$ de l'exemple 1.5. Nous avons $m(G_E) = 3$ et donc la partition canonique de G_E est

$$G_E = G_0 \sqcup G_1 \sqcup G_2 \sqcup G_3 = \{1, 2\} \sqcup \{4, 5\} \sqcup \{8\} \sqcup \{11\}.$$

1.3 m-extensions et m-filtrations

Nous venons de voir à la section précédente comment découper un gouffre en une suite d'ensembles à l'aide de sa partition canonique. La notion de m-extension introduite maintenant généralise la notion de partition canonique à n'importe quel ensemble.

Définition 1.13. Soit m un entier de $\mathbb{N}_+$. Une *m-extension* est un sous-ensemble fini A de $\mathbb{N}_+$ admettant une partition

$$A = A_0 \sqcup A_1 \sqcup \cdots \sqcup A_t \tag{6.3}$$

pour un certain $t \geqslant 0$, avec $A_0 = [1, m-1]$ ainsi que $A_{i+1} \subseteq m + A_i$ pour tout $i \geqslant 0$.

Tout comme un gouffre, une m-extension A vérifie $A \cap m\mathbb{N} = \emptyset$. De même, les conditions sur les ensembles A_i impliquent

$$A_i = A \cap [im+1, (i+1)m-1] \quad \text{pour tout } i \geqslant 0. \tag{6.4}$$

Ainsi les ensembles A_i peuvent être entièrement déterminés à partir de A. Notons que, par la proposition 1.10, tout gouffre de multiplicité m est une m-extension. L'inverse n'est cependant pas vrai en général comme l'illustre l'exemple suivant.

Exemple 1.14. L'ensemble $A = \{1, 2, 3, 6, 7, 10\}$ est une 4-extension. En effet, on a

$$A = A_0 \sqcup A_1 \sqcup A_2 = \{1, 2, 3\} \sqcup \{6, 7\} \sqcup \{10\}.$$

Cependant on a $10 \in A$ avec $10 = 5 + 5$ et $5 \notin A$ et donc A n'est pas un gouffre.

Comme les morceaux de la partition d'une m-extension sont localisés entre deux multiples de m, il est naturel de translater chacune des parties pour que celle-ci se trouve incluse dans l'intervalle $[1, m-1]$. C'est le but de la notion de m-filtration que nous allons maintenant introduire.

Définition 1.15. Soit $m \in \mathbb{N}_+$. Une *m-filtration* est une suite $F = (F_0, F_1, \ldots, F_t)$ décroissante de sous-ensembles de $\mathbb{N}_+$ vérifiant

$$[1, m-1] = F_0 \supseteq F_1 \supseteq \cdots \supseteq F_t.$$

Nous pouvons facilement passer d'une m-extension à une m-filtration grâce à l'application suivante.

$$\begin{array}{rcl} \Phi_m : \{m\text{-extensions}\} & \to & \{m\text{-filtrations}\} \\ A_0 \sqcup A_1 \sqcup \cdots \sqcup A_t & \mapsto & (A_0, -m + A_1, \ldots, -tm + A_t) \end{array} \tag{6.5}$$

Exemple 1.16. Les filtrations associées au gouffre G_E de l'exemple 1.12 et à la 4-extension de l'exemple 1.14 sont respectivement

$$F_E = (\{1,2\}, \{1,2\}, \{2\}, \{2\}) \quad \text{et} \quad F = (\{1,2,3\}, \{2,3\}, \{2\})$$

Définition 1.17. On appelle *filtration de gouffre* toute m-filtration F, associée à un gouffre G de multiplicité m.

Voyons comment obtenir une m-filtration à partir d'un gouffre G de multiplicité m et de profondeur q. Comme en (6.1), on pose $G_i = G \cap [im+1, (i+1)m-1]$ pour tout entier i de l'intervalle $[0, q-1]$, de sorte qu'on ait $G = G_0 \sqcup G_1 \sqcup \cdots \sqcup G_{q-1}$. La m-filtration F associée à G est donnée par $F = \Phi_m(G) = (F_0, \ldots, F_{q-1})$ avec $F_i = -im + G_i$.

Définition 1.18. Nous définissons la multiplicité, le genre, le Frobenius, le conducteur et la profondeur d'une filtration de gouffre F comme étant ceux du gouffre $G = \Phi_m^{-1}(F)$.

La définition précédente est correcte seulement si on peut retrouver m à partir d'une filtration de gouffre $F = (F_0, \ldots, F_{q-1})$. C'est en effet le cas car nous avons $m = 1 + \max F_0$. De même q est la longueur de la filtration, g est la somme des cardinaux des F_i, le Frobenius vaut $(q-1)m + \max F_{q-1}$ et donc $c = 1 + (q-1)m + \max F_{q-1}$.

Notation 1.19. On note Γ l'ensemble de tous les gouffres et $\Gamma(g)$ l'ensemble de tous les gouffres de genre g. De même, on note $\mathcal{F}$ l'ensemble de toutes les filtrations de gouffres et $\mathcal{F}(g)$ celles de genre g.

Les bijections Φ_m induisent alors naturellement une bijection entre Γ et $\mathcal{F}$ ainsi qu'entre $\Gamma(g)$ et $\mathcal{F}(g)$ pour tout $g \geqslant 0$. En particulier, nous avons

$$n_g = \operatorname{card}(\Gamma(g)) = \operatorname{card}(\mathcal{F}(g)) \quad \text{pour } g \geqslant 0.$$

Notation 1.20. Étant donné un ensemble $\mathcal{C}$ de conditions, on note $\Gamma(\mathcal{C})$ et $\Gamma(g, \mathcal{C})$ les sous-ensembles de Γ et $\Gamma(g)$ satisfaisant $\mathcal{C}$. On note de même les sous-ensembles $\mathcal{F}(\mathcal{C})$ et $\mathcal{F}(g, \mathcal{C})$ de $\mathcal{F}$ et $\mathcal{F}(g)$ respectivement.

Avec le notation précédente, l'ensemble $\mathcal{F}(g, q \leqslant 3)$ est l'ensemble de toutes les filtrations de genre g et de profondeur $q \leqslant 3$. En particulier pour tout $g \geqslant 0$, nous avons

$$n'_g = \operatorname{card}(\Gamma(g, q \leqslant 3)) = \operatorname{card}(\mathcal{F}(g, q \leqslant 3)).$$

2 La suite n'_g des semigroupes génériques

Avec S. Eliahou, nous avons utilisé les notions développées à la section précédente afin de valider les conjectures de M. Bras-Amorós aux semigroupes génériques [53].

Avant de considérer les semigroupes génériques, c'est-à-dire, les semigroupes numériques de profondeur au plus 3 nous commençons par nous intéresser à ceux de profondeur 2. Nous avons fait ce choix car les techniques utilisées dans le cas $q \leqslant 2$ seront en grande partie utilisées pour le cas $q \geqslant 3$.

2.1 Cas de la profondeur au plus 2.

Dans [135], Y. Zhao montre que le nombre de semigroupes numériques de genre $g \geqslant 0$ et de profondeur $q \leqslant 2$ est égal au nombre de Fibonacci Fib_{g+1}. Pour cela il exprime Fib_n comme une somme de coefficients binomiaux.

Dans cette sous-section nous proposons une démonstration plus simple basée sur la notion de filtration.

Lemme 2.1. *Soit $m \geqslant 1$. Toute m-filtration $F = (F_0, F_1)$ est une filtration de gouffre de multiplicité m et de profondeur $q \geqslant 2$.*

Démonstration. Soit $F = (F_0, F_1)$ une m-filtration et $H = H_0 \sqcup H_1 = \Phi_m^{-1}(F)$ la m-extension associée. On a donc $H_0 = F_0 = [1, m-1]$ et $H_1 = m + F_1$. Soient $z \in H$ et $x, y \in \mathbb{N}_+$ tels que $z = x + y$ avec $x \leqslant y$. Pour montrer que H est un gouffre et donc que F est une filtration de gouffre, il suffit d'établir $\{x, y\} \cap H \neq \emptyset$. Si z est dans H_0 alors $1 \leqslant x+y \leqslant m-1$ est vérifié et donc $1 \leqslant x \leqslant m-1$ l'est aussi puis x est un élément de $H_0 \subseteq H$. Supposons maintenant $z \in H_1 \subseteq [m+1, 2m-1]$. On a donc $2x \leqslant z \leqslant 2m-1$ puis $x \leqslant m-1$ et enfin $x \in H_0 \subseteq H$. □

Proposition 2.2. *Pour tout $g \geqslant 2$, on a*

$$\mathrm{card}\,(\mathcal{F}(g, q \leqslant 2)) = \mathrm{card}\,(\mathcal{F}(g-1, q \leqslant 2)) + \mathrm{card}\,(\mathcal{F}(g-2, q \leqslant 2)) \tag{6.6}$$

Démonstration. Soit $F = (F_0, F_1)$ une filtration de gouffre. Son genre g vaut donc $\mathrm{card}\,(F_0) + \mathrm{card}\,(F_1)$. Pour $g = 0$, on a nécessairement $F_0 = F_1 = \emptyset$ et donc $m = 1$ puis $\mathrm{card}\,(\mathcal{F}(0, q \leqslant 2)) = 1$. De même pour $g = 1$, on a $F_0 = \{1\}$ et $F_1 = \emptyset$ et donc $\mathrm{card}\,(\mathcal{F}(1, q \leqslant 2)) = 1$. Si g vaut 2 on a soit $(F_0, F_1) = (\{1, 2\}, \emptyset)$, soit $(F_0, F_1) = (\{1\}, \{1\})$ et alors

$$\mathrm{card}\,(\mathcal{F}(2, q \leqslant 2)) = 2 = \mathrm{card}\,(\mathcal{F}(1, q \leqslant 2)) + \mathrm{card}\,(\mathcal{F}(0, q \leqslant 2))\,.$$

Supposons maintenant $g \geqslant 3$. Ceci implique en particulier $\mathrm{card}\,(F_0) \geqslant 2$ et donc $m \geqslant 3$. Nous construisons deux ensembles F'_0 et F'_1 en posant

$$\begin{cases} F'_0 = F_0 \setminus \{m-1\} \text{ et } F'_1 = F_1 & \text{si } m-1 \notin F_1, \\ F'_0 = F_0 \setminus \{m-1\} \text{ et } F'_1 = F_1 \setminus \{m-1\} & \text{si } m-1 \in F_1. \end{cases}$$

Par le lemme 2.1, la $(m-2)$-filtration $F' = (F'_0, F'_1)$ est une filtration de gouffre. Le genre de F' est $g-1$ dans le cas $m-1 \notin F_1$ et $g-2$ sinon. Nous avons donc obtenu

$$\mathrm{card}\,(\mathcal{F}(g, q \leqslant 2)) \leqslant \mathrm{card}\,(\mathcal{F}(g-1, q \leqslant 2)) + \mathrm{card}\,(\mathcal{F}(g-2, q \leqslant 2))\,. \tag{6.7}$$

Réciproquement, nous construisons deux applications α_1 et α_2 de $\mathcal{F}(q \leqslant 2)$ dans lui-même en posant

$$\alpha_1(F_0, F_1) = (F_0 \sqcup \{m(F)\}, F_1),$$
$$\alpha_2(F_0, F_1) = (F_0 \sqcup \{m(F)\}, F_1 \sqcup \{m(F)\}),$$

où $m(F) = 1 + \max(F_0)$. Le lemme 2.1 garantit que ces applications α_1 et α_2 sont bien définies. Par construction de α_1 et α_2, nous avons

$$\alpha_1(\mathcal{F}(g, q \leqslant 2)) \subseteq \mathcal{F}(g+1, q \leqslant 2),$$
$$\alpha_2(\mathcal{F}(g, q \leqslant 2)) \subseteq \mathcal{F}(g+2, q \leqslant 2).$$

Les images de α_1 et α_2 sont disjointes. En effet, en posant $(F'_1, F'_2) = \alpha_1(F)$ et $(F''_1, F''_2) = \alpha_2(F)$ nous obtenons $\max(F'_1) > \max(F'_2)$ et $\max(F''_1) = \max(F''_2)$. Ainsi, pour $g \geqslant 2$, nous avons

$$\mathcal{F}(g, q \leqslant 2) \supseteq \alpha_1(\mathcal{F}(g-1, q \leqslant 2)) \sqcup \alpha_1(\mathcal{F}(g-2, q \leqslant 2)),$$

ce qui donne

$$\operatorname{card}(\mathcal{F}(g, q \leqslant 2)) \geqslant \operatorname{card}(\mathcal{F}(g-1, q \leqslant 2)) + \operatorname{card}(\mathcal{F}(g-2, q \leqslant 2)), \tag{6.8}$$

puis le résultat annoncé en utilisant (6.7). □

Corollaire 2.3. *Pour tout $g \geqslant 0$, on a $\operatorname{card}(\mathcal{F}(g, q \leqslant 2)) = Fib_{g+1}$, où Fib_n est le n-ème terme de la suite de Fibonacci.*

Démonstration. Lors de la démonstration de la proposition 2.2, nous avons constaté

$$\operatorname{card}(\mathcal{F}(0, q \leqslant 2)) = 1 = \mathrm{Fib}_1 \quad \text{et} \quad \operatorname{card}(\mathcal{F}(1, q \leqslant 2)) = 1 = \mathrm{Fib}_2.$$

Par la proposition 2.2, les suites $\operatorname{card}(\mathcal{F}(g, q \leqslant 2))$ et F_{g+1} vérifient la même relation de récurrence pour $g \geqslant 2$. □

2.2 Une borne inférieure pour n'_g

Donnons maintenant une borne inférieure pour le nombre de semigroupes génériques de genre g. Comme pour le cas $q \leqslant 2$, nous définissons deux applications sur les filtrations de gouffre $\mathcal{F}(q \leqslant 3)$.

Définition 2.4. Soient $m \in \mathbb{N}_+$. Pour toute m-filtration $F = (F_0, F_1, F_2)$ nous définissons des $(m+1)$-filtrations $\beta_1(F)$ et $\beta_2(F)$ en posant :

$$\beta_1(F) = (F_0 \cup \{m\}, F_1, F_2),$$
$$\beta_2(F) = (F_0 \cup \{m\}, F_1 \cup \{m\}, F_2).$$

Montrons maintenant que les filtrations $\beta_1(F)$ et $\beta_2(F)$ sont bien des filtrations de gouffre. Nous n'avions pas dû faire cette vérification pour les applications α_1 et α_2 du cas $q \leqslant 2$ grâce au lemme 2.1. L'exemple 1.14 montre qu'il ne peut pas y avoir d'équivalent du lemme 2.1 au cas $q \leqslant 3$.

Proposition 2.5. *Si $F = (F_0, F_1, F_2)$ est une filtration de gouffre de genre g, alors $\beta_1(F)$ et $\beta_2(F)$ sont des filtrations de gouffre de genre $g+1$ et $g+2$ respectivement.*

Démonstration. Soit $F = (F_0, F_1, F_2)$ une filtration de gouffre de genre g. On note m sa multiplicité. Le gouffre associé à F et sa partition sont donnés par

$$G = \Phi_m^{-1}(F) = G_0 \sqcup G_1 \sqcup G_2.$$

Par construction, nous avons alors $G_0 = F_0 = [1, m-1]$ ainsi que

$$G_1 = m + F_1 \subseteq [m+1, 2m-1] \tag{6.9}$$
$$G_2 = 2m + F_2 \subseteq [2m+1, 3m-1]. \tag{6.10}$$

Soit $H = \Phi_m^{-1}(\beta_1(F))$ la $(m+1)$-extension associée à $\beta_1(F)$ et $H = H_0 \sqcup H_1 \sqcup H_2$ sa partition canonique. Toujours par construction, nous avons

$$\begin{aligned} H_0 &= F_0 \sqcup \{m\} = [1, m], \\ H_1 &= (m+1) + F_1, \\ H_2 &= 2(m+1) + F_2, \end{aligned}$$

et donc $H_1 = 1 + G_1$, $H_2 = 2 + G_2$. Ainsi, de (6.9) et (6.10) nous obtenons

$$H_1 \subseteq [m+2, 2m], \tag{6.11}$$
$$H_2 \subseteq [2m+3, 3m+1]. \tag{6.12}$$

Le genre de $\beta_1(F)$ puis le genre de H valent $g+1$. Montrons que H est un gouffre. Soit $z \in H$ et $x, y \in \mathbb{N}_+$ tels que $z = x + y$ avec $x \leqslant y$. Nous devons établir $\{x, y\} \cap H \neq \emptyset$. Si x est inférieur à m alors on a $x \in H_0 \subseteq H$. Supposons $x \geqslant m+1$. Nous avons donc $z \geqslant 2m+2$ puis $z \notin H_1$ par (6.11) et donc z est un élément de H_2, ce qui implique $z \leqslant 3m+1$ puis $y \leqslant 2m$. Considérons

$$z' = z - 2 = (x-1) + (y-1).$$

De $z \in H_2 = 2 + G_2$, on obtient $z' \in G_2 \subseteq G$ et donc $\{x-1, y-1\} \in G$ car G est un gouffre. Plus précisément de $m \leqslant x-1 \leqslant y-1 \leqslant 2m-1$, nous avons même $\{x-1, y-1\} \in G_1$ et donc $\{x, y\} \cap H_1 \neq \emptyset$. Comme H_1 est un sous-ensemble de H l'intersection $\{x, y\} \cap H$ est non vide et la $(m+1)$-filtration $\beta_1(F)$ est donc une filtration de gouffre.

Soit $H' = \Phi_m^{-1}(\beta_2(F))$ la $(m+1)$-extension associée à $\beta_2(F)$. La seule différence entre β_1 et β_2 est l'ajout de m à F_1, ce qui contribue pour $m+1+m = 2m+1$ dans H'. Nous avons donc $H' = H \sqcup \{2m+1\}$. Comme nous savons, par ce qui précède, que H est un gouffre, l'ensemble H' est un gouffre si pour tous $x, y \in \mathbb{N}_+$ tels que $2m+1 = x + y$ avec $x \leqslant y$, nous avons $\{x, y\} \cap H' \neq \emptyset$. Or, de $2x \leqslant x + y = 2m+1$, nous obtenons $x \leqslant m$ puis $x \in H_0 \subseteq H'$. □

La proposition 2.5 implique que les applications β_1 et β_2 induisent deux injections :

$$\beta_1, \beta_2 : \mathcal{F}(q \leqslant 3) \to \mathcal{F}(q \leqslant 3).$$

Comme le montre l'exemple suivant, il n'y a aucun espoir de généraliser la proposition 2.5 aux filtrations de profondeur quelconque.

Exemple 2.6. Le gouffre $\{1, 3, 5, 7\}$ a pour filtration $F = (\{1\}, \{1\}, \{1\}, \{1\})$. La seule possibilité d'ajouter un entier à F sans augmenter sa profondeur est de considérer $F' = (\{1, 2\}, \{1\}, \{1\}, \{1\})$. Cependant la 3-extension associée à F' est $\{1, 2, 4, 7, 10\}$ qui contient 10 mais pas 5 tandis que la relation $10 = 5 + 5$ est vérifiée.

Proposition 2.7. *Les images des applications β_1 et β_2 sont disjointes.*

Démonstration. Soit $F = (F_0, F_1, F_2)$ une filtration de $\mathcal{F}(q \leqslant 3)$. Posons

$$F' = (F'_0, F'_1, F'_2) \quad \text{et} \quad F'' = (F''_0, F''_1, F''_2),$$

les images de F par β_1 et β_2 respectivement. Par définition des applications β_1 et β_2 nous avons $\max(F'_0) > \max(F'_1)$ et $\max(F''_0) = \max(F''_1)$. Les images des applications β_1 et β_2 sont donc d'intersection vide. □

Corollaire 2.8. *Pour tout $g \geqslant 2$, nous avons $n'_g \geqslant n'_{g-1} + n'_{g-2}$.*

Démonstration. Soit $g \geqslant 2$. De la proposition 2.5 nous obtenons

$$\beta_1\left(\mathcal{F}(g-1, q \leqslant 3)\right) \subseteq \mathcal{F}(g, q \leqslant 3), \quad \beta_2\left(\mathcal{F}(g-2, q \leqslant 3)\right) \subseteq \mathcal{F}(g, q \leqslant 3),$$

ce qui par la proposition 2.7 donne

$$\mathcal{F}(g-1, q \leqslant 3) \sqcup \mathcal{F}(g-2, q \leqslant 3) \subseteq \mathcal{F}(g, q \leqslant 3)),$$

et donc la relation souhaitée. □

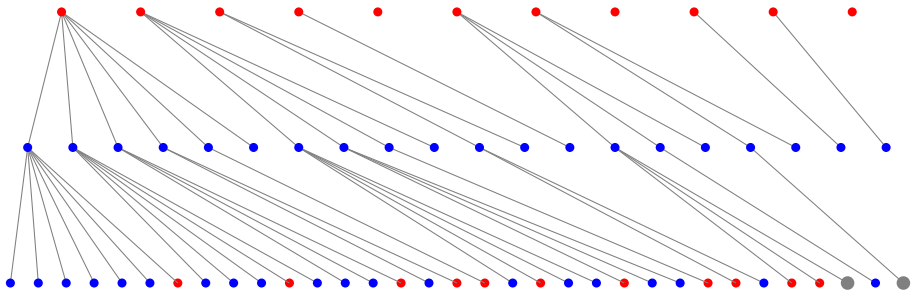


FIGURE 6.2 – Inclusions disjointes des niveaux 5, 6 dans le niveau 7 de l'arbre $\mathcal{T}'$ des semigroupes numériques génériques.

Notons $\mathcal{T}'$ le sous-arbre de $\mathcal{T}$ constitué des semigroupes numériques génériques. Au niveau g, l'arbre $\mathcal{T}'$ a exactement n'_g noeuds. La figure 6.2 montre les niveaux 5, 6 et 7 de $\mathcal{T}'$. Il y a $n'_5 = 11$ points • au niveau 5, et $n'_6 = 20$ points • au niveau 6. Le niveau 7 de l'arbre $\mathcal{T}'$ contient des images disjointes des niveaux 5 et 6 plus deux points •, ce qui donne $n'_7 = 33$ points pour ce niveau.

Nous conjecturons qu'il existe un résultat similaire pour les plus grandes profondeurs q, ce qui donnerait une preuve de la conjecture 2.6.

Conjecture 2.9. *Pour tout $d, g \geqslant 2$, on a*

$$\operatorname{card}\left(\mathcal{F}(g, q \leqslant d)\right) \geqslant \operatorname{card}\left(\mathcal{F}(g-1, q \leqslant d)\right) + \operatorname{card}\left(\mathcal{F}(g-2, q \leqslant d)\right).$$

Les corollaires 2.3 et 2.8 impliquent la conjecture dans les cas $d = 2$ et $d = 3$. Cependant l'exemple 2.6 implique que les méthodes employées dans ces deux cas ne sont pas utilisables pour de plus grandes valeurs de d.

2.3 Une borne supérieure pour n'_g

Montrons maintenant que nous avons $n'_g \leqslant n'_{g-1} + n'_{g-2} + n'_{g-3}$ pour tout $g \geqslant 3$. Nous commençons par caractériser les images de β_1 et β_2.

Proposition 2.10. *Pour toute filtration de gouffre $F = (F_0, F_1, F_2)$ de genre $g \geqslant 2$ on a*

$$F \in \operatorname{Im}(\beta_1) \Leftrightarrow \max(F_0) > \max(F_1),$$
$$F \in \operatorname{Im}(\beta_2) \Leftrightarrow \max(F_0) = \max(F_1) > \max(F_2).$$

Démonstration. Soit $F = (F_0, F_1, F_2)$ une filtration de gouffre de genre g. Par construction des applications β_i, les conditions que doit vérifier F pour appartenir aux images $\operatorname{Im}(\beta_i)$ sont nécessaires. Montrons qu'elles sont suffisantes. L'ensemble $\mathbb{N}$ est le seul semigroupe numérique de multiplicité 1 et il est de genre 0. La multiplicité m de F est donc au moins 2. Nous avons donc

$$\emptyset \neq [1, m-1] = F_0 \supseteq F_1 \supseteq F_2.$$

Ainsi $\max(F_0) = m - 1$ et nous avons deux cas à considérer :

$$\textbf{Cas 1.}\ \max(F_1) < m-1, \qquad \textbf{Cas 2.}\ \max(F_2) < \max(F_1) = m-1.$$

Dans les deux cas on a $\max(F_2) < m - 1$. Montrons $F \in \operatorname{Im}(\beta_1)$ dans le cas 1 et $F \in \operatorname{Im}(\beta_2)$ dans le cas 2. Soit $G = \Phi_m^{-1}(F)$ la m-extension associée à F et $G = G_0 \sqcup G_1 \sqcup G_2$ sa partition canonique. Par construction, nous avons $G_i = im + F_i$ pour $i = 0, 1, 2$. Comme F est une filtration de gouffre, l'ensemble G est un gouffre. Considérons la $(m-1)$-filtration $F' = (F'_0, F'_1, F'_2)$, donnée par

$$F'_0 = F_0 \setminus \{m-1\} = [1, m-2], \quad F'_1 = F_1 \setminus \{m-1\}, \quad F'_2 = F_2.$$

Remarquons, qu'on a $F'_1 = F_1$ dans le cas 1. Soit $G' = \Phi_{m-1}^{-1}(F')$ la $(m-1)$-extension associée à F' et $G' = G'_0 \sqcup G'_1 \sqcup G'_2$ sa partition canonique. Nous avons donc

$$G'_0 = F'_0 = [1, m-2], \quad G'_1 = (m-1) + F'_1, \quad G'_2 = 2(m-1) + F_2.$$

Le genre de G' est $g-1$ dans le cas 1 et $g-2$ dans le cas 2. Montrons que G' est un gouffre dans les deux cas. Le lemme 2.1 garantit que (F'_0, F'_1) est une filtration de gouffre. Ainsi $G'_0 \sqcup G'_1$ est nécessairement un gouffre. Soient $z \in G'_2$ et $x, y \in \mathbb{N}_+$ vérifiant $z = x + y$ et $x \leqslant y$. Montrons qu'on a $\{x, y\} \cap G' \neq \emptyset$. Si x est inférieur à $m-2$ alors c'est un élément de $G'_0 \subseteq G'$.

Supposons $x \geqslant m-1$. De $z \in G'_2$, on obtient l'existence d'un élément t de F_2 tel qu'on ait $z = 2(m-1) + t$. La relation $t \leqslant \max(F_2) \leqslant m-2$ implique $z \leqslant 3m-4$ puis $y \leqslant 2m-3$ et donc :

$$m-1 \leqslant x \leqslant y \leqslant 2m-3.$$

Par ailleurs nous avons

$$(x+1) + (y+1) = z + 2 = 2m + t \in 2m + F_2 = G_2 \subseteq G.$$

Comme G est un gouffre l'intersection de $\{x+1, y+1\}$ avec G est non vide. Les entiers $x+1$ et $y+1$ appartenant à l'intervalle $[m, 2m-2]$, nous obtenons $\{x+1, y+1\} \cap G_1 = \emptyset$ car $\max(G_0) = m-1$ et $\min(G_2) \geqslant 2m+1$. Ainsi soit x, soit y, appartient à $-1 + G_1 = (m-1) + F_1$.

Dans le cas 1 nous avons $F'_1 = F_1$ et donc soit x, soit y, appartient à $(m-1) + F'_1 = G'_1 \subseteq G'$. La filtration F' est alors une filtration de gouffre de genre $g-1$ telle qu'on ait $F = \beta_1(F')$.

Dans le cas 2 nous avons $F'_1 = F_1 \setminus \{m-1\}$. De $x \leqslant y \leqslant 2m-3$ on obtient que x et y sont nécessairement différents de $2m-2 = (m-1) + (m-1)$. Il en suit que soit x, soit y, appartient en fait à $(m-1) + (F_1 \setminus \{m-1\}) = (m-1) + F'_1 = G'_1 \subseteq G'$. La filtration F' est alors une filtration de gouffre de genre $g-2$ telle qu'on ait $F = \beta_2(F')$. □

Soit $F = (F_0, F_1, F_2)$ une filtration de gouffre de genre $g \geqslant 3$ et de profondeur $q \leqslant 3$. Par la proposition précédente, la filtration F est dans l'image de β_1 si et seulement si $\max(F_0) > \max(F_1)$. L'antécédent de F par β_1 est alors la filtration

$$\beta_1^{-1}(F) = (F_0 \setminus \max(F_0), F_1, F_2).$$

De même, s'il existe, l'antécédent de F par l'application β_2 est la filtration

$$\beta_2^{-1}(F) = (F_0 \setminus \max(F_0), F_1 \setminus \max(F_1), F_2).$$

Proposition 2.11. *Soit $F = (F_0, F_1, F_2)$ une filtration de gouffre de multiplicité $m+1 \geqslant 2$ et de profondeur 3. Posons $a_i = \max(F_i)$ et $F'_i = F_i \setminus \{a_i\}$ pour $i = 0, 1, 2$. La suite $F' = (F'_0, F'_1, F'_2)$ est une filtration de gouffre.*

Démonstration. Par hypothèse, nous avons $F_0 = [1, m] \supseteq F_1 \supseteq F_2 \neq \emptyset$ et $m = a_0 \geqslant a_1 \geqslant a_2 \geqslant 1$. Par construction F' est une m-filtration. Notons $G = \Phi_{m+1}(F)$ et $G' = \Phi_m(F')$ les filtrations associées à F et F'. Les partitions canoniques de G et G' sont $G = G_0 \sqcup G_1 \sqcup G_2$ et $G' = G'_0 \sqcup G'_1 \sqcup G'_2 = \Phi_m(F')$ où

$$G_i = i(m+1) + F_i, \quad G'_i = im + F'_i \qquad \text{pour } i = 0, 1, 2.$$

Par hypothèse G est un gouffre et nous devons montrer que c'est aussi le cas pour G'. Par le lemme 2.1, la suite (F'_0, F'_1) est une filtration de gouffre. Ainsi $G'' = G'_0 \sqcup G'_1$ est un gouffre. Nous avons donc fini dans le cas $G'_2 = \emptyset$, qui correspond à $F'_2 = \emptyset$.

Supposons maintenant $F'_2 \neq \emptyset$. Soient $z \in G'$ et $x, y \in \mathbb{N}_+$ vérifiant $z = x + y$ ainsi que $x \leqslant y$. Montrons que l'intersection $\{x, y\} \cap G'$ est non vide. Si z est un élément de G'', qui est un gouffre, nous avons $\{x, y\} \cap G'' \neq \emptyset$ puis $\{x, y\} \cap G' \neq \emptyset$ car G'' est inclus dans G'. On peut donc supposer $z \in G'_2$. Posons $z = 2m + b$ avec $b \in F'_2$ et $b < a_2 \leqslant m$. Si x est inférieur à $m-1$ alors c'est un élément de $F'_0 = G'_0 \subseteq G'$ et nous avons fini. Supposons $x \geqslant m$. De $x + y = z = 2m + b \leqslant 3m - 1$, nous obtenons $y \leqslant 2m-1$. Par ailleurs $z + 2 = 2(m+1) + b$ est un élément de G_2. Comme G est un gouffre, la relation $z + 2 = (x+1) + (y+1)$ implique que l'intersection de $\{x+1, y+1\} \cap G$ est non vide. De $\max(G_0) = m$,

$\min(G_2) \geqslant 2m+3$ et $m+1 \leqslant x+1 \leqslant y+1 \leqslant 2m$, nous obtenons alors $\{x+1, y+1\} \cap G_1 \neq \emptyset$. Ainsi, en retranchant $m+1$, nous avons

$$\{x-m, y-m\} \cap F_1 \neq \emptyset. \tag{6.13}$$

Si l'intersection $\{x-m, y-m\} \cap F'_1$ est non vide alors nous avons fini car alors $\{x, y\} \cap G'_1 \neq \emptyset$. Supposons finalement $\{x-m, y-m\} \cap F'_1 = \emptyset$. La relation (6.13) implique $\{x-m, y-m\} \cap F_1 = \{a_1\}$. Ainsi nous avons soit $x = m+a_1$ soit $y = m+a_1$. Comme la relation $y \geqslant x$ doit être satisfaite, on a nécessairement la relation $y - m \geqslant a_1$. Dans ce cas on obtient

$$2m + b = z = x + y \geqslant x + a_1 + m,$$

et donc $m+b \geqslant x+a_1$. Ce qui implique $x \leqslant m+(b-a_1) < m$ en utilisant $b < a_2 \leqslant a_1$, une contradiction avec l'hypothèse $x \geqslant m$. Le cas $\{x-m, y-m\} \cap F'_1 = \emptyset$ est donc impossible et la preuve est complète. □

Comme l'illustre l'exemple suivant la proposition 2.11 ne peut pas être généralisée aux profondeurs $q \geqslant 4$.

Exemple 2.12. Considérons la 4-filtration $F = (\{1,2,3\}, \{1,3\}, \{1,3\}, \{1,3\})$ correspondant au gouffre $\{1,2,3,5,7,9,11,13,15\}$. Lorsqu'on enlève les éléments maximaux de F, nous obtenons la 3-filtration $F' = (\{1,2\}, \{1\}, \{1\}, \{1\})$ qui est associée à la 3-extension $G' = \{1,2,4,7,10\}$. Cependant $10 = 5+5$ appartient à G' mais pas 5 et donc G' n'est pas un gouffre.

Corollaire 2.13. *Pour tout $g \geqslant 3$, nous avons $n'_g \leqslant n'_{g-1} + n'_{g-2} + n'_{g-3}$.*

Démonstration. Soit $g \geqslant 3$. On pose $X = \mathcal{F}(g, q \leqslant 3)$ qu'on partitionne en $X = X_1 \sqcup X_2 \sqcup X_3$ où pour $F = (F_0, F_1, F_2) \in X$ nous avons

$$\begin{aligned} F \in X_1 &\Leftrightarrow \max(F_0) > \max(F_1); \\ F \in X_2 &\Leftrightarrow \max(F_0) = \max(F_1) > \max(F_2); \\ F \in X_3 &\Leftrightarrow \max(F_0) = \max(F_1) = \max(F_2). \end{aligned}$$

La proposition 2.10 implique $F \in X_i$ si et seulement si $F \in \mathrm{Im}(\beta_i)$ pour $i = 1, 2$. Nous avons donc $\mathrm{card}\,(X_1) = n'_{g-1}$ et $\mathrm{card}\,(X_2) = n'_{g-2}$. Soit F une filtration de X_3. Le maximum de F_0 vaut $m-1$. Posons $F'_i = F_i \setminus \{m-1\}$ pour $i = 0, 1, 2$. La proposition 2.11 garantit que la suite $F' = (F'_0, F'_1, F'_2)$ est une filtration de gouffre de genre $g-3$. A partir de F' nous pouvons retrouver $m = 2 + \max F'_0$ puis F et donc l'application envoyant F sur F' est injective. Le cardinal de X_3 est donc majoré par $\mathrm{card}\,(\mathcal{F}(g-3, q \leqslant 3)) = n'_{g-3}$. Finalement, nous obtenons

$$n'_g = \mathrm{card}\,(X) = \mathrm{card}\,(X_1) + \mathrm{card}\,(X_2) + \mathrm{card}\,(X_3) \leqslant n'_{g-1} + n'_{g-2} + n'_{g-3}. \qquad \square$$

2.4 Résultat principal

Les corollaires 2.8 et 2.13 donnent l'encadrement suivant pour la suite n'_g

Théorème 2.14. *Pour tout $g \geqslant 3$, on*

$$n'_{g-1} + n'_{g-2} \leqslant n'_g \leqslant n'_{g-1} + n'_{g-2} + n'_{g-3}.$$

Le résultat précédent établit des variantes des conjectures 2.9 et 2.6 pour n'_g qui rappelons-le, tend vers n_g lorsque g tend vers $+\infty$ d'après le théorème 4.5 du chapitre V. Il est facile d'obtenir un encadrement clos de la suite n'_g. La suite de *Tribonacci* [132] est la suite d'entiers $(T_n)_{n \geqslant 0}$ définie récursivement par $T_0 = 0$, $T_1 = 1$, $T_2 = 1$ et $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ pour tout $n \geqslant 3$. Les premiers termes de $(T_n)_n$ sont :

$$0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 5\,927, 1705,$$

et son polynôme caractéristique est $p_T = x^3 - x^2 - x - 1$. Nous obtenons ainsi que le taux d'accroissement de $(T_n)_n$ est

$$\lim_{n\to+\infty} \frac{T_n}{T_{n-1}} = \rho_T = \frac{1 + \sqrt[3]{19 + 3\sqrt{33}} + \sqrt[3]{19 - 3\sqrt{33}}}{3} \approx 1.839,$$

où ρ_T est la seule racine réelle de p_t.

Corollaire 2.15. *Pour tout $g \geqslant 2$ nous avons $2Fib_g \leqslant n'_g \leqslant T_{g+1}$.*

Démonstration. Nous avons $(n'_2, n'_3) = (2, 4) = (2F_2, 2F_3)$ et $(n'_1, n'_2, n'_3) = (1, 2, 4) = (T_2, T_3, T_4)$. Nous concluons alors par induction sur g en utilisant les formules de récurrence de n'_g données au théorème 2.14 et celles de Fib_g et T_g. □

L'inégalité $n'_g \geqslant 2F_g$ est une amélioration de $n_g \geqslant 2F_g$ établie par M. Bras-Amorós dans [14]. En utilisant les valeurs de n'_g pour de plus grand genre g, nous pouvons améliorer notre estimation.

Corollaire 2.16. *Pour tout $g \geqslant 63$, nous avons*

$$8F_g \leqslant n'_g \leqslant \frac{7}{1000} T_{g+1}.$$

Démonstration. Nous vérifions que c'est le cas pour $g = 63, 64$ et 65 à l'aide de la figure 5.9 du chapitre V et on conclut par induction sur g à l'aide des formules de récurrence de n'_g, F_g et T_g. □

3 Cas de petite multiplicité

Nous allons maintenant considérer un raffinement de la suite n_g des semigroupes numériques de genre g.

Définition 3.1. On note $\Gamma(g, m)$ l'ensemble des gouffres de genre g et de multiplicité m et on pose $n_{g,m} = \mathrm{card}\,(\Gamma(g, m))$.

Nous rappelons qu'un gouffre est le complémentaire d'un semigroupe numérique et donc $\Gamma(g, m)$ est naturellement en bijection avec l'ensemble des semigroupes numériques de genre g et de multiplicité m. Le nombre $n_{g,m}$ compte donc le nombre de semigroupes numériques de genre g et de multiplicité m.

g	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$m=1$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	...
$m=2$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	...
$m=3$	0	0	1	2	2	2	3	3	3	4	4	4	5	5	5	...
$m=4$	0	0	0	1	3	4	6	7	9	11	13	15	18	20	23	...
$m=5$	0	0	0	0	1	4	7	10	13	16	22	24	32	35	43	...
$m=6$	0	0	0	0	0	1	5	11	17	27	37	49	66	85	106	...

FIGURE 6.3 – Les premières valeurs de la suite $n_{g,m}$ pour le nombre de semigroupes numériques de genre g et de multiplicité m.

N. Kaplan a conjecturé [87] que les suites $(n_{g,m})_g$ étaient croissantes dès que la multiplicité m est supérieure à 2 :

Conjecture 3.2. *Pour $m \geqslant 2$ et $g \geqslant 0$, on a $n_{g+1,m} \geqslant n_{g,m}$.*

À l'aide des valeurs de la suite $n_{g,m}$ présentes à la figure 6.3 nous pouvons constater que nous ne pouvons pas espérer avoir un équivalent de la conjecture 2.6. En effet, nous avons par exemple $n_{3,2} = 1$ tandis que $n_{2,2} + n_{1,2}$ vaut $1 + 1 = 2$ et donc la relation $n_{3,2} \geqslant n_{2,2} + n_{1,2}$ n'est pas vérifiée, de même pour $n_{10,6}$ par exemple.

Comme $n_{g,2}$ vaut 1 pour tout g, la croissance de $(n_{g,2})_g$ est triviale. La conjecture 3.2 a été établie [72] pour les multiplicités $m = 3, 4, 5$ par P.A. García-Sánchez, D. Marín-Aragón et A.M. Robles-Pérez. Pour cela ils utilisent un logiciel de programmation linéaire pour compter les points à coordonnées entières du polytope de Kunz décrivant des inégalités que doivent satisfaire les semigroupes numériques de multiplicité m. Ils obtiennent ainsi des formules closes pour $n_{g,3}$, $n_{g,4}$ et $n_{g,5}$. Finalement ils établissent la croissance de ces suites à l'aide d'un logiciel de calcul formel. La conjecture est aujourd'hui toujours ouverte pour les multiplicités $m \geqslant 6$.

Avec S. Eliahou nous avons utilisé les filtrations de gouffre et les outils associés pour obtenir une démonstration de la croissance des $(n_{g,3})_g$ et $(n_{g,4})_g$ sans avoir recours à l'outil informatique. Les résultats de cette section sont issus de [51].

Nous finissons cette introduction par le résultat général suivant, liant la suite $(n_g)_g$ aux suites $(n_{g,m})_g$.

Lemme 3.3. *Pour $g \geqslant 0$, nous avons*

$$n_g = \sum_{m=1}^{g+1} n_{g,m}.$$

Démonstration. Par le lemme 3.6, on a $m(S) \leqslant g(S) + 1$ pour tout semigroupe numérique S et donc $n_{g,m} = 0$ pour $m \geqslant g + 1$. □

3.1 Le cas $m = 3$

Toute 3-filtration $F = (F_0, \ldots, F_q - 1)$ de profondeur q

$$\{1, 2\} = F_0 \supseteq F_1 \supseteq \cdots \supseteq F_q \neq \emptyset$$

peut s'écrire de l'une des deux manières suivantes

$$F = (\underbrace{\{1,2\}, \ldots, \{1,2\}}_{a}, \underbrace{\{1\}, \ldots, \{1\}}_{b}) = \{1,2\}^a\{1\}^b \tag{6.14}$$

$$F = (\underbrace{\{1,2\}, \ldots, \{1,2\}}_{a}, \underbrace{\{2\}, \ldots, \{2\}}_{b}) = \{1,2\}^a\{2\}^b \tag{6.15}$$

avec $a \geqslant 1$, $b \geqslant 0$. Par définition de la profondeur et du genre d'une filtration nous avons $q = a + b$ ainsi que $g(F) = \sum_i \operatorname{card}(F_i) = 2a + b$.

Théorème 3.4. *Les filtrations de gouffre de multiplicité 3 sont*

$$\{1,2\}^a\{1\}^b \qquad \textit{avec } 0 \leqslant b \leqslant a + 1,$$
$$\{1,2\}^a\{2\}^b \qquad \textit{avec } 0 \leqslant b \leqslant a,$$

et dans les deux cas $a \geqslant 1$.

Démonstration. Si F est une filtration de gouffre de multiplicité 3, alors F est de la forme (6.14) ou (6.15). Nous devons donc caractériser les filtrations de gouffre parmi les 3-filtrations de chacune des deux formes.

Cas 1. Soit $F = \{1,2\}^a\{1\}^b$ avec $a \geqslant 1$ et $b \geqslant 0$ une 3-filtration de la forme (6.14). Montrons que F est une filtration de gouffre si et seulement si on a $b \leqslant a$. On pose $G = \Phi_m^{-1}(F)$ la m-extension associée à F et $G = G_0 \sqcup G_1 \sqcup \cdots \sqcup G_{a+b-1}$ sa partition canonique. Nous avons donc $G_i = 3i + F_i$ pour $i \in [0, a+b-1]$. De $F_0 = \cdots = F_{a-1} = \{1,2\}$ et $F_a = \cdots = F_{a+b-1} = \{1\}$, nous obtenons

$$3\mathbb{N} \cap G = \emptyset \tag{6.16}$$

$$3i+1 \in G \Leftrightarrow i \leqslant a+b-1 \tag{6.17}$$

$$3i+2 \in G \Leftrightarrow i \leqslant a-1. \tag{6.18}$$

Soit z un élément de G et considérons la décomposition $z = x + y$ avec $0 < x \leqslant y$. Par les relations précédentes, l'entier z est nécessairement congru à 1 ou 2 modulo 3. Déterminons en fonction de la classe d'équivalence de z des conditions nécessaires et suffisantes sur a et b pour que nous ayons $G \cap \{x,y\} \neq \emptyset$.

Cas 1.1. Supposons $z = 3i+1$. Nous avons donc $i \leqslant a+b-1$. La décomposition $z = 3i+1 = x+y$ vérifie nécessairement :

$$(x,y) = (3r+1, 3(i-r)) \quad \text{ou} \quad (x,y) = (3s+2, 3(i-1-s)+2),$$

avec $0 \leqslant r \leqslant i-1$ ou $0 \leqslant s \leqslant i-1$. Dans le cas $(x,y) = (3r+1, 3(i-r))$, la relation (6.17) implique que l'entier $3r+1$ appartient à G car les inégalités $r \leqslant i-1 \leqslant a+b-1$ sont forcément vérifiées. Supposons qu'on ait $(x,y) = (3s+2, 3(i-1-s)+2)$ et $\{x,y\} \cap G \neq \emptyset$. La relation (6.18) implique alors soit $s \leqslant a-1$ soit $i-1-s \leqslant a-1$. La dernière inégalité se réécrit $s \geqslant i-a$. Si s est supérieur à a, la relation $s \leqslant a-1$ n'est pas vérifiée et nous devons avoir $s \geqslant i-a$ puis $a \geqslant i-a$. Comme la plus grande valeur que peut prendre i est $a+b-1$, nous devons avoir $a \geqslant a+b-1-a = b-1$ et donc $b \leqslant a+1$ pour que G soit un gouffre. Nous venons donc de montrer que pour tout $x, y \in \mathbb{N}_+$ la relation $3i+1 = x+y \Rightarrow \{x,y\} \cap G \neq \emptyset$ est vérifiée pour tout i tel que $3i+1$ appartient à G si et seulement si $b \leqslant a+1$.

Cas 1.2. Supposons $z = 3i+2 \in G$. Nous avons donc $i \geqslant a-1$. La décomposition $z = 3i+2 = x+y$ vérifie nécessairement :

$$(x,y) = (3r+2, 3(i-r)) \quad \text{ou} \quad (x,y) = (3s+1, 3(i-s)+1)$$

avec $0 \leqslant r \leqslant i-1$ ou $0 \leqslant s \leqslant i$. Dans le cas $(x,y) = (3r+2, 3(i-r))$, la relation (6.18) implique que l'entier $3r+2$ appartient à G car nous avons déjà $r \leqslant i-1 \leqslant a-1$. Dans le cas $(x,y) = (3s+1, 3(i-s)+1)$, la relation (6.17) implique $3s+1 \in G$ car nous avons déjà $s \leqslant i \leqslant a+b-1$. Nous venons donc de montrer que pour tout $x, y \in \mathbb{N}_+$ la relation $3i+2 = x+y \Rightarrow \{x,y\} \cap G \neq \emptyset$ est toujours vérifiée dès que $3i+2$ appartient à G.

Finalement nous avons obtenu que l'ensemble G est un gouffre si et seulement si la relation $b \leqslant a+1$ est vérifiée.

Cas 2. On traite le cas d'une filtration $F = \{1,2\}^a\{2\}^b$ de façon similaire au cas 1. □

Corollaire 3.5. *Pour tout $g \geqslant 0$ nous avons $n_{g+1,3} \geqslant n_{g,3}$.*

Démonstration. Comme $n_{g,3}$ vaut 0 pour $g \leqslant 1$, nous pouvons supposer $g \geqslant 2$. Il est suffisant de construire une injection de $\mathcal{F}(g,3)$ dans $\mathcal{F}(g+1,3)$. Soit $F = (F_0, \ldots, F_t)$ une 3-filtration de genre g. On note $f^{(1)}(F)$, *resp.* $f^{(2)}(F)$, la 3-filtration obtenue en ajoutant 1, *resp.* 2, à la première partie F_i qui n'en contient pas. Dans le cas $F_0 = \cdots = F_t = \{1,2\}$ nous posons $f^{(1)}(F) = (F_0, \ldots, F_t, \{1\})$, de même pour $f^{(2)}(F)$. À l'aide de la caractérisation des 3-filtrations donnée en (6.14) et en (6.15), nous avons

$$\{1,2\}^a \overset{f^{(1)}}{\longmapsto} \{1,2\}^a\{1\} \qquad \{1,2\}^a \overset{f^{(2)}}{\longmapsto} \{1,2\}^a\{2\},$$

$$\{1,2\}^a\{1\}^b \overset{f^{(1)}}{\longmapsto} \{1,2\}^a\{1\}^{b+1} \qquad \{1,2\}^a\{1\}^b \overset{f^{(2)}}{\longmapsto} \{1,2\}^{a+1}\{1\}^b,$$

$$\{1,2\}^a\{2\}^b \overset{f^{(1)}}{\longmapsto} \{1,2\}^{a+1}\{2\}^b \qquad \{1,2\}^a\{2\}^b \overset{f^{(2)}}{\longmapsto} \{1,2\}^a\{2\}^{b+1}.$$

Par construction $f^{(1)}(F)$ et $f^{(2)}(F)$ sont des 3-filtrations de genre $g+1$ mais ne sont pas nécessairement des filtrations de gouffre même si F en est une. Le théorème 3.4 nous permet d'obtenir les conditions

suivantes pour que ce soit le cas :

$$f^{(1)}\left(\{1,2\}^a\{1\}^b\right) \in \mathcal{F}(g+1,3) \Leftrightarrow b+1 \leqslant a+1, \qquad f^{(2)}\left(\{1,2\}^a\{1\}^b\right) \in \mathcal{F}(g+1,3) \Leftrightarrow b \leqslant a+2,$$
$$f^{(1)}\left(\{1,2\}^a\{2\}^b\right) \in \mathcal{F}(g+1,3) \Leftrightarrow b \leqslant a+1, \qquad f^{(2)}\left(\{1,2\}^a\{2\}^b\right) \in \mathcal{F}(g+1,3) \Leftrightarrow b+1 \leqslant a.$$

Si par exemple F est une partition de gouffre de la forme $\{1,2\}^a\{2\}^b$, le théorème 3.4 implique $b \leqslant a$ et donc $f^{(1)}(F)$ est toujours une filtration de gouffre dans ce cas car la relation $b \leqslant a+1$ est évidemment vérifiée. En faisant de même pour les autres cas, nous obtenons

$$F = \{1,2\}^a\{1\}^b \in \mathcal{F}(g,3) \Rightarrow \begin{cases} f^{(1)}(F) \in \mathcal{F}(g+1,3) & \text{si } b \leqslant a, \\ f^{(2)}(F) \in \mathcal{F}(g+1,3) & \text{pour tout } a \text{ et } b, \end{cases}$$
$$F = \{1,2\}^a\{2\}^b \in \mathcal{F}(g,3) \Rightarrow \begin{cases} f^{(1)}(F) \in \mathcal{F}(g+1,3) & \text{pour tout } a \text{ et } b, \\ f^{(2)}(F) \in \mathcal{F}(g+1,3) & \text{si } b+1 \leqslant a. \end{cases}$$

Toujours par le théorème 3.4, le seul cas où F est une filtration de gouffre mais pas $f_g^{(1)}(F)$ est obtenu pour $F = \{1,2\}^a\{1\}^{a+1}$ et dans ce cas le genre g de F vaut $2a+a+1 = 3a+1$. Notons que dans ce cas nous avons $g \equiv 1 \mod 3$. De même le seul cas où $F \in \mathcal{F}(g,3)$ et $f_g^{(2)}(F) \notin \mathcal{F}(g+1,3)$ est $F = \{1,2\}^a\{2\}^a$ et alors le genre de F est $g = 2a+a = 3a$. Notons que dans ce cas nous avons $g \equiv 0 \mod 3$. Nous construisons ainsi une injection f_g de $\mathcal{F}(g,3)$ dans $\mathcal{F}(g+1,3)$ en posant

$$f_g = \begin{cases} f^{(1)} & \text{pour } g \equiv 0,2 \mod 3, \\ f^{(2)} & \text{pour } g \equiv 1 \mod 3. \end{cases}$$

Nous obtenons ainsi $\operatorname{card}(\mathcal{F}(g,3)) \leqslant \operatorname{card}(\mathcal{F}(g+1,3))$ puis $n_{g,3} \leqslant n_{g+1,3}$. □

3.2 Représentation compacte de filtration

Avant de démontrer la croissance de la suite $(n_{g,4})_g$ nous développons des outils généraux à l'étude des suites $(n_{g,m})_g$ basés sur une représentation compacte de m-filtration. Ces outils généralisent et formalisent les notions utilisées pour les démonstrations du théorème 3.4 et du corollaire 3.5

Proposition 3.6. *Pour toute m-filtration $F = (F_0, \dots, F_t)$ il existe une permutation $\sigma \in \mathfrak{S}_{m-1}$ et des entiers $e_0, \dots, e_{m-2}$, appelés* e-coordonnées, *tels que*

$$F = \big(\underbrace{F'_0, \dots, F'_0}_{e_0}, \underbrace{F'_1, \dots, F'_1}_{e_1}, \dots, \underbrace{F'_{m-2}, \dots, F'_{m-2}}_{e_{m-2}}\big)$$

où $F'_0 = [1, m-1]$ et $F'_i = F'_{i-1} \setminus \{\sigma(i)\}$ pour $i = 1, \dots, m-2$. En particulier le cardinal de F'_i est $m-i-1$.

Démonstration. Comme F est une m-filtration, nous avons

$$[1, m-1] = F_0 \supseteq F_1 \supseteq \cdots \supseteq F_t, \tag{6.19}$$

avec de possibles égalités. Après avoir retiré les répétitions, nous obtenons

$$[1, m-1] = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_s,$$

avec $\{F_0, F_1, \dots, F_t\} = \{H_0, H_1, \dots, H_s\}$. Notons μ_i le nombre d'occurrences de H_i dans (6.19) :

$$F = (\underbrace{H_0, \dots, H_0}_{\mu_0}, \underbrace{H_1, \dots, H_1}_{\mu_1}, \dots, \underbrace{H_s, \dots, H_s}_{\mu_s}). \tag{6.20}$$

Maintenant, entre chaque paire $H_{i-1} \supsetneq H_i$, nous insérons une chaîne descendante maximale de sous-ensemble $H'_{i,j}$:

$$H_{i-1} = H'_{i,0} \supsetneq H'_{i,1} \supsetneq \cdots \supsetneq H'_{i,k_i} = H_i,$$

où $k_i = |H_{i-1}| - |H_i|$. Ainsi $|H'_{i,j}| = |H_{i-1}| - j$ pour tout $0 \leqslant j \leqslant k_i$. Nous obtenons ainsi une chaîne maximale de sous-ensembles

$$F' = [1, m-1] = F'_0 \supsetneq F'_1 \supsetneq \cdots \supsetneq F'_{m-2},$$

où chaque terme a un élément de moins que le précédent. Par construction, nous avons les égalités

$$\{F_0, F_1, \ldots, F_t\} = \{H_0, H_1, \ldots, H_s\} \subseteq \{F'_0, F'_1, \ldots, F'_{m-2}\},$$

et chaque F'_i apparaît $e_i \geqslant 0$ fois dans $\{F_0, F_1, \ldots, F_t\}$. On a donc

$$F = (\underbrace{F'_0, \ldots, F'_0}_{e_0}, \underbrace{F'_1, \ldots, F'_1}_{e_1}, \ldots, \underbrace{F'_{m-2}, \ldots, F'_{m-2}}_{e_{m-2}}).$$

Finalement, comme chaque F'_i est obtenu en retirant un élément particulier de F'_{i-1} pour $1 \leqslant i \leqslant m-2$, il existe une permutation σ de $[1, m-1]$ telle que nous ayons

$$F'_i = F'_{i-1} \setminus \{\sigma(i)\}$$

pour $1 \leqslant i \leqslant m-2$. □

Notation 3.7. Étant donnés $\sigma \in \mathfrak{S}_{m-1}$ et $e = (e_0, \ldots, e_{m-2}) \in \mathbb{N}^{m-1}$ avec $e_0 \geqslant 1$, nous notons $F(\sigma, e)$ la m-filtration

$$F = (\underbrace{F'_0, \ldots, F'_0}_{e_0}, \underbrace{F'_1, \ldots, F'_1}_{e_1}, \ldots, \underbrace{F'_{m-2}, \ldots, F'_{m-2}}_{e_{m-2}})$$

où $F'_i = F'_{i-1} \setminus \{\sigma(i)\}$ pour $1 \leqslant i \leqslant m-2$. Nous notons aussi $G(\sigma, e) = \Phi_m^{-1}(F)$ la m-extension associée et $S(\sigma, e) = \mathbb{N} \setminus G(\sigma, e)$ son complémentaire.

Malgré ce que peut suggérer la notation, l'ensemble $S(\sigma, e)$ n'est pas nécessairement un semigroupe numérique, ce sera le cas lorsque $F(\sigma, e)$ sera une filtration de gouffre.

Exemple 3.8. Considérons la 5-filtration $F = (\{1,2,3,4\}, \{1,2\}, \{1\})$. Nous pouvons décomposer F de la façon suivante :

$$F = \big(\underbrace{\{1,2,3,4\}}_{1}, \underbrace{\{1,2,3\}}_{0}, \underbrace{\{1,2\}}_{1}, \underbrace{\{1\}}_{1}\big).$$

Ainsi F est égale à $F(\sigma, e)$ avec $\sigma = (4,3,2,1) \in \mathfrak{S}_4$ et $e = (1,0,1,1)$. Il est important de noter que la permutation σ n'est pas unique car nous avons aussi $F = F(\sigma', e)$ avec $\sigma' = (3,4,2,1)$. Par contre l'exposant e est unique car il est caractérisé par la suite des cardinaux $\operatorname{card}(F_i)$.

Une question naturelle est de savoir sous quelle(s) condition(s), portant sur σ et e, la filtration $F(\sigma, e)$ est une filtration de gouffre.

Lemme 3.9. *Pour $\sigma \in \mathfrak{S}_{m-1}$ et $e = (e_0, \ldots, e_{m-2}) \in \mathbb{N}^{m-1}$ avec $e_0 \geqslant 1$, nous avons*

$$S(\sigma, e) = \bigsqcup_{i=0}^{m-1} \sigma(i) + m(e_0 + \cdots + e_{i-1} + \mathbb{N}), \tag{6.21}$$

avec les conventions $\sigma(0) = 0$ et $e_0 + \cdots + e_{i-1} = 0$ pour $i = 0$.

Démonstration. Pour $0 \leqslant i \leqslant m-1$, nous posons $F_i = [1, m-1] \setminus \{\sigma(1), \dots, \sigma(i)\}$. Par définition, nous avons

$$F(\sigma, e) = (\underbrace{F_0, \dots, F_0}_{e_0}, \underbrace{F_1, \dots, F_1}_{e_1}, \dots, \underbrace{F_{m-2}, \dots, F_{m-2}}_{e_{m-2}}).$$

Posons $F = F(\sigma, e)$ et $G = G(\sigma, e) = \Phi_m^{-1}(F)$. Pour $k \in [0, m-1]$, on pose $G^{(k)} = \{x \in G \mid x \equiv k \bmod m\}$. Nous obtenons ainsi

$$G = \bigsqcup_{k=0}^{m-1} G^{(k)}.$$

Comme G est une m-extension, l'intersection $G \cap m\mathbb{N}$ est vide et donc $G^{(0)} = \emptyset$. Déterminons $G^{(k)}$ pour $k \geqslant 1$. Comme σ est une permutation de $[1, m-1]$, il existe $i \in [1, m-1]$ tel qu'on ait $k = \sigma(i)$. Ainsi pour tout $r \geqslant 0$ nous avons

$$\sigma(i) \in F_r \Leftrightarrow r \leqslant i - 1. \tag{6.22}$$

À partir de la caractérisation de G à l'aide des F_i au travers de l'application Φ_m^{-1}, nous obtenons

$$G = \bigsqcup_{l=0}^{m-2} \left(\bigsqcup_{j=e_0+\cdots+e_{\ell-1}}^{e_0+\cdots+e_\ell-1} (jm + F_\ell) \right). \tag{6.23}$$

Les relations (6.22) et (6.23) impliquent alors

$$\sigma(i) + jm \in G \Leftrightarrow j \leqslant e_0 + \cdots + e_{i-1} - 1,$$

pour tout $j \geqslant 0$ et donc

$$G^{(k)} = G^{(\sigma(i))} = \sigma(i) + m[0, e_0 + \cdots + e_{i-1} - 1].$$

En prenant le complément dans $\mathbb{N}$, nous obtenons :

$$\sigma(i) + jm \in \mathbb{N} \setminus G \Leftrightarrow j \geqslant e_0 + \cdots + e_{i-1},$$

ce qui établit la relation (6.21). □

Déterminons maintenant des conditions nécessaires et suffisantes sur σ et e pour que $F(\sigma, e)$ soit une filtration de gouffre et donc que $S(\sigma, e)$ soit un semigroupe numérique.

Théorème 3.10. *Soient $m \geqslant 3$, $\sigma \in \mathfrak{S}_{m-1}$ et $e = (e_0, \dots, e_{m-2}) \in \mathbb{N}^{m-1}$ avec $e_0 \geqslant 1$. Alors $F(\sigma, e)$ est une filtration de gouffre si et seulement si pour tous $1 \leqslant i, j, k \leqslant m-1$ avec $i \leqslant j < k$, nous avons*

$$e_j + \cdots + e_{k-1} \leqslant \begin{cases} e_0 + \cdots + e_{i-1} & \text{si } \sigma(i) + \sigma(j) = \sigma(k), \\ e_0 + \cdots + e_{i-1} + 1 & \text{si } \sigma(i) + \sigma(j) = \sigma(k) + m. \end{cases}$$

Démonstration. Posons $S_0 = \mathbb{N}$ et $S_i = \sigma(i) + m(e_0 + \cdots + e_{i-1} + \mathbb{N})$ pour $1 \leqslant i \leqslant m-1$. Par le lemme 3.9 nous obtenons

$$S(\sigma, e) = \bigsqcup_{i=0}^{m-1} S_i.$$

L'ensemble $S(\sigma, e)$ contient 0 car $0 \in S_0 \subset S(\sigma, e)$. Le complément de $S(\sigma, e)$ dans $\mathbb{N}$ est $G(\sigma, e)$ qui est fini car obtenu d'une m-filtration. Il reste à montrer que $S(\sigma, e)$ est stable par addition si et seulement si les conditions du théorème sont satisfaites. Soient i et j des entiers vérifiant $0 \leqslant i \leqslant j \leqslant m-1$. Si i est nul alors $S_i + S_j = m\mathbb{N} + S_j = S_j$. Supposons $i \geqslant 1$. Nous avons trois cas à traiter.

Cas $\sigma(i) + \sigma(j) \leqslant m-1$. Il existe alors $k \in [1, m-1]$ satisfaisant $\sigma(k) = \sigma(i) + \sigma(j)$ et nous avons

$$\begin{aligned} S_i + S_j &= \sigma(i) + m(e_0 + \cdots + e_{i-1} + \mathbb{N}) + \sigma(j) + m(e_0 + \cdots + e_{j-1} + \mathbb{N}) \\ &= \sigma(k) + m(e_0 + \cdots + e_{i-1} + e_0 + \cdots + e_{j-1} + \mathbb{N}). \end{aligned}$$

Ainsi $S_i + S_j$ est contenu dans $S(\sigma, e)$ si et seulement s'il est contenu dans S_k. Ce qui, par construction de S_k, est possible si et seulement si

$$e_0 + \cdots + e_{k-1} \leqslant e_0 + \cdots + e_{i-1} + e_0 + \cdots + e_{j-1}.$$

Cette dernière condition est trivialement satisfaite pour $k \leqslant j$ et est équivalente à

$$e_j + \cdots + e_{k-1} \leqslant e_0 + \cdots + e_{i-1}$$

pour $j < k$.

Cas $\sigma(i) + \sigma(j) \leqslant m + 1$**.** Il existe alors $k \in [1, m-1]$ satisfaisant $\sigma(k) + m = \sigma(i) + \sigma(j)$ et donc

$$\begin{aligned} S_i + S_j &= \sigma(i) + m(e_0 + \cdots + e_{i-1} + \mathbb{N}) + \sigma(j) + m(e_0 + \cdots + e_{j-1} + \mathbb{N}) \\ &= \sigma(k) + m(e_0 + \cdots + e_{i-1} + e_0 + \cdots + e_{j-1} + 1 + \mathbb{N}). \end{aligned}$$

Comme précédemment, $S_i + S_j$ est contenu dans $S(\sigma, e)$ si et seulement s'il l'est dans S_k, ce qui est possible si et seulement si

$$e_0 + \cdots + e_{k-1} \leqslant e_0 + \cdots + e_{i-1} + e_0 + \cdots + e_{j-1} + 1.$$

Cette condition est trivialement satisfaite pour $k \leqslant j$ et est équivalente à

$$e_j + \cdots + e_{k-1} \leqslant e_0 + \cdots + e_{i-1}$$

pour $j < k$.

Cas $\sigma(i) + \sigma(j) = m$**.** Nous avons alors $S_i + S_j \subseteq m\mathbb{N} = S_0 \subset S'$. □

Il est possible de passer des e-coordonnées de la filtration d'un semigroupe à celles dites de Kunz utilisées par P.A. García-Sánchez, D. Marín-Aragón et A.M. Robles-Pérez dans [72] pour établir la conjecture 3.2 dans le cas $m \leqslant 5$.

Définition 3.11. Soit S un semigroupe numérique S de multiplicité m. Pour tout entier i de $[0, m-1]$, on note k_i l'unique entier tel que $i + m\,k_i \in \mathrm{Ap}(S)$. Les entiers $k_1, \ldots, k_{m-1}$ sont appelés *coordonnées de Kunz* de S.

Soit $S = S(\sigma, e)$ un semigroupe numérique de multiplicité m. Par (6.21) le plus petit élément de $S(\sigma, e)$ qui soit congru à $\sigma(i)$ modulo m est $\sigma(i) + m(e_0 + \cdots + e_{i-1})$. Nous obtenons ainsi

$$\begin{aligned} k_{\sigma(i)} &= e_0 + \cdots + e_{i-1} \quad \text{pour tout } i \in [1, m-1], \\ e_j &= k_{\sigma(j+1)} - k_{\sigma(j)} \quad \text{pour tout } j \in [0, m-2], \end{aligned}$$

avec la convention $k_{\sigma(0)} = 0$. Les e-coordonnées peuvent ainsi être vues comme une σ-déformation de la dérivée discrète des coordonnées de Kunz.

Comme dans le cas $m = 3$, nous pouvons toujours définir des fonctions d'adjonction d'entiers aux m-filtrations.

Définition 3.12. Soit $F = (F_0, \ldots, F_t)$ une m-filtration et k un entier de $[1, m-1]$. Soit ℓ l'unique entier se $[1, t+1]$ vérifiant $k \in F_{\ell-1} \setminus F_\ell$ (avec la convention $F_{t+1} = \emptyset$). On définit une m-filtration $f^{(k)}(F)$ en posant

$$f^{(k)}(F) = \begin{cases} (F_0, \ldots, F_t, \{k\}) & \text{si } \ell = t+1, \\ (F_0, \ldots, F_\ell \cup \{k\}, \ldots, F_t) & \text{sinon.} \end{cases}$$

Soit $F = F(\sigma, e)$ une m-filtration. Comme en (6.20), nous posons

$$F = \big(\underbrace{H_0, \dots, H_0}_{\mu_0}, \dots, \underbrace{H_j, \dots, H_j}_{\mu_j}, \dots, \underbrace{H_s, \dots, H_s}_{\mu_s}\big)$$

avec $\mu_i \geqslant 1$ et $H_i \subsetneq H_{i-1}$. Par définition de σ, il existe une suite $c_1 < \cdots < c_{s+2}$ telle que

$$H_{i-1} \setminus H_i = \{\sigma(c_i), \sigma(c_i + 1), \dots, \sigma(c_{i+1} - 1)\}$$

pour $i \in [1, s+1]$ avec la convention $H_{s+1} = \emptyset$. Notons j l'unique entier de $[1, s+1]$ tel que $k \in H_{j-1} \setminus H_j$. Pour $j \leqslant s$, nous avons

$$f^{(k)}(F) = \big(\underbrace{H_0, \dots, H_0}_{\mu_0}, \dots, H_j \sqcup \{k\}, \underbrace{H_j, \dots, H_j}_{\mu_j - 1}, \dots, \underbrace{H_s, \dots, H_s}_{\mu_s}\big).$$

La permutation σ^k de $f^{(k)}(F)$ est alors la même que celle de F si et seulement si $\sigma(c_j) = k$. De même dans le cas $j = s+1$. Les permutations de $f^{(k)}(F)$ et $F(\sigma, e)$ ne sont donc pas toujours les mêmes. Cependant la permutation caractérisant $F(\sigma, e)$ n'est pas unique et on peut toujours trouver une permutation $\tau \in \mathfrak{S}_{m-1}$ telle qu'on ait $F = F(\tau, e)$ et que la permutation de $f^{(k)}(F)$ soit aussi τ.

Définition 3.13. Soit $F = F(\sigma, e)$ une m-filtration et $k \in [1, m-1]$. Nous appellons permutation k-*adaptée* de F toute permutation τ telle que $F = F(\tau, e)$ et $f^{(k)}(F) = F(\tau, e')$ pour certaines coordonnées e'.

Par ce qui précède nous savons qu'une filtration quelconque possède toujours une permutation k-adaptée.

3.3 Le cas $m = 4$

Le théorème 3.10 permet d'obtenir le résultat suivant, qui est un analogue du théorème 3.4 au cas $m = 4$.

Corollaire 3.14. *Les filtrations de gouffre de multiplicité* 4 *sont les* 4*-filtrations* $F(\sigma, e)$ *avec* $\sigma \in \mathfrak{S}_3$, $e = (a, b, c) \in \mathbb{N}^3$ *vérifiant* $a \geqslant 1$ *et les conditions suivantes sur* e

$\sigma \in \mathfrak{S}_3$	$F = F(\sigma, e)$	conditions sur $e = (a, b, c)$:
$(1, 2, 3)$	$\{1, 2, 3\}^a \{2, 3\}^b \{3\}^c$	$b \leqslant a,\ c \leqslant a$
$(1, 3, 2)$	$\{1, 2, 3\}^a \{2, 3\}^b \{2\}^c$	$b + c \leqslant a$
$(2, 1, 3)$	$\{1, 2, 3\}^a \{1, 3\}^b \{3\}^c$	$c \leqslant a$
$(2, 3, 1)$	$\{1, 2, 3\}^a \{1, 3\}^b \{1\}^c$	$c \leqslant a + 1$
$(3, 1, 2)$	$\{1, 2, 3\}^a \{1, 2\}^b \{2\}^c$	$b + c \leqslant a + 1$ *et* $c \leqslant a + b$
$(3, 2, 1)$	$\{1, 2, 3\}^a \{1, 2\}^b \{1\}^c$	$b \leqslant a + 1$ *et* $c \leqslant a + 1$

(6.24)

Démonstration. Nous traitons indépendamment chacune des 6 permutations de $\mathfrak{S}_3$. Prenons par exemple $\sigma = (1, 3, 2)$. Nous avons alors $\sigma(1) + \sigma(1) = \sigma(3)$ et $\sigma(2) + \sigma(2) = \sigma(3) + m$. Par le théorème 3.10, les conditions sur $e = (a, b, c)$ pour que $F(\sigma, e)$ soit une filtration de gouffre sont $b + c \leqslant a$ et $c \leqslant a + b + 1$. Comme la dernière condition est conséquence de la première on peut l'ignorer. On obtient finalement que $F(\sigma, e)$ est une filtration de gouffre si et seulement si $b + c \leqslant a$ est vérifiée. □

Soit F une filtration de gouffre de multiplicité m. Comme pour le cas $m = 3$, la démonstration de la conjecture 3.2 dans le cas $m = 4$ reposera sur l'adjonction à F d'un certain entier $i \in [1, m-1]$ de telle sorte que la filtration obtenue soit celle d'un gouffre, et donc respecte les conditions du théorème 3.10.

Corollaire 3.15. *Pour tout $g \geqslant 0$, on a $n_{g+1,4} \geqslant n_{g,4}$.*

Démonstration. Le résultat est immédiat pour $g \leqslant 2$ car dans ce cas nous avons $n_{g,4} = 0$. Supposons maintenant $g \geqslant 3$. Soit F une filtration de gouffre de multiplicité 4 et de genre g. Soient $\sigma^{(1)}$ et $\sigma^{(3)}$ des permutations respectivement 1- et 3-adaptées de F. Nous avons ainsi $F = (\sigma^{(1)}, e) = (\sigma^{(3)}, e)$ avec $e = (a, b, c)$. Notons $F^{(1)}$ et $F^{(3)}$ les m-filtrations $f^{(1)}(F)$ et $f^{(3)}(F)$. La permutation $\sigma^{(1)}$ étant 1-adaptée, on a $F^{(1)} = F(\sigma^{(1)}, e^{(1)})$ avec

$$e^{(1)} = \begin{cases} (a+1, b-1, c) & \text{si } \sigma^{(1)} \in \{(1,2,3),(1,3,2)\}, \\ (a, b+1, c-1) & \text{si } \sigma^{(1)} \in \{(2,1,3),(3,1,2)\}, \\ (a, b, c+1) & \text{si } \sigma^{(1)} \in \{(2,3,1),(3,2,1)\}. \end{cases}$$

Supposons par exemple $\sigma^{(1)} = (1,2,3)$. Comme F est une filtration de gouffre, le corollaire 3.14 garantit $b \leqslant a$ et $c \leqslant a+1$. Toujours par le même corollaire, $F^{(1)}$ est une filtration de gouffre si et seulement si nous avons $b - 1 \leqslant a + 1$ et $c \leqslant a + 1$. Ces deux dernières conditions sont toujours vérifiées et donc $F^{(1)}$ est toujours une filtration de gouffre dans le cas $\sigma^{(1)} = (1,2,3)$. En traitant de la même manière les autres cas, le corollaire 3.14 implique que la 4-filtration $F^{(1)}$ n'est pas une filtration de gouffre si et seulement si $\sigma^{(1)} \in \{(2,3,1),(3,2,1)\}$ et $e = (a, b, a+1)$ et donc si et seulement si F est de la forme

$$\{1,2,3\}^a\{1,3\}^b\{1\}^{a+1} \quad \text{ou} \quad \{1,2,3\}^a\{2,3\}^b\{1\}^{a+1}.$$

Dans les deux cas F est de genre $3a + 2b + a + 1 = 4a + 2b + 1$ qui est impair. Ainsi $F^{(1)}$ est toujours une filtration de gouffre si g est pair. Une étude similaire montre que $F^{(3)}$ n'est pas une filtration de gouffre si et seulement si F est de la forme

$$\{1,2,3\}^a\{1,3\}^b\{3\}^a \quad \text{ou} \quad \{1,2,3\}^a\{2,3\}^b\{3\}^a.$$

Encore une fois, dans les deux cas F est de genre $3a+2b+a = 4a+2b$ qui est pair et donc $F^{(3)}$ est toujours une filtration de gouffre si g est impair. On construit ainsi une injection de $\mathcal{F}(g,4)$ dans $\mathcal{F}(g+1,4)$ en posant

$$\begin{array}{rcl} \mathcal{F}(g,4) & \mapsto & \mathcal{F}(g+1,4) \\ F & \to & \begin{cases} f^{(1)}(F) & \text{si } g \text{ est pair,} \\ f^{(3)}(F) & \text{si } g \text{ est impair.} \end{cases} \end{array}$$

Nous obtenons finalement $n_{g,4} = \operatorname{card}(\mathcal{F}(g,4)) \leqslant \operatorname{card}(\mathcal{F}(g,4)) = n_{g+1,4}$. □

Nous avons montré que pour $m = 3$ et $m = 4$ une injection de $\mathcal{F}(g,4)$ dans l'ensemble $\mathcal{F}(g+1,4)$ peut être obtenue par l'une des fonctions d'adjonction $f^{(i)}$ où le choix de i dépend de g. Malheureusement ceci n'est plus vrai à partir de $m \geqslant 5$ en général. Construire une injection de $\mathcal{F}(g,m)$ dans $\mathcal{F}(g+1,m)$ est toujours un problème ouvert à ce jour.

VII. Triplets pythagoriciens

Dans ce chapitre je présente les résultats que nous avons obtenus dans [54] avec S. Eliahou, V. Marion-Poty et D. Robilliard sur l'existence de coloriages des entiers positifs évitant les triplets pythagoriciens monochromatiques. Nous nous sommes particulièrement intéressés aux coloriages morphiques qui permettent à partir d'un choix de couleurs pour chacun des nombres premiers d'obtenir un coloriage de tous les entiers positifs.

La section 1 est une introduction aux triplets pythagoriciens et à l'état de l'art du sujet. À la section 2 nous définissons les coloriages morphiques et donnons des résultats dans les cas à 2 ou 3 couleurs. La dernière section est consacrée aux coloriages morphiques partiels et à la présentation des résultats expérimentaux que nous avons obtenus avec 2 couleurs.

1 Introduction

Définition 1.1. Un triplet (a, b, c) d'entiers positifs est dit *pythagoricien* s'il satisfait la relation $a^2 + b^2 = c^2$.

Une question typique en théorie de Ramsey est :

Question 1.2. Soit $k \geqslant 2$. Tout coloriage des entiers de $\mathbb{N}_+$ avec k couleurs doit-il nécessairement contenir un triplet pythagoricien monochromatique ?

Bien qu'ouverte depuis 1980 [59], il n'y a pas de consensus sur ce que doit être la réponse [77] à la question 1.2. Il faut attendre 2016 pour que le cas le plus simple avec seulement 2 couleurs obtienne une réponse positive grâce aux travaux de M. J. H. Heule, O. Kullmann et V. W. Marek basés sur des calculs `SAT` massifs [80].

Théorème 1.3 (M. J. H. Heule, O. Kullmann, V. W. Marek [80])**.** *Pour tout coloriage binaire de l'intervalle $I = [1, 7825]$, il existe un triplet pythagoricien monochromatique dans I. De plus* 7825 *est le plus petit entier pour cette propriété.*

Ce résultat a nécessité 35 000 heures de calculs qui ont été validés en générant un certificat au format `DRAT` d'environ `200TB` en un peu plus de 16 000 heures de calcul. Avant cela, J. Cooper et R. Overstreet avaient obtenu en 2013, déjà avec l'aide d'un solveur `SAT`, un coloriage binaire particulier de l'intervalle $[1, 7664]$ évitant les triplets pythagoriciens monochromatiques [23].

Définition 1.4. Un triplet pythagoricien (a, b, c) est *primitif* si les entiers a, b et c sont premiers entre eux.

L'équation $X^2 + Y^2 = Z^2$ étant homogène, tout triplet pythagoricien est un multiple d'un triplet pythagoricien primitif. Le résultat classique suivant de la théorie des nombres permet d'obtenir une paramétrisation simple de tous les triplets pythagoriciens primitifs.

Proposition 1.5. *Tout triplet pythagoricien primitif est de la forme*

$$(m^2 - n^2, 2mn, m^2 + n^2),$$

où m et n sont des entiers positifs, premiers entre eux et tels que $m - n$ soit positif et impair.

En suivant la terminologie introduite par R. Rado en 1933 dans [104] nous introduisons la définition suivante.

Définition 1.6. Soit $k \in \mathbb{N}_+$. Une équation diophantienne $f(X_1, \ldots, X_n) = 0$ est dite *k-régulière* si, pour tout coloriage de $\mathbb{N}_+$ avec k couleurs, il existe une solution monochromatique. Elle est dite *régulière* si elle est k-régulière pour tout $k \in \mathbb{N}_+$.

Remarquons que si une équation diophantienne est k-régulière pour $k \geqslant 2$ alors elle est aussi $(k-1)$-régulière. Avec cette terminologie la question 1.2 revient à déterminer si l'équation diophantienne

$$X^2 + Y^2 - Z^2 = 0 \tag{7.1}$$

est régulière ou non. Et, si non, nous aimerions déterminer le plus grand $k \geqslant 2$ tel qu'elle soit k-régulière. Le seul résultat que nous ayons à ce jour est celui du théorème 1.3 impliquant que l'équation 7.1 est 2-régulière.

L'approche que nous avons développée dans [54] avec S. Eliahou, V. Marion-Poty et D. Robilliard consiste à réduire l'espace des coloriages en ne considérant que des coloriages *morphiques*. Il y a essentiellement trois intérêts à considérer ce type de coloriage. Le premier est qu'il nous permet d'obtenir des résultats pour les coloriages à 3 couleurs. Le second est que pour tout coloriage morphique à 2 couleurs, les triplets pythagoriciens monochromatiques sont inévitables plus rapidement et ceci est établi pour un coût en calcul largement inférieur à celui requis pour le théorème 1.3. Et troisièmement les fonctions partiellement multiplicatives, comme nos coloriages morphiques, semblent être un bon banc d'essai pour le problème à étudier, voir par exemple la récente solution par T. Tao [122] de la conjecture de discrépance de P. Erdős,

Il me semble important de préciser que le théorème 1.3 a été annoncé après que nous ayons effectué nos recherches présentées dans une version préliminaire [1] de [54].

2 Coloriages morphiques

Notation 2.1. Nous notons par $\mathbb{P}$ l'ensemble de tous les entiers premiers.

2.1 Définition

Définition 2.2. Soit $(G, +)$ un groupe abélien. Un *coloriage morphique sur G* est un morphisme de monoïde f de $\mathbb{N}_+$ dans G, c'est-à-dire une application $f : \mathbb{N}_+ \to G$ vérifiant la relation $f(ab) = f(a) + f(b)$.

Remarquons qu'un coloriage morphique f est entièrement et librement déterminé par ses valeurs $\{f(p)\}_{p \in \mathbb{P}}$ sur les nombres premiers.

1. Disponible sur arXiv : `https://arxiv.org/abs/1605.00859v1`

Lemme 2.3. *Soit f un coloriage morphique. Si (a, b, c) est un triplet monochromatique pour f alors ce sera aussi le cas pour tous les triplets (ad, bd, cd) avec $d \in \mathbb{N}_+$.*

Démonstration. Si $f(x) = f(y)$ alors $f(xd) = f(x) + f(d) = f(y) + f(d) = f(yd)$. □

Comme un coloriage morphique sur $\mathbb{Z}/2\mathbb{Z}$ est un coloriage particulier à 2 couleurs, le théorème 1.3 donne immédiatement le résultat suivant.

Corollaire 2.4. *Pour tout coloriage morphique sur $\mathbb{Z}/2\mathbb{Z}$, il existe un triplet pythagoricien qui soit monochromatique.*

Le principal intérêt de considérer un coloriage morphique f est que le lemme 2.3 implique que f admet un triplet pythagoricien monochromatique si et seulement s'il admet un triplet pythagoricien primitif monochromatique. Comme le nombre de triplets pythagoriciens primitifs dans un intervalle donné I est bien inférieur au nombre de triplets pythagoriciens de cet intervalle, nous avons moins de tests à faire pour détecter si un coloriage morphique donné admet un triplet pythagoricien monochromatique ou non.

2.2 Coloriage morphique à 2 couleurs

Proposition 2.5. *Tout coloriage morphique f dans $\mathbb{Z}/2\mathbb{Z}$ admet un triplet pythagoricien monochromatique dans l'intervalle $[1, 533]$ et 533 est minimal pour cette propriété.*

Démonstration. Soit $f\colon \mathbb{N}_+ \to \mathbb{Z}/2\mathbb{Z}$ un coloriage morphique. Alors f est entièrement déterminé par ses valeurs sur les nombres premiers. En effet pour tout $n \in \mathbb{N}_+$, nous avons :

$$f(n) = f\left(\prod_{p\in\mathbb{P}} p^{\nu_p(n)}\right) = \sum_{p\in\mathbb{P}} \nu_p(n) f(p).$$

En fait les seuls premiers p qui contribuent réellement à la valeur de $f(n)$ sont ceux pour qui $\nu_p(n)$ est impair. Par exemple, nous avons $f(12) = f(3)$.

Pour $n \in \mathbb{N}_+$, nous notons supp_impair(n) le *support impair* de n, c'est-à-dire, l'ensemble des premiers p pour lesquels $\nu_p(n)$ est impair. Ainsi la formule de $f(n)$ devient

$$f(n) = \sum_{p\in\text{supp\_impair}(n)} f(p). \tag{7.2}$$

Nous ne nous concentrons que sur les 13 plus petits nombres premiers, notés $p_1, \ldots, p_{13}$ dans l'ordre croissant. Leur ensemble est $\mathbb{P}_{13} = \{2, 3, \ldots, 37, 41\}$. De plus, nous posons

$$\mathbb{N}_{|\mathbb{P}_{13}} = \{n \in \mathbb{N}_+ \mid \text{supp\_impair}(n) \subseteq \mathbb{P}_{13}\}.$$

Par la formule (7.2), la valeur de $f(n)$ pour tout entier $n \in \mathbb{N}_{|\mathbb{P}_{13}}$ est entièrement déterminée par le vecteur binaire de longueur 13

$$v(f) = (f(p_1), \ldots, f(p_{13})) \in (\mathbb{Z}/2\mathbb{Z})^{13}.$$

Considérons maintenant l'ensemble $\mathcal{T}$ de tous les triplets pythagoriciens primitifs de l'intervalle $[1, 532]$. Il y en a exactement 84, le plus grand pour l'ordre lexicographique étant $\{279, 440, 521\}$. Parmi eux, nous distinguons le sous-ensemble $\mathcal{T}_{13}$ des triplets pythagoriciens primitifs à valeur dans $\mathbb{N}_{|\mathbb{P}_{13}}$:

$$\mathcal{T}_{13} = \left\{(a, b, c) \in \mathcal{T} \mid a, b, c \in \mathbb{N}_{|\mathbb{P}_{13}}\right\}.$$

L'ensemble $\mathcal{T}_{13}$ contient exactement 32 triplets. À l'aide de l'ordinateur nous trouvons qu'il n'existe que deux morphismes

$$f_1, f_2\colon \mathbb{N}_{|\mathbb{P}_{13}} \to \mathbb{Z}/2\mathbb{Z}$$

sans triplet pythagoricien monochromatique dans $\mathcal{T}_{13}$. Ils sont donnés par les vecteurs binaires de longueur 13 suivants

$$v(f_1) = 0101111101001, \tag{7.3}$$
$$v(f_2) = 0101111111001. \tag{7.4}$$

Remarquons que les vecteurs $v(f_1)$ et $v(f_2)$ ne diffèrent qu'au neuvième bit. Le 85ème triplet pythagoricien de $[1, 532]$ est $(308, 435, 533)$. Les factorisations en facteurs premiers de $308, 435$ et 533 font seulement intervenir les premiers

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7,$$
$$p_5 = 11, \quad p_6 = 13, \quad p_{10} = 29, \quad p_{13} = 41,$$

et nous avons : $308 = p_1^2 p_4 p_5$, $435 = p_2 p_3 p_{10}$, $533 = p_6 p_{13}$. Ainsi, pour $f = f_1$ ou f_2, nous obtenons

$$\begin{array}{rclcrcl} f(308) &=& f(p_4) + f(p_5) &=& 1+1 &\equiv& 0 \mod 2, \\ f(435) &=& f(p_2) + f(p_3) + f(p_{10}) &=& 1+0+1 &\equiv& 0 \mod 2, \\ f(533) &=& f(p_6) + f(p_{13}) &=& 1+1 &\equiv& 0 \mod 2. \end{array}$$

Nous concluons que tout coloriage morphique $g\colon \mathbb{N}_+ \to \mathbb{Z}/2\mathbb{Z}$ admet un triplet pythagoricien primitif dans $[1, 533]$ qui est monochromatique.

Le fait que 533 soit minimal pour cette propriété est établi par l'existence de nombreux coloriages morphiques f pour lesquels aucun des 84 triplets pythagoriciens primitifs dans $[1, 532]$ n'est monochromatique. En fait f doit vérifier l'un des deux ensembles de contraintes suivants

$$f(p_i) = \begin{cases} 0 & \text{pour } i = 1, 3, 9, 11, 12, 18, 21, 30, 57, 74, 80, 89, \\ 1 & \text{pour } i = 2, 4, 5, 6, 7, 8, 10, 13, 16, 24, 26, 55, 65, \end{cases}$$

ou

$$f(p_i) = \begin{cases} 0 & \text{pour } i = 1, 3, 11, 12, 18, 21, 25, 30, 59, 74, 89, \\ 1 & \text{pour } i = 2, 4, 5, 6, 7, 8, 9, 24, 26, 55, 65, 70, \end{cases}$$

avec une liberté totale sur tous les autres premiers. Remarquons que dans les deux cas le vecteur $(f(p_1), \ldots, f(p_{13}))$ est soit $v(f_1)$, soit $v(f_2)$, donné en (7.3) et (7.4) respectivement. □

2.3 Coloriage morphique à 3 couleurs

Proposition 2.6. *Pour tout coloriage morphique $f\colon \mathbb{N}_+ \to \mathbb{Z}/3\mathbb{Z}$, les triplets pythagoriciens monochromatiques sont inévitables. Plus précisément, au moins un tel triplet dans l'intervalle $[1, 4633]$ est monochromatique pour f. De plus 4633 est minimal pour cette propriété.*

Démonstration. À l'aide d'une exploration informatique nous obtenons qu'il existe un seul coloriage morphique $f\colon \mathbb{N}_+ \to \mathbb{Z}/3\mathbb{Z}$ sans triplet pythagoricien monochromatique dans l'intervalle $[1, 4632]$. Pour le décrire, il est suffisant de spécifier les premiers de cet intervalle qui sont coloriés avec 1 ou 2, les autres étant coloriés avec 0. En notant p_i le $i$ème nombre premier pour $i \geq 1$, nous posons

$$f(p_i) = \begin{cases} 1 & \text{si } i \in A, \\ 2 & \text{si } i \in \{6, 7, 23, 24, 29, 30, 33, 74\}, \\ 0 & \text{sinon,} \end{cases}$$

où l'ensemble A est donné par

$$A = \{1, 2, 5, 11, 12, 13, 16, 17, 19, 20, 21, 25, 37, 45, 55, 65, 68, 70, 71, 82, 84, 89, 98, 112, 123, 130, 135,$$
$$151, 189, 198, 203, 220, 245, 267, 345, 355, 359, 381, 401, 443, 464, 514, 561, 583, 610, 612, 624\}.$$

Le triplet $(4615, 408, 4633)$ est pythagoricien. Comme nous avons

$$\begin{array}{rclcrcrcl} f(4615) &=& f(5 \times 13 \times 71) &=& f(p_3) + f(p_6) + f(p_{20}) &=& 0+2+1 &\equiv& 0 \mod 3, \\ f(408) &=& f(2^3 \times 3 \times 17) &=& 3f(p_1) + f(p_2) + f(p_7) &=& 3 \times 1 + 1 + 2 &\equiv& 0 \mod 3, \\ f(4633) &=& f(41 \times 113) &=& f(p_{13}) + f(p_{30}) &=& 1+2 &\equiv& 0 \mod 3, \end{array}$$

il est monochromatique pour f. Il n'existe donc pas de coloriage morphique dans $\mathbb{Z}/3\mathbb{Z}$ de $[1, 4633]$ évitant les triplets monochromatiques. □

Les propositions 2.5 et 2.6 suggèrent fortement que la question de l'existence de coloriages morphiques à valeurs dans $\mathbb{Z}/m\mathbb{Z}$ et évitant les triplets pythagoriciens monochromatiques, semble plus abordable que le problème général de la m-régularité de l'équation $X^2 + Y^2 - Z^2 = 0$.

Problème 2.7. Est-il vrai que pour $m \geq 4$ et tout coloriage morphique $f : \mathbb{N}_+ \to \mathbb{Z}/m\mathbb{Z}$, les triplets pythagoriciens monochromatiques sont inévitables ? Et si oui, comment le seuil d'inévitabilité se comporte-t-il en fonction de m ?

Pour $m = 2$ et 3 les seuils d'inévitabilité correspondant sont 533 et 4633, respectivement.

3 Coloriages morphiques partiels

Dans cette section nous considérons des versions moins contraignantes que les coloriages morphiques.

3.1 Définition

Définition 3.1. Pour tout entier positif n, le *support de* n, noté $\mathrm{supp}(n)$, est l'ensemble des nombres premiers qui divisent n.

Notation 3.2. Soit $\mathbb{P}_0 \subseteq \mathbb{P}$ un sous-ensemble des nombres premiers. Pour tout $n \in \mathbb{N}_+$, on note $n_{\mathbb{P}_0}$ le plus grand diviseur de n à support dans $\mathbb{P}_0$. L'entier $n/n_{\mathbb{P}_0}$ est alors noté $n_{\overline{\mathbb{P}_0}}$.

Exemple 3.3. Pour $n = 60$ et $\mathbb{P}_0 = \{2, 3, 7\}$, nous avons $\mathrm{supp}(60) = \{2, 3, 5\}$, $n_{\mathbb{P}_0} = 12$ et $n_{\overline{\mathbb{P}_0}} = 5$.

Définition 3.4. Soient $(G, +)$ un groupe abélien et $\mathbb{P}_0 \subset \mathbb{P}$ un sous-ensemble des nombres premiers. Nous disons qu'une application $f : \mathbb{N}_+ \to G$ est un $\mathbb{P}_0$-*coloriage sur* G si les propriétés suivantes sont satisfaites pour tout entier $n \in \mathbb{N}_+$:

— $f(n) = f(n_{\mathbb{P}_0}) + f(n_{\overline{\mathbb{P}_0}})$;

— $f(n_{\overline{\mathbb{P}_0}}) = f(a) + f(b)$ pour tous entiers a et b premiers entre eux vérifiant $ab = n_{\overline{\mathbb{P}_0}}$.

De manière équivalente nous pouvons décrire un $\mathbb{P}_0$-coloriage morphique partiel sur G de la façon suivante. Pour tout $n \in \mathbb{N}_+$ considérons l'unique factorisation en facteurs premiers

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

où $\nu_p(n) \in \mathbb{N}$ pour tout premier p. L'application $f : \mathbb{N}_+ \to G$ est un $\mathbb{P}_0$-coloriage morphique sur G si pour tout $n \in \mathbb{N}_+$, nous avons

$$f(n) = f\left(\prod_{p \in \mathbb{P}_0} p^{\nu_p(n)}\right) + \sum_{p \notin \mathbb{P}_0} f\left(p^{\nu_p(n)}\right).$$

Ainsi un $\mathbb{P}_0$-coloriage morphique est entièrement et librement déterminé par ses valeurs sur l'ensemble des entiers

$$S(\mathbb{P}_0) = \{n_0 \in \mathbb{N}_+ \mid \mathrm{supp}(n_0) \subseteq \mathbb{P}_0\} \bigsqcup \{p^\nu \mid p \in \mathbb{P} \setminus \mathbb{P}_0, \nu \in \mathbb{N}_+\}. \tag{7.5}$$

Par exemple un $\{2,3\}$-coloriage morphique est entièrement déterminé par sa valeur sur les entiers 2^a3^b et p^c avec $p \in \mathbb{P}$, $p \geqslant 4$ et où $a, b, c \in \mathbb{N}$, $a + b \geqslant 1$ et $c \geqslant 1$.

Remarque 3.5. Les $\mathbb{P}$-coloriages morphiques sur G sont tous les coloriages ensemblistes à valeurs dans G. Plus généralement, si nous avons $\mathbb{P}_0 \subseteq \mathbb{P}_1 \subseteq \mathbb{P}$ alors tout $\mathbb{P}_0$-coloriage morphique est un $\mathbb{P}_1$-coloriage morphique.

3.2 Cas des $\emptyset$-coloriages morphiques

Un $\emptyset$-coloriage morphique dans G est une application $f : \mathbb{N}_+ \to G$ vérifiant $f(xy) = f(x) + f(y)$ pour tout entier x et y de $\mathbb{N}_+$ premiers entre eux. Les coloriages morphiques sont ainsi une sous-famille des $\emptyset$-coloriages morphiques.

Lemme 3.6. *Soit $(G, +)$ un groupe abélien avec au moins 2 éléments. Il existe des $\emptyset$-coloriages morphiques $f\colon \mathbb{N}_+ \to G$ pour lesquels il n'existe pas de triplet pythagoricien primitif monochromatique.*

Démonstration. Considérons l'application f_2 de $\mathbb{N}_+$ dans G définie par

$$f_2(n) = \begin{cases} g & \text{si } n \text{ est pair,} \\ 0 & \text{sinon,} \end{cases}$$

où g est un élément non nul de G. Nous vérifions immédiatement que nous avons $f_2(xy) = f_2(x) + f_2(y)$ si x et y sont premiers entre eux. Comme tout triplet pythagoricien primitif (a, b, c) contient exactement un nombre pair, il ne peut pas être monochromatique pour f_2.

□

La situation est donc vraiment différente du cas des coloriages morphiques où le lemme 2.3 implique que l'existence de triplets pythagoriciens monochromatiques primitifs est équivalente à l'existence de triplets pythagoriciens monochromatiques.

3.3 Un algorithme

Par le théorème 1.3 nous savons qu'aucun $\mathbb{P}_0$-coloriage morphique à valeurs sur $\mathbb{Z}/2\mathbb{Z}$ ne peut éviter les triplets pythagoriciens monochromatiques.

Notation 3.7. Pour tout $\mathbb{P}_0 \subseteq \mathbb{P}$ on note $N(\mathbb{P}_0)$ le plus grand entier tel qu'il existe un $\mathbb{P}_0$-coloriage morphique sur $\mathbb{Z}/2\mathbb{Z}$ évitant les triplets pythagoriciens monochromatiques dans $[1, N(\mathbb{P}_0)]$.

Décrivons maintenant le fonctionnement de l'algorithme qui nous a permis de déterminer certaines valeurs de $N(\mathbb{P}_0)$. Fixons un sous-ensemble $\mathbb{P}_0$ de $\mathbb{P}$. Un $\mathbb{P}_0$-coloriage à valeurs dans $\mathbb{Z}/2\mathbb{Z}$ est alors entièrement déterminé par les couleurs qu'il donne aux éléments de l'ensemble $S(\mathbb{P}_0)$ donné en (7.5). Pour $n \in \mathbb{N}_+$, nous posons $\text{fact}(n) = \{q_1, \ldots, q_k\}$ l'unique ensemble de $S(\mathbb{P}_0)$ tel que nous ayons

$$n = \prod_{i=1}^{k} q_i$$

et où chaque $q_i \in S(\mathbb{P}_0)$ est *maximal*, dans le sens qu'aucun multiple propre de q_i divisant n appartient à $S(\mathbb{P}_0)$. Ainsi pour un $\mathbb{P}_0$-coloriage morphique f sur $\mathbb{Z}/2\mathbb{Z}$, et pour tout

$n \in \mathbb{N}_+$, nous avons

$$f(n) = \sum_{q \in \mathrm{fact}(n)} f(q).$$

Par exemple, si $\mathbb{P}_0 = \{2,3,5\}$ et $n = 64680 = 2^3 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11$, les $S(\mathbb{P}_0)$-facteurs de n sont $120 = 2^3 \cdot 3 \cdot 5$, $49 = 7^2$ et 11. Ainsi $\mathrm{fact}(n) = \{120, 49, 11\}$, et $f(n) = f(120) + f(49) + f(11)$ pour tout $\mathbb{P}_0$-coloriage morphique f sur $\mathbb{Z}/2\mathbb{Z}$.

L'algorithme essaye alors d'assigner une couleur de $\mathbb{Z}/2\mathbb{Z}$ à chacune des variables non déjà coloriées. L'ordre dans lequel les affectations de couleurs sont faites est important et peut fortement affecter le temps d'exécution.

Afin de définir un ordre d'assignation des variables nous introduisons les notations suivantes. Étant donné un entier positif M, nous notons $\mathcal{T}_M$ l'ensemble des triplets pythagoriciens contenus dans l'intervalle $[1, M]$. Alors, pour $q \in S(\mathbb{P}_0)$ et $\{a,b,c\} \in \mathcal{T}_M$, nous posons

$$\delta_q^{\{a,b,c\}} = \begin{cases} 1 & \text{si } q \in \mathrm{fact}(a) \cup \mathrm{fact}(b) \cup \mathrm{fact}(c), \\ 0 & \text{sinon.} \end{cases}$$

Le *poids* de la variable q est alors défini par

$$w(q) = \sum_{t \in \mathcal{T}_M} \delta_q^t,$$

ce qui correspond au nombre de triplets de $\mathcal{T}_M$ où q apparaît dans au moins un ensemble fact(..) de l'un des termes du triplet. L'algorithme assigne alors une couleur de $\mathbb{Z}/2\mathbb{Z}$ à chacune des variables par poids décroissant. Ainsi les variables apparaissant dans le plus grand nombre de triplets de $\mathcal{T}_M$ sont traitées en premières. Une fois qu'une variable est coloriée, l'algorithme essaie de calculer, si possible, la couleur des entiers apparaissant dans les triplets de $\mathcal{T}_M$. Si un triplet de $\mathcal{T}_M$ est monochromatique, nous essayons une autre couleur, si possible, sinon l'algorithme fait un *backtrack*.

3.4 Résultats

Nous avons tout d'abord commencé à déterminer $N(\mathbb{P}_0)$ lorsque $\mathbb{P}_0$ est composé des plus petits premiers de $\mathbb{P}$.

Proposition 3.8. *Nous avons*

$$N(\{2,3,5\}) = 532,$$
$$N(\{2,3,5,7\}) = 564,$$
$$N(\{2,3,5,7,11\}) = 695.$$

Nous avons aussi considéré les $\mathbb{P}_0$-coloriages morphiques lorsque $\mathbb{P}_0$ est n'importe quel sous-ensemble de $\mathbb{P} \cap [1,100]$ de cardinal 3, 4 ou 5, sachant que l'ensemble $[1,100]$ contient exactement 25 premiers.

Il existe $\binom{25}{3} = 2\,300$ ensembles composés de 3 premiers distincts inférieurs à 100.

Proposition 3.9. *Tous les sous-ensembles $\mathbb{P}_0$ de $\mathbb{P} \cap [1,100]$ de cardinal 3 vérifient $N(\mathbb{P}_0) = 532$ sauf pour 29 exceptions :*

$$N(\mathbb{P}_0) = \begin{cases} 544 & \textit{si } \mathbb{P}_0 \in \big\{\{2,3,13\},\{3,5,17\},\{5,13,41\}\big\}, \\ 564 & \textit{si } \mathbb{P}_0 \in \big\{\{2,3,7\}\big\} \cup \big\{\{7,11,a\} \mid a \in \mathbb{P} \cap [2,100] \setminus \{7,11\}\big\}, \\ 628 & \textit{si } \mathbb{P}_0 \in \big\{\{2,3,19\},\{3,13,19\}\big\}. \end{cases}$$

Il existe $\binom{25}{4} = 12\,650$ ensembles composés de quatre premiers distincts inférieurs à 100.

Proposition 3.10. *Tous les sous-ensembles* $\mathbb{P}_0 \subset \mathbb{P} \cap [1, 100]$ *de cardinal* 4 *vérifient*

$$532 \leqslant N(\mathbb{P}_0) \leqslant 784$$

et, plus précisément,

$$N(\mathbb{P}_0) \in \{532, 543, 544, 547, 564, 577, 594, 614, 624, 628, \\ 649, 656, 662, 666, 679, 688, 696, 739, 778, 784\}.$$

Il existe $\binom{25}{5} = 53\,130$ ensembles composés de cinq premiers distincts inférieurs à 100.

Proposition 3.11. *Tous les sous-ensembles* $\mathbb{P}_0 \subset \mathbb{P} \cap [1, 100]$ *de cardinal* 5 *vérifient*

$$532 \leq N(\mathbb{P}_0) \leq 900.$$

De plus, les seuls sous-ensembles $\mathbb{P}_0$ *atteignant la valeur maximale* $N(\mathbb{P}_0) = 900$ *sont*

$$\{2, 3, 7, 19, 23\}, \ \{2, 3, 17, 19, 23\}.$$

Les résultats précédents peuvent être résumés de la manière suivante.

Proposition 3.12. *Pour tout sous-ensemble* $\mathbb{P}_0 \subseteq \mathbb{P} \cap [1, 100]$ *de cardinal au plus* 5 *et pour tout* $\mathbb{P}_0$*-coloriage morphique* f *sur* $\mathbb{Z}/2\mathbb{Z}$*, l'intervalle* $[1, 901]$ *contient nécessairement des triplets pythagoriciens monochromatiques.*

Le cas des sous-ensembles $\mathbb{P}_0 \subseteq \mathbb{P} \cap [1, 100]$ de cardinal 6 n'a pas pu être entièrement traité à ce jour.

VIII. Nombres de Schur faibles

Dans ce chapitre nous décrivons comment avec S. Eliahou, C. Fonlupt, V. Marion-Poty, D. Robilliard et F. Teytaud nous avons obtenu en 2013 la meilleure borne inférieure connue à ce jour pour le sixième nombre de Schur faible à l'aide d'exploration arborescente de Monte-Carlo [49].

La première section est une introduction aux nombres de Schur. À la section 2 nous décrivons la méthode d'exploration de Monte-Carlo que nous avons utilisée. La dernière section décrit les résultats expérimentaux obtenus ainsi que les heuristiques que nous avons dû ajouter.

1 Nombres de Schur et nombres de Schur faibles

Définition 1.1. Un sous-ensemble P de $\mathbb{N}_+$ est dit

- *libre de somme* si pour tous x, y éléments de P, la somme $x + y$ n'est pas dans P.
- *faiblement libre de somme* si pour tous x, y éléments distincts de P, la somme $x + y$ n'est pas dans P.

Par exemple l'ensemble $\{1, 2, 5, 8\}$ est faiblement libre de somme mais pas libre de somme car il contient 1 et son double 2.

Définition 1.2. Une partition $[1, N] = P_1 \sqcup \cdots \sqcup P_k$ est une *partition de Schur à k couleurs de longueur N* si les ensembles P_i sont libres de somme. Nous définissons de même des partitions de Schur faibles en considérant des parties P_i faiblement libres de somme.

1.1 Nombres de Schur

En 1916 I. Schur montre le résultat suivant sur les partitions de Schur.

Théorème 1.3 (I. Schur [119])**.** *Pour tout entier $k \geqslant 1$, il existe un entier maximal N pour lequel il existe une partition de Schur à k couleurs de longueur N.*

Nous considérons alors la définition suivante.

Définition 1.4. Pour $k \geqslant 1$, le k-ième *nombre de Schur*, noté $\mathrm{S}(k)$, est l'unique entier N donné par le théorème 1.3.

Exemple 1.5. Nous avons $\mathrm{S}(1) = 1$. Pour $k = 2$, la partition $\{\{1, 4\}, \{2, 3\}\}$ est la seule de longueur 4 qui soit de Schur. Comme 5 ne peut pas être ajouté, nous avons $\mathrm{S}(2) = 4$. Il est encore possible à la main d'obtenir $\mathrm{S}(3) = 13$ comme en témoigne la partition

$$\{\ \{1, 4, 10, 13\},\ \{2, 3, 11, 12\},\ \{5, 6, 7, 8, 9\}\ \}.$$

À l'aide de calculs sur ordinateur [76], S. W. Golomb et L. D. Baumert ont établi que le quatrième nombre de Schur est $S(4) = 44$. En 2017, M. J. H. Heule [79] a établi à l'aide de calculs `SAT` massifs que le cinquième nombre de Schur est $S(5) = 160$. Jusqu'à ce résultat, nous avions l'encadrement $160 \leqslant S(5) \leqslant 305$. La borne inférieure avait été établie par G. Exoo en 1994 [60] et la majoration est une conséquence d'une relation établie la même année par S. P. Radziszowski dans [106]. Pour le sixième et le septième nombre de Schur nous avons les bornes inférieures suivantes

$$S(6) \geqslant 536 \qquad S(7) \geqslant 1680,$$

qui ont été établies par H. Fredricksen et M. M. Sweet en 2000 dans [63].

1.2 Nombres de Schur faible

En 1941, R. Rado [105] démontre un équivalent du théorème 1.3 pour les partitions faiblement libres de somme :

Théorème 1.6. *Pour tout entier $k \geqslant 1$, il existe un entier maximal N pour lequel il existe une partition de Schur faible à k couleurs de longueur N.*

Définition 1.7. Pour $k \geqslant 1$, le k-ième *nombre de Schur faible*, noté $WS(k)$ est l'unique entier N donné par le théorème 1.3.

Exemple 1.8. L'ensemble $\{1, 2\}$ étant faiblement libre de somme nous obtenons facilement $WS(1) = 2$. Avec un peu d'effort nous obtenons $WS(2) = 8$, correspondant par exemple à la partition

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

En 1972, F. Blanchard, F. Harary et R. Reis [10] ont utilisé un algorithme de recherche exhaustive pour obtenir $WS(3) = 23$ et $WS(4) = 66$ ainsi que $WS(5) \geqslant 189$. Il est remarquable qu'une note faite par le révérend G. W.Walker [129] annonce $WS(5) = 196$ sans en faire la démonstration ni même fournir une partition en témoignant. Il faut attendre 2011, pour que S. Eliahou, J. M. Marín, P. Revuelta et M. I. Sanz [56] établissent $WS(5) \geqslant 196$ à l'aide d'un solveur `SAT`. Ils établissent aussi la minoration $WS(6) \geqslant 572$. Cette borne inférieure fût poussée à $WS(6) \geqslant 574$ par C. Fonlupt, D. Robilliard, V. Marion-Poty et A. Boumaza en 2012 à l'aide de recherche meta heuristique [112]. Ce résultat a ensuite été amélioré en $WS(6) \geqslant 581$ la même année par R. Le Bras, C. P. Gomes et B. Selman à l'aide d'un solveur de contrainte [11].

Grâce aux travaux de H. Abbott et D. Hanson en 1972 pour la borne inférieure et P. Bornstein en 2002 pour la borne supérieure nous avons l'encadrement général suivant pour $k \geqslant 5$:

$$\frac{44}{89}\, 89^{k/4} \leqslant S(k) \leqslant WS(k) \leqslant \lfloor k!ke \rfloor\,.$$

Pour $k = 5$ et 6 nous obtenons respectivement $WS(5) \leqslant 1630$ et $WS(6) \leqslant 11742$. Les meilleurs minorants connus à ce jour pour $WS(k)$ avec $k = 7, 8, 9$ on été donnés par F. Rafilipojaona en 2015 durant sa thèse [107, 108] :

$$WS(7) \geqslant 1740, \quad WS(8) \geqslant 5201 \quad \text{et} \quad WS(9) \geqslant 15596.$$

1.3 Une corrélation

Une k-partition de Schur faible de $[1, n]$ peut être codée par un mot $w = a_1 a_2 \cdots a_n$ où les lettres a_i sont dans l'alphabet $\{1, \ldots, k\}$ et où $a_i = j$ signifie que l'entier i est dans la partie j de la partition.

Exemple 1.9. Le mot 112134 code la partition $\{\ \{1, 2, 4\},\ \{3\},\ \{5\},\ \{6\}\ \}$ tandis que le mot 221243 code pour la partition $\{\ \{3\},\ \{1, 2, 4\},\ \{6\},\ \{5\}\ \}$.

Les deux partitions de l'exemple précédent sont les mêmes à renumérotation des parties près. Afin d'éviter qu'une même partition ne soit codée par deux mots différents nous imposons des contraintes sur le mot d'une partition.

Définition 1.10. Un mot $w = a_1 a_2 \ldots a_n$ est *valide* si pour tout $j \in [2, n]$, nous avons

$$\{a_1, \ldots, a_{j-1}\} = [1, a_j - 1].$$

Dans un mot valide la lettre ℓ peut occuper la position i si et seulement si les lettres $1, \ldots, \ell - 1$ sont dans le préfixe de longueur $i - 1$ de w.

Définition 1.11. Une partition de Schur faible de longueur N est dite *terminale* s'il est impossible d'ajouter l'entier $N + 1$ à l'une de ses parties en obtenant encore une partition de Schur faible.

Il est assez facile de concevoir un algorithme énumérant dans l'ordre lexicographique tous les mots valides de partitions de Schur faibles terminales en k couleurs. Pour $k = 3$, il y a 8 066 partitions terminales de Schur faibles à 3 couleurs. Parmi elles, seulement 3 sont de longueur $\mathrm{WS}(3) = 23$. Nous les avons regroupées par paquets de 100 puis calculé les longueurs moyennes et maximales obtenues sur chacun de ces paquets. La figure 8.1 donne les résultats obtenus.

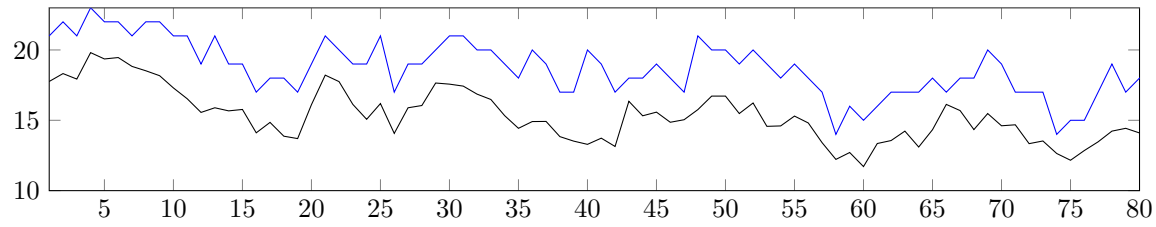


FIGURE 8.1 – Longueur minimale (noir) et longueur maximale (bleu) obtenues sur des paquets de taille 100 pour les partitions de Schur faibles à 3 couleurs enumérées dans l'ordre lexicographique des mots représentatifs.

Les longueurs moyennes et maximales des paquets présentent une corrélation de 0.89. Nous remarquons aussi que les partitions maximales sont très localisées.

Nous avons fait de même pour les partitions de Schur faibles avec 4 couleurs. Il y a 536 994 391 720 partitions terminales de Schur faibles en 4 couleurs et parmi elles 29 931 sont de longueur maximale $\mathrm{WS}(4) = 66$. La figure 8.2 représente les longueurs moyennes et maximales lorsque nous regroupons les partitions par paquets d'un milliard. L'énumération est faite dans l'ordre lexicographique des mots des partitions. Nous obtenons une corrélation de 0.69 entre les longueurs moyennes et maximales.

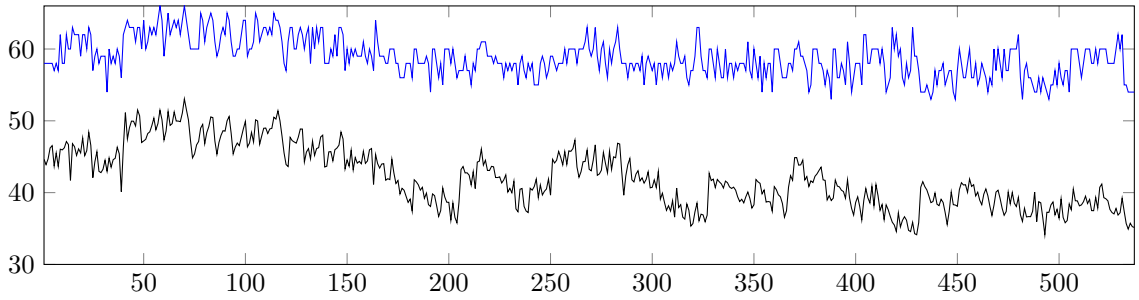


FIGURE 8.2 – Longueur minimale (noir) et longueur maximale (bleu) obtenues sur des paquets de taille un milliard pour les partitions de Schur faibles à 4 couleurs énumérées dans l'ordre lexicographique des mots représentatifs.

Comme pour le cas à 3 couleurs nous constatons que les partitions de longueur maximale sont regroupées dans 2 paquets très proches.

Ces corrélations entre longueurs moyennes et longueurs maximales de paquets de partitions terminales suggèrent que des méthodes d'exploration d'arbre type Monte-Carlo peuvent être efficaces pour déterminer des partitions de Schur faibles de longueur maximale avec un nombre de couleurs fixé.

Remarquons que la corrélation entre longueur moyenne et longueur maximale semble spécifique aux partitions de Schur faibles. Nous avons fait les mêmes calculs pour les partitions de Schur à 4 couleurs. Il y a 92 292 017 partitions terminales et parmi elles 273 sont de longueur maximale $S(4) = 44$. La figure 8.3 donne les longueurs moyennes et maximales obtenues lorsque nous regroupons ces partitions par paquet de un million. Nous obtenons alors une corrélation de -0.17.

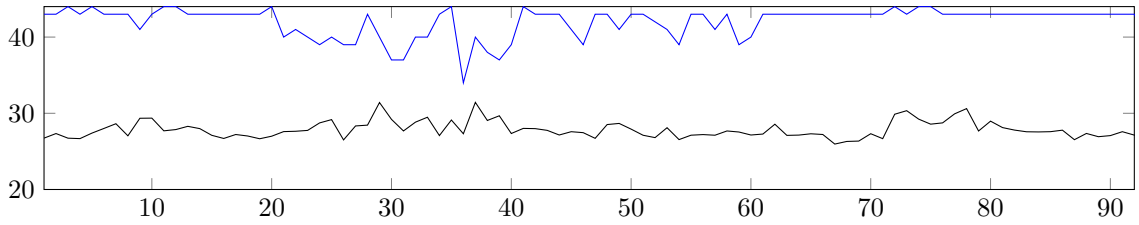


FIGURE 8.3 – Longueur minimale (noir) et longueur maximale (bleu) obtenue sur des paquets de taille un million pour les partitions de Schur à 4 couleurs énumérées dans l'ordre lexicographique des mots représentatifs.

2 Méthode de Monte-Carlo

La méthode d'exploration arborescente *Nested Monte-Carlo* `NMC` [20] a prouvé son efficacité pour résoudre des problèmes contraints, principalement dans le domaine de l'intelligence artificielle (par exemple le sudoku 16x16, le morpion solitaire ou le *SameGame*).

L'exploration d'un arbre de recherche par la méthode de Monte-Carlo consiste à construire progressivement un chemin (ou solution) depuis la racine jusqu'à une feuille de l'arbre. Si un nœud possède plusieurs fils alors l'algorithme choisit l'un de ces fils au hasard et continue la construction jusqu'à atteindre une feuille. Nous attribuons alors un score au chemin ainsi construit.

La méthode `NMC` est une variante multi niveau de la méthode de Monte-Carlo classique. Le but de cette méthode est d'obtenir une solution avec un score élevé. Le `NMC` de niveau 0

correspond à une méthode de Monte-Carlo classique. Pour les niveaux supérieurs $\ell \geqslant 1$ tous les fils d'un nœud sont explorés à l'aide d'un `NMC` de niveau $\ell - 1$; l'algorithme choisit alors le fils ayant obtenu le meilleur score et ainsi de suite jusqu'à ce qu'aucune décision ne puisse plus être prise (correspondant à une feuille de l'arbre de recherche). Le pseudo-code de l'algorithme est donné à l'algorithme 7 où

— `position` décrit l'état de la solution en cours de construction (la position racine est vide, aucune décision n'ayant déjà été prise). Ici, une solution est une partition de Schur faible en k couleurs. Une `position` est toujours passée en argument par copie, et jamais par référence.

— `joue(position, d)` est une fonction qui renvoie la nouvelle position obtenue après avoir exécuté la décision `d` relativement à `position`. Ici une décision consiste à choisir dans quel sous-ensemble de la partition placer le prochain entier. La sélection du prochain entier à placer est déterministe (voir section 3) et ne fait pas partie de la décision.

— `MonteCarlo(position)` est une fonction qui complète une `position` en jouant des décisions aléatoirement, jusqu'à obtenir une solution complète (voir section 2.3). La fonction renvoie un couple : le score obtenu par la solution, ainsi que la séquence des décisions qui ont été prises pour l'obtenir. Comme les entiers ne sont pas toujours joués de manière consécutive, il y a éventuellement des "trous" dans la partition, le score attribué à la solution est alors le plus grand entier L tel que l'intervalle $[1, L]$ soit dans la partition.

Algorithme 7 Méthode de Monte-Carlo `NMC`

```
procedure NMC(position,niveau)
    si niveau=0 alors
        renvoie MonteCarlo(position)
    sinon
        meilleur_score ← −∞
        meilleur_coups ← {}
        tant que la solution n'est pas complète faire
            (score_max,coups_max) ← arg max_d(NMC(joue(position, d), niveau − 1)
            si score_max > meilleur_score alors
                meilleur_score ← score_max
                meilleurs_coups ← coups_max
            fin si
            d ← première décision restante dans meilleurs_coups
            position← joue(position,d)
        fin tant que
        renvoie (meilleur_score, meilleurs_coups)
    fin si
fin procedure
```

L'algorithme `NMC` offre un bon compromis entre *exploration* et *exploitation*. Il est particulièrement efficace pour les jeux à un joueur et donne de bons résultats même sans ajout de connaissances expertes. Cependant, les résultats peuvent être améliorés par l'ajout d'heuristiques [111].

3 Résultats expérimentaux

Une implémentation naturelle de NMC consiste à affecter les entiers dans l'ordre croissant : nous plaçons 1, puis 2, etc. Une autre solution consiste à placer en premier l'un des entiers les plus contraints, c'est-à-dire l'un de ceux ne pouvant être placés que dans le plus petit nombre de parties. Comme l'illustre l'exemple suivant l'avantage de cette méthode est de pouvoir couper prématurément les branches mortes de l'arbre.

Exemple 3.1. Supposons que nous souhaitions compléter la partition $\{\{1,2\},\{3,4\}\}$ faiblement de Schur en une partition de longueur 8 avec 2 couleurs. L'entier 5 peut être placé indifféremment dans l'une des deux parties. De même pour 6 et 8. Par contre l'entier 7 ne peut aller que dans la première partie ; c'est l'entier le plus contraint et c'est donc le prochain à être placé. Nous obtenons ainsi $\{\{1,2,7\},\{3,4\}\}$. Chacun des entiers manquants $5, 6$ et 8 ne peut être placé que dans une seule des deux parties, 5 est le prochain à être placé car c'est le plut petit. On obtient alors $\{\{1,2,7\},\{3,4,5\}\}$. Nous constatons maintenant que l'entier 8 ne peut être placé dans aucune des deux parties. Nous savons alors que la partition $\{\{1,2\},\{3,4\}\}$ ne peut pas être complétée en une partition faiblement de Schur de longueur 8 et ceci avant même d'avoir essayé de placer l'entier 6.

Il a été démontré dans [75, 111] qu'il est souvent possible d'améliorer les performances de NMC en y ajoutant des connaissances spécifiques. Une façon habituelle est de biaiser la probabilité de choix de décision.

3.1 Premières heuristiques

Comme constaté dans [112, 56] toutes les partitions faiblement de Schur avec 4 couleurs et de longueur WS(4) sont des extensions de deux des trois partitions faiblement de Schur avec 3 couleurs et de longueur WS(3). En supposant que cette propriété reste valide pour les partitions faiblement de Schur en k couleurs, nous imposons les couleurs suivantes pour la recherche de partitions faiblement de Schur en 5 couleurs

— $[1,2]$ de couleur 1 ;
— $[3,8]$ de couleur 1 ou 2 ;
— $[9,23]$ de couleur 1, 2 ou 3 ;
— $[24,66]$ de couleur 1, 2, 3 ou 4.

Dans le cas de la recherche d'une partition faiblement de Schur en 6 couleurs nous imposons aussi

— $[67,196]$ de couleur 1, 2, 3, 4 ou 5.

À l'aide de ces hypothèses un appel à NMC de niveau 3 permet de trouver à presque tous les coups une partition faiblement de Schur en 5 couleurs de longueur 196. Pour la longueur 197 l'algorithme n'arrive pas à trouver une partition sans trous, ce qui conforte la conjecture $\mathrm{WS}(5) = 196$.

3.2 Heuristiques supplémentaires

Les hypothèses précédentes ne permettent pas d'obtenir une partition faiblement de Schur de longueur "raisonnable" en 6 couleurs. Nous sommes ainsi amener à ajouter des heuristiques supplémentaires.

Heuristique 1. Les deux partitions faiblement de Schur de longueur 23 en 3 couleurs étendables en des partitions faiblement de Schur en 4 couleurs de longueur 66 sont :

$$\{\,\{1,2,4,8,11,22\},\ \{3,5,6,7,19,21,23\},\ \{9,10,12,13,14,15,16,17,18,20\}\,\}$$
$$\{\,\{1,2,4,8,11,16,22\},\ \{3,5,6,7,19,21,23\},\ \{9,10,12,13,14,15,17,18,20\}\,\}$$

Nous constatons que tous les entiers sont coloriés de la même façon à l'exception de 16 qui peut être de couleur 1 ou 3. Nous choisissons donc de fixer la couleur des 23 premiers entiers à l'exception de 16 et de forcer 16 à être de couleur 1 ou 3.

Heuristique 2. Comme souligné dans [11] les ensembles constituant une partition de longueur maximale contiennent souvent des intervalles de nombres consécutifs. Nous ajoutons une probabilité de 90% qu'un entier soit dans la même partie que son prédécesseur ou son successeur immédiat. Si deux choix de parties sont possibles nous choisissons la plus petite.

Heuristique 3. Dans [56] il est suggéré de construire une partition faiblement de Schur en 6 couleurs telle que les parts 5 et 6 contiennent des suites de la forme

$$\{a\} \cup [a+2, \ldots, 2a+1]$$

où a est le plus élément de la partie considérée. Il semble alors intéressant de placer l'entier $a+1$ dans la première partie. Nous ajoutons une probabilité de 90% de placer un entier de $[a, 2a+1]$ à l'endroit suggéré par l'heuristique lorsque a est le plus petit élément de la partie 5 ou de la partie 6.

3.3 Résultat pour 6 couleurs

À l'aide de l'algorithme `NMC` muni des heuristiques de la sous-section précédente nous avons réussi à obtenir une partition faiblement de Schur avec 6 couleurs de longueur 582 :

$$\begin{array}{l}
\{\\
\quad \{\,[1,2],4,8,11,22,25,53,63,68,136,149,154,159,177,182,187,192,197,394,407,412,435,440,450,455,\\
\quad\quad 471,500,521,526,536,541,555,564,569,582\,\}\\
\quad \{\,3,[5,7],19,21,23,[50,52],[64,66],[137,139],[150,152],165,[179,181],[193,195],[395,397],[408,410],\\
\quad\quad [422,424],[437,439],[451,453],[465,466],[479,481],493,495,497,[509,510],[523,525],[537,539],\\
\quad\quad [552,554],[566,568],[579,581]\,\}\\
\quad \{\,[9,10],[12,18],20,[54,62],[140,148],[183,186],[188,191],[398,406],[441,449],[485,492],[527,535],\\
\quad\quad [570,578]\,\}\\
\quad \{\,24,[26,49],153,[155,158],[160,164],[166,176],178,411,[413,421],[425,434],436,540,[542,551],\\
\quad\quad [556,563],565\,\}\\
\quad \{\,67,[69,135],454,[456,464],[467,470],[472,478],[482,484],494,496,[498,499],[501,508],[511,520],522\,\}\\
\quad \{\,196,[198,393]\,\}\\
\}.
\end{array}$$

À ce jour nous n'avons pas réussi à améliorer ce résultat ni à améliorer la borne $WS(7) \geqslant 1740$ établie par F. Rafilipojaona [107, 108].

Index

Références bibliographiques

[1] Albenque, M., and Nadeau, P. Growth function for a class of monoids. In *21st International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2009)*. Assoc. Discrete Math. Theor. Comput. Sci., Nancy, 2009, pp. 25–38.

[2] Artin, E. Theorie der Zöpfe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 4*, 1 (1925), 47–72.

[3] Artin, E. Theory of braids. *Annals of Mathematics 48* (1947), 101–126.

[4] Bessis, D. The dual braid monoid. *Annales Scientifiques de l'École Normale Supérieure 36*, 5 (2003), 647–683.

[5] Biane, P., and Dehornoy, P. Dual Garside structure of braids and free cumulants of products. *Séminaire Lotharingien de Combinatoire 72* (2014), 15pp.

[6] Bigelow, S. J. Braid groups are linear. *Journal of the American Mathematical Society 14*, 2 (2001), 471–486.

[7] Biggs, N. *Algebraic Graph Theory*. Cambridge University Press, London, 1974.

[8] Birman, J., Ko, K. H., and Lee, S. J. A New Approach to the Word and Conjugacy Problems in the Braid Groups. *Advances in Mathematics 139*, 2 (1998), 322–353.

[9] Björner, A., and Brenti, F. *Combinatorics of Coxeter Groups*. No. 231 in Graduate Texts in Mathematics. Springer, New York, 2005.

[10] Blanchard, P. F., Harary, F., and Reis, R. Partitions into sum-free sets. *Integers. Electronic Journal of Combinatorial Number Theory 6* (2006), A7, 10.

[11] Bras, R. L., Gomes, C., and Selman, B. From Streamlined Combinatorial Search to Efficient Constructive Procedures. In *Twenty-Sixth AAAI Conference on Artificial Intelligence* (2012).

[12] Bras-Amorós, M. Addition behavior of a numerical semigroup. In *Arithmetic, Geometry and Coding Theory (AGCT 2003)*, vol. 11 of *Sémin. Congr.* Soc. Math. France, Paris, 2005, pp. 21–28.

[13] Bras-Amorós, M. Fibonacci-like behavior of the number of numerical semigroups of a given genus. *Semigroup Forum 76*, 2 (2008), 379–384.

[14] Bras-Amorós, M. Bounds on the number of numerical semigroups of a given genus. *Journal of Pure and Applied Algebra 213*, 6 (2009), 997–1001.

[15] Brieskorn, E., and Saito, K. Artin-Gruppen und Coxeter-Gruppen. *Inventiones Mathematicae 17*, 4 (1972), 245–271.

[16] Bronfman, A. Growth functions of a class of monoids. preprint, 2001.

[17] Broué, M., Malle, G., and Rouquier, R. Complex reflection groups, braid groups, Hecke algebras. *Journal für die Reine und Angewandte Mathematik 500* (1998), 127–190.

[18] Burckel, S. The wellordering on positive braids. *Journal of Pure and Applied Algebra 120*, 1 (1997), 1–17.

[19] Campbell, C. M., Robertson, E. F., Ruškuc, N., and Thomas, R. M. Automatic semigroups. *Theoretical Computer Science 250*, 1-2 (2001), 365–391.

[20] Cazenave, T. Nested Monte-Carlo Search. In *IJCAI 2009, Proceedings of the 21st International Joint Conference on Artificial Intelligence, Pasadena, California, USA, July 11-17, 2009* (2009), pp. 456–461.

[21] Charney, R. Artin groups of finite type are biautomatic. *Mathematische Annalen 292*, 4 (1992), 671–683.

[22] Charney, R. Geodesic automation and growth functions for Artin groups of finite type. *Mathematische Annalen 301*, 2 (1995), 307–324.

[23] Cooper, J., Filaseta, M., Harrington, J., and White, D. On colorings of Pythagorean triples within colorings of the positive integers. *Journal of Combinatorics and Number Theory 6*, 1 (2014), 1–16.

[24] Coxeter, H. S. M. The Complete Enumeration of Finite Groups of the Form $r_i^2 = (r_i r_j)^{k_{ij}} = 1$. *Journal of the London Mathematical Society s1-10*, 1 (1935), 21–25.

[25] Curtis, F. On formulas for the Frobenius number of a numerical semigroup. *Mathematica Scandinavica 67*, 2 (1990), 190–192.

[26] Dehornoy, P. Braid groups and left distributive operations. *Transactions of the American Mathematical Society 345*, 1 (1994), 115–150.

[27] Dehornoy, P. A Fast Method for Comparing Braids. *Advances in Mathematics 125*, 2 (1997), 200–235.

[28] Dehornoy, P. Groups with a complemented presentation. *Journal of Pure and Applied Algebra 116*, 1-3 (1997), 115–137.

[29] Dehornoy, P. Groupes de Garside. *Annales Scientifiques de l'École Normale Supérieure 35*, 2 (2002), 267–306.

[30] Dehornoy, P. Combinatorics of normal sequences of braids. *Journal of Combinatorial Theory. Series A 114*, 3 (2007), 389–409.

[31] Dehornoy, P. Alternating normal forms for braids and locally Garside monoids. *Journal of Pure and Applied Algebra 212*, 11 (2008), 2413–2439.

[32] Dehornoy, P. Multifraction reduction I : The 3-Ore case and Artin-Tits groups of type FC. *Journal of Combinatorial Algebra 1*, 2 (2017), 185–228.

[33] Dehornoy, P. Multifraction reduction II : Conjectures for Artin-Tits groups. *Journal of Combinatorial Algebra 1*, 3 (2017), 229–287.

[34] Dehornoy, P. *Le calcul des tresses*. Nano. Calvage et Mounet, 2019.

[35] Dehornoy, P., Digne, F., Godelle, E., Krammer, D., and Michel, J. *Foundations of Garside Theory*. European Mathematical Society Publishing House, Zuerich, Switzerland, 2015.

[36] Dehornoy, P., Dyer, M., and Hohlweg, C. Garside families in Artin–Tits monoids and low elements in Coxeter groups. *Comptes Rendus Mathématique. Académie des Sciences. Paris 353*, 5 (2015), 403–408.

[37] Dehornoy, P., Dynnikov, I., Rolfsen, D., and Wiest, B. *Ordering Braids*, vol. 148 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.

[38] Dehornoy, P., Holt, D. F., and Rees, S. Multifraction reduction IV : Padding and Artin–Tits monoids of sufficiently large type. *Journal of Pure and Applied Algebra 222*, 12 (2018), 4082–4098.

[39] Dehornoy, P., and Paris, L. Gaussian Groups and Garside Groups, Two Generalisations of Artin Groups. *Proceedings of the London Mathematical Society 79*, 3 (1999), 569–604.

[40] Delgado, M. Numbers. https ://cmup.fc.up.pt/cmup/mdelgado/numbers/.

[41] Delgado, M. On a question of Eliahou and a conjecture of Wilf. *Mathematische Zeitschrift 288* (2016), 595–627.

[42] Delgado, M. Trimming the numerical semigroups tree to probe Wilf' sconjecture to higher genus, 2019. En préparation.

[43] Delgado, M., Garcia-Sanchez, P. A., and Morais, J. NumericalSgps, A package for numerical semigroups, Version 1.2.0. https ://gap-packages.github.io/numericalsgps, 2019. Refereed GAP package.

[44] Deligne, P. Les immeubles des groupes de tresses généralisés. *Inventiones Mathematicae 17* (1972), 273–302.

[45] Dobbs, D. E., and Matthews, G. L. On a question of Wilf concerning numerical semigroups. In *Focus on Commutative Rings Research*. Nova Sci. Publ., New York, 2006, pp. 193–202.

[46] Duchamp, G., Hivert, F., and Thibon, J.-Y. Noncommutative symmetric functions. VI. Free quasi-symmetric functions and related algebras. *International Journal of Algebra and Computation 12*, 5 (2002), 671–717.

[47] Eliahou, S. Wilf's conjecture and Macaulay's theorem. *Journal of the European Mathematical Society 20*, 9 (2018), 2105–2129.

[48] Eliahou, S. A graph-theoretic approach to Wilf's conjecture. *arXiv :1909.03699* (Sept. 2019).

[49] Eliahou, S., Fonlupt, C., Fromentin, J., Marion-Poty, V., Robilliard, D., and Teytaud, F. Investigating Monte-Carlo methods on the weak Schur problem. In *Evolutionary Computation in Combinatorial Optimization*, vol. 7832 of *Lecture Notes in Comput. Sci.* Springer, Heidelberg, 2013, pp. 191–201.

[50] Eliahou, S., and Fromentin, J. A remarkable 20-crossing tangle. *Journal of Knot Theory and its Ramifications 26*, 14 (2017), 1750091, 12.

[51] Eliahou, S., and Fromentin, J. Gapsets of small multiplicity. In *International Meeting on Numerical Semigroups - Cortona 2018*, INdAM Meeting. Springer, 2019. To appear.

[52] Eliahou, S., and Fromentin, J. Near-misses in Wilf's conjecture. *Semigroup Forum 98*, 2 (2019), 285–298.

[53] Eliahou, S., and Fromentin, J. Gapsets and numerical semigroups. *Journal of Combinatorial Theory, Series A 169* (2020).

[54] Eliahou, S., Fromentin, J., Marion-Poty, V., and Robilliard, D. Are monochromatic Pythagorean triples unavoidable under morphic colorings ? *Experimental Mathematics 27*, 4 (2018), 419–425.

[55] Eliahou, S., Kauffman, L. H., and Thistlethwaite, M. B. Infinite families of links with trivial Jones polynomial. *Topology 42*, 1 (2003), 155–169.

[56] Eliahou, S., Marín, J. M., Revuelta, M. P., and Sanz, M. I. Weak Schur numbers and the search for G. W. Walker's lost partitions. *Computers & Mathematics with Applications 63*, 1 (2012), 175–182.

[57] Elizalde, S. Improved bounds on the number of numerical semigroups of a given genus. *Journal of Pure and Applied Algebra 214*, 10 (2010), 1862–1873.

[58] Epstein, D. B. A., Cannon, J. W., Holt, D. F., Levy, S. V. F., Paterson, M. S., and Thurston, W. P. *Word Processing in Groups*. Jones and Bartlett Publishers, Boston, MA, 1992.

[59] Erdős, P., and Graham, R. L. *Old and New Problems and Results in Combinatorial Number Theory*, vol. 28 of *Monographies de L'Enseignement Mathématique*. Université de Genève, L'Enseignement Mathématique, Geneva, 1980.

[60] Exoo, G. A lower bound for Schur numbers and multicolor Ramsey numbers of k_3. *Electronic Journal of Combinatorics 1* (1994), Research Paper 8, approx. 3.

[61] Foissy, L. Algèbres de Hopf combinatoires. http ://loic.foissy.free.fr/pageperso/Hopf.pdf.

[62] Foissy, L., and Fromentin, J. A divisibility result in combinatorics of generalized braids. *Journal of Combinatorial Theory. Series A 152* (2017), 190–224.

[63] Fredricksen, H., and Sweet, M. M. Symmetric sum-free partitions and lower bounds for Schur numbers. *Electronic Journal of Combinatorics 7* (2000), Research Paper 32, 9.

[64] Fröberg, R., Gottlieb, C., and Häggkvist, R. On numerical semigroups. *Semigroup Forum 35*, 1 (1987), 63–83.

[65] Fromentin, J. A well-ordering of dual braid monoids. *Comptes Rendus Mathématique. Académie des Sciences. Paris 346*, 13-14 (2008), 729–734.

[66] Fromentin, J. The well-ordering of dual braid monoid. *Journal of Knot Theory and its Ramifications 19*, 5 (2010), 631–654.

[67] Fromentin, J. Every braid admits a short sigma-definite expression. *Journal of the European Mathematical Society 13*, 6 (2011), 1591–1631.

[68] Fromentin, J. The rotating normal form of braids is regular. *Journal of Algebra 501* (2018), 545–570.

[69] Fromentin, J., and Hivert, F. Exploring the tree of numerical semigroups. *Mathematics of Computation 85*, 301 (2016), 2553–2568.

[70] Fromentin, J., and Paris, L. A simple algorithm for finding short sigma-definite representatives. *Journal of Algebra 350* (2012), 405–415.

[71] GAP – Groups, Algorithms, and Programming, Version 4.10.2, 2019.

[72] García-Sánchez, P. A., Marín-Aragón, D., and Robles-Pérez, A. M. The tree of numerical semigroups with low multiplicity. *arXiv :1803.06879* (2018).

[73] Garside, F. A. The braid group and other groups. *The Quarterly Journal of Mathematics 20* (1969), 235–254.

[74] Gebhardt, V. Computing growth functions of braid monoids and counting vertex-labelled bipartite graphs. *Journal of Combinatorial Theory. Series A 120*, 1 (2013), 232–244.

[75] Gelly, S., and Silver, D. Combining Online and Offline Knowledge in UCT. In *Proceedings of the 24th International Conference on Machine Learning* (New York, 2007), ICML '07, ACM, pp. 273–280.

[76] Golomb, S. W., and Baumert, L. D. Backtrack programming. *Journal of the Association for Computing Machinery 12* (1965), 516–524.

[77] Graham, R. Old and new problems and results in Ramsey theory. In *Horizons of Combinatorics*, vol. 17 of *Bolyai Soc. Math. Stud.* Springer, Berlin, 2008, pp. 105–118.

[78] H. Kauffman, L. State models and the jones polynomial. *Topology 26*, 3 (1987), 395–407.

[79] Heule, M. J. H. Schur Number Five. In *Thirty-Second AAAI Conference on Artificial Intelligence* (2018).

[80] Heule, M. J. H., Kullmann, O., and Marek, V. W. Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer. In *Theory and Applications of Satisfiability Testing—SAT 2016*, vol. 9710 of *Lecture Notes in Comput. Sci.* Springer, 2016, pp. 228–245.

[81] Hivert, F., Novelli, J.-C., and Thibon, J.-Y. Sur une conjecture de Dehornoy. *Comptes Rendus Mathématique. Académie des Sciences. Paris 346*, 7-8 (2008), 375–378.

[82] Hoste, J., Thistlethwaite, M., and Weeks, J. The first 1,701,936 knots. *The Mathematical Intelligencer 20*, 4 (1998), 33–48.

[83] Iyer, B., Geva, R., and Halpern, P. Cilk$^{\text{TM}}$ Plus in GCC. In *GNU Tools Cauldron* (2012).

[84] Jones, V. F. R. A polynomial invariant for knots via von Neumann algebras. *American Mathematical Society. Bulletin. 12*, 1 (1985), 103–111.

[85] Jones, V. F. R. Hecke algebra representations of braid groups and link polynomials. *Annals of Mathematics 126*, 2 (1987), 335–388.

[86] Kannan, R. Lattice translates of a polytope and the Frobenius problem. *Combinatorica 12*, 2 (1992), 161–177.

[87] Kaplan, N. Counting numerical semigroups by genus and some cases of a question of Wilf. *Journal of Pure and Applied Algebra 216*, 5 (2012), 1016–1032.

[88] Krammer, D. The braid group B_4 is linear. *Inventiones Mathematicae 142*, 3 (2000), 451–486.

[89] Krammer, D. Braid Groups are Linear. *The Annals of Mathematics 155*, 1 (2002), 131.

[90] Laver, R. Braid group actions on left distributive structures, and well orderings in the braid groups. *Journal of Pure and Applied Algebra 108*, 1 (1996), 81–98.

[91] Lickorish, W. B. R. Prime knots and tangles. *Transactions of the American Mathematical Society 267*, 1 (1981), 321–332.

[92] Mairesse, J., and Mathéus, F. Randomly Growing Braid on Three Strands and the Manta Ray. *The Annals of Applied Probability 17*, 2 (2007), 502–536.

[93] Malvenuto, C., and Reutenauer, C. Duality between quasi-symmetric functions and the Solomon descent algebra. *Journal of Algebra 177*, 3 (1995), 967–982.

[94] Markoff, A. On the impossibility of certain algorithms in the theory of associative systems. *C. R. Acad. Sci. URSS 55* (1947), 583–586.

[95] Matsumoto, H. Générateurs et relations des groupes de Weyl généralisés. *Comptes Rendus Mathématique. Académie des Sciences. Paris 258* (1964), 3419–3422.

[96] Medeiros, N. Numerical Semigroups. http ://w3.impa.br/˜nivaldo/algebra/semigroups/index.html.

[97] Novelli, J.-C., and Thibon, J.-Y. Free quasi-symmetric functions and descent algebras for wreath products, and noncommutative multi-symmetric functions. *Discrete Mathematics 310*, 24 (2010), 3584–3606.

[98] Novikov, P. S. *Ob Algoritmičeskoĭ Nerazrešimosti Problemy Toždestva Slov v Teorii Grupp.* Trudy Mat. Inst. Im. Steklov. No. 44. Izdat. Akad. Nauk SSSR, Moscow, 1955.

[99] Ore, O. Linear equations in non-commutative fields. *Annals of Mathematics 32*, 3 (1931), 463–477.

[100] Pagel, G. Thèse de doctorat - ulco, 2018.

[101] Paris, L. Artin monoids inject in their groups. *Commentarii Mathematici Helvetici 77*, 3 (2002), 609–637.

[102] Paterson, M. S., and Razborov, A. A. The set of minimal braids is co-NP-complete. *Journal of Algorithms 12*, 3 (1991), 393–408.

[103] Post, E. L. Recursive unsolvability of a problem of Thue. *The Journal of Symbolic Logic 12* (1947), 1–11.

[104] Rado, R. Studien zur Kombinatorik. *Mathematische Zeitschrift 36*, 1 (1933), 424–470.

[105] Rado, R. Some Solved and Unsolved Problems in the Theory of Numbers. *The Mathematical Gazette 25*, 264 (1941), 72–77.

[106] Radziszowski, S. P. Small Ramsey numbers. *Electronic Journal of Combinatorics 1* (1994), Dynamic Survey 1, 30.

[107] Rafilipojaona, F. Lower bounds on the weak Schur numbers up to 9 colors. *Integers 17* (2017), Paper No. A39, 35.

[108] Rafilipojaona, F. A. *Nombres de Schur classiques et faibles.* PhD thesis, ULCO, 2015.

[109] Ramírez-Alfonsín, J. L. Complexity of the Frobenius problem. *Combinatorica 16*, 1 (1996), 143–147.

[110] Ramírez Alfonsin, J. L. *The Diophantine Frobenius Problem.* No. 30 in Oxford Lectures Series in Mathematics and Its Applications. Oxford University Press, Oxford ; New York, 2005.

[111] Rimmel, A., Teytaud, F., and Cazenave, T. Optimization of the Nested Monte-Carlo Algorithm on the Traveling Salesman Problem with Time Windows. In *Applications of Evolutionary Computation* (2011), Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 501–510.

[112] Robilliard, D., Fonlupt, C., Marion-Poty, V., and Boumaza, A. A Multilevel Tabu Search with Backtracking for Exploring Weak Schur Numbers. In *Artificial Evolution* (2012), J.-K. Hao, P. Legrand, P. Collet, N. Monmarché, E. Lutton, and M. Schoenauer, Eds., Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp. 109–119.

[113] Rolfsen, D. *Knots and Links.* Publish or Perish, Inc., Berkeley, Calif., 1976.

[114] Rosales, J. C., and García-Sánchez, P. A. *Numerical Semigroups.* No. v. 20 in Developments in Mathematics. Springer, New York, 2009.

[115] Rosales, J. C., García-Sánchez, P. A., García-García, J. I., and Jiménez Madrid, J. A. The oversemigroups of a numerical semigroup. *Semigroup Forum 67*, 1 (2003), 145–158.

[116] Rosales, J. C., García-Sánchez, P. A., García-García, J. I., and Jiménez Madrid, J. A. Fundamental gaps in numerical semigroups with respect to their multiplicity. *Acta Mathematica Sinica 20*, 4 (2004), 629–646.

[117] Sabalka, L. Geodesics in the braid group on three strands. In *Group Theory, Statistics, and Cryptography*, vol. 360 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 2004, pp. 133–150.

[118] Sammartano, A. Numerical semigroups with large embedding dimension satisfy Wilf's conjecture. *Semigroup Forum 85*, 3 (2012), 439–447.

[119] Schur, I. Über Kongruenz $x^m + y^m \equiv z^m \pmod{p}$. *Jahresbericht der Deutschen Mathematiker 25* (1916), 114–116.

[120] Software.intel.com. Intel® Cilk™ Homepage. https ://www.cilkplus.org/.

[121] Sylvester, J. Mathematical questions with their solutions. *Educational times 41*, 21 (1884).

[122] Tao, T. The Erdős discrepancy problem. *Discrete Analysis* (2016), Paper No. 1, 29.

[123] Tao, T., and Vu, V. *Additive Combinatorics*, vol. 105 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 2006.

[124] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 8.8), 2019. https ://www.sagemath.org.

[125] Thistlethwaite, M. B. A spanning tree expansion of the Jones polynomial. *Topology 26*, 3 (1987), 297–309.

[126] Thistlethwaite, M. B. Links with trivial Jones polynomial. *Journal of Knot Theory and its Ramifications 10*, 4 (2001), 641–643.

[127] Tits, J. Normalisateurs de tores. I. Groupes de Coxeter étendus. *Journal of Algebra 4* (1966), 96–116.

[128] Ulco. Calculco. https ://www-calculco.univ-littoral.fr.

[129] Walker, G. W. Elementary Problems and Solutions : Solutions : E985. *American Mathematical Monthly 59*, 4 (1952), 253.

[130] Wikipedia. Intel Turbo Boost. https ://en.wikipedia.org/wiki/Intel_Turbo_Boost.

[131] Wikipedia. Race condition. https ://en.wikipedia.org/wiki/Race_condition.

[132] Wikipedia. Suite de Tribonacci. https ://fr.wikipedia.org/wiki/Suite_de_Tribonacci.

[133] Wilf, H. S. A circle-of-lights algorithm for the "money-changing problem". *American Mathematical Monthly 85*, 7 (1978), 562–565.

[134] Zhai, A. Fibonacci-like growth of numerical semigroups of a given genus. *Semigroup Forum 86*, 3 (2013), 634–662.

[135] Zhao, Y. Constructing numerical semigroups of a given genus. *Semigroup Forum 80*, 2 (2010), 242–254.

Résumé

L'expérimentation sur machine pour la combinatoire algébrique devient incontournable. Elle permet par exemple de construire des objets mathématiques ayant certaines propriétés souhaitées ou encore de conjecturer certains phénomènes qu'elle seule aura permis de voir émerger. Cette approche est à l'origine des différents travaux présentés ici, portant sur la théorie des tresses et des nœuds, la combinatoire additive et la théorie de Ramsey.

La forme normale tournante est définie sur le monoïde de Birman-Ko-Lee et possède de bonnes propriétés vis-à-vis de l'ordre des tresses. Elle permet de sélectionner un unique mot, dit tournant, parmi tous les mots représentant une tresse donnée. Nous montrons alors que l'ensemble des mots tournants forme un langage rationnel.

Depuis les travaux de F.A. Garside, nous savons que toute tresse positive peut être décrite comme une suite finie de permutations. Grâce à la caractérisation locale de telles suites, nous obtenons que leur combinatoire est obtenue à partir d'une certaine matrice d'adjacence. Dans le cas classique, correspondant aux groupes de Coxeter de type A, il a été montré que le polynôme caractéristique de la matrice de rang n divise celui de rang $n+1$. Nous montrons un résultat analogue pour les tresses de type B en utilisant l'algèbre de Hopf des permutations signées.

Le polynôme de Jones est un invariant des entrelacs. Nous savons depuis 2003 qu'il existe une infinité d'entrelacs non triviaux avec au moins deux composantes qui ne sont pas détectés par le polynôme de Jones. Cependant le cas des entrelacs à une seule composante, correspondant aux nœuds, est toujours ouvert. Nous montrons qu'il existe une infinité de nœuds premiers non triviaux admettant un polynôme de Jones trivial modulo n'importe quelle puissance donnée de 2.

Les semigroupes numériques sont des sous-ensembles des entiers naturels stables par addition, contenant 0 et de complément fini. L'ensemble des semigroupes numériques peut être décrit à l'aide d'un arbre infini. Dans cet arbre les semigroupes numériques à distance g de la racine sont tous les semigroupes de genre g, c'est-à-dire ayant un complément de cardinal g. En 2008, M. Bras-Amorós a formulé trois conjectures sur la suite n_g des semigroupes numériques à distance g de la racine de l'arbre. Nous montrons que l'une de ces conjectures est satisfaite pour les semigroupes numériques *génériques*, dont la proportion parmi les semigroupes numériques de genre g tend vers 1 avec g. Nous décrivons aussi un algorithme exploitant les capacités vectorielles des processeurs modernes afin d'explorer efficacement l'arbre des semigroupes numériques. Nous avons ainsi obtenu que le nombre de semigroupes numériques de genre 70 est 1 607 394 814 170 158. Une des plus célèbres conjectures sur les semigroupes numériques est sans doute celle de Wilf. Depuis les travaux de S. Eliahou, nous savons que la conjecture de Wilf est satisfaite par les semigroupes génériques, la démonstration revient essentiellement à montrer qu'une certaine quantité W_0 est positive pour tous les semigroupes génériques. Nous montrons ici que dans le cas des semigroupes numériques non génériques il est possible d'obtenir une valeur négative de W_0 aussi petite que l'on souhaite.

Finalement, nous montrons qu'il n'existe pas de coloriage morphique à deux ou trois couleurs évitant les triplets pythagoriciens monochromatiques et nous montrons comment une exploration arborescente de Monte-Carlo imbriquée nous permet de construire une partition faiblement de Schur en 6 couleurs de longueur 582, qui est le record actuel.

Mots clés : Combinatoire algébrique, algorithme, tresses duales, tresses généralisées, automates, forme normale de Garside, algèbre de Hopf, nœuds, polynôme de Jones, semigroupes numériques, vectorialisation, conjecture de Wilf, nombre de Schur.