Université de Caen / Basse-Normandie

U.F.R. de Sciences

ÉCOLE DOCTORALE SIMEM

T H È S E

présentée par

M. Jean FROMENTIN

et soutenue le **mardi 30 juin 2009**
en vue de l'obtention du

Doctorat de l'Université de Caen

Spécialité : Mathématiques et leurs interactions
(Arrêté du 7 août 2006)

Forme normale tournante des tresses

Membres du jury

M. Patrick DEHORNOY, professeur, Unsiversité de Caen *(directeur de thèse)*
M. François DIGNE, professeur, Université de Picardie Jules-Verne
M. Philippe DUCHON, maître de conférences (H.d.R) à l'ENSEIRB, Bordeaux
M. Daan KRAMMER, professeur, University of Warwick (Grande Bretagne)
M. Jean MAIRESSE, directeur de recherche au CNRS, Université Paris Diderot
M. Jean MICHEL, directeur de recherche au CNRS, Université Paris Diderot

Rapporteurs

M. Volker GEBHARDT, professeur, University of Western Sydney (Australie)
M. Jean MAIRESSE, directeur de recherche au CNRS, Université Paris Diderot

Table des matières

À mes deux filles, Claire et Laure.

Je tiens à remercier mon directeur de thèse, Patrick Dehornoy, pour sa grande disponibilité. L'intérêt qu'il a porté à mon travail m'a permis d'affronter les moments un peu difficiles de ces trois années de thèse. Je le remercie aussi pour les longues heures qu'on a passées devant son ordinateur à modifier et à améliorer mon premier article. Au fait, combien vous dois-je ?

Au cours de ma thèse, j'ai été amené à travailler avec Volker Gehardt. Il a fait preuve d'une extrême patience envers mon anglais approximatif durant nos discussions mathématiques ou algorithmiques à propos du problème de conjugaison. Je le remercie d'autant plus qu'il a accepté d'être rapporteur de ma thèse. Malheureusement il ne pourra pas assister à la soutenance. J'exprime ma profonde gratitude envers Jean Mairesse qui a accepté d'être rapporteur de ma thèse sans l'ombre d'une hésitation. Je garde un bon souvenir de ma visite au LIAFA.

Je tiens à remercier François Digne et Jean Michel d'avoir accepté d'être membres de mon jury. Cela est particulièrement important pour moi, car ils ont écouté mon tout premier exposé en dehors de l'université de Caen. Je n'oublie pas Philippe Duchon qui me fait l'honneur d'être membre de mon jury malgré la distance entre nos thèmes de recherche. Je remercie également Daan Krammer d'avoir accepté de faire partie de mon jury, d'autant plus que mon stage de Master 2 consistait à comprendre sa démonstration de la linéarité des groupes de tresses. Je remercie également François Digne, Eddy Godelle, Ivan Marin, Jean Mairesse, Luis Paris, Bert Wiest et les membres du GDR tresses de m'avoir permis d'exposer mes résultats. Je tiens aussi à remercier toutes les personnes qui sont venues m'écouter aujourd'hui ou avant.

Je remercie Laurent et Jérémy pour avoir lu et corrigé de nombreuses fautes de mon manuscrit. Merci à Jean-Philippe, Jérémy et Pierre pour ces discussions très agréables autour d'un café ou d'un repas. Alors Pinocchio est-il le meilleur mathématicien ? Bien sûr je n'oublie pas tous les autres jeunes du laboratoire pour l'ambiance si sympathique qu'ils y apportent. Je remercie le personnel administratif pour tous les services rendus.

J'aimerais aussi remercier ma femme, Laurène, pour les sacrifices des week-ends et des soirées que j'ai passés à travailler sur ma thèse. Je n'oublie pas tous les autres membres de ma famille, mon père, ma mère, Sébastien, Anaëlle et Esteban que je n'ai pas réussi à rencontrer autant de fois que je le voulais. J'exprime mes remerciement envers mes beaux parents Anne et Daniel pour l'aide qu'ils m'ont apporté ainsi que pour leurs précieuses relectures.

Introduction

Cette thèse porte sur certaines propriétés combinatoires des groupes de tresses. Plus spécifiquement, nous étudions les monoïdes de Birman–Ko–Lee (ou monoïdes de tresses duaux) ainsi que l'ordre standard des tresses (ou ordre de Dehornoy).

CONTEXTE GÉNÉRAL ET RÉSULTATS PRÉCÉDEMMENT CONNUS

Il semble que la première référence où les groupes de tresses sont explicitement introduits et étudiés soit un texte de E. Artin qui fut publié en 1925 [Art25]. Ce texte a ensuite été republié sous une forme légèrement différente dans [Art47]. Cependant, la notion de tresse et plusieurs idées qui y sont liées remontent au XIXe siècle, dans les travaux d'A. Hurwitz, F. Klein, H. Poincaré, B. Reimann et certainement d'autres. On peut même trouver un schéma de tresses dans des notes de C.F. Gauß [Gau].

Les tresses ont fait l'objet de plusieurs travaux de recherche ces dernières années, en particulier, parce qu'elles sont assez simples pour obtenir des preuves accessibles et, en même temps, assez difficiles pour donner lieu à des résultats profonds. Un important tournant fut la découverte de V. Jones d'un lien profond entre les groupes de tresses et la théorie des opérateurs, la mécanique statistique et d'autres notions de physique mécanique aux alentours de 1984 [Jon87]. Plus récemment, D. Krammer [Kra00, Kra02] et S. Bigelow [Big01] ont établi la linéarité des groupes de tresses, c'est-à-dire qu'ils admettent une représentation fidèle dans un espace vectoriel de dimension finie.

D'autre part, de nombreuses généralisations des groupes de tresses ont été introduites avec profit. En 1966, J. Tits a défini et étudié les groupes de tresses associés à des groupes de Coxeter quelconques dans [Tit66]. Cette étude a été poursuivie en 1972 par P. Deligne dans [Del72] et E. Brieskorn avec K. Saito dans [BS72]. En 1998, M. Broué, G. Malle et R. Rouquier ont étendu l'étude aux groupes de tresses de groupes de réflexions complexes [BMR98]. En 1999, P. Dehornoy et L. Paris ont introduit la notion de groupe de Garside [DP99], une version abstraite de l'approche développée par F.A. Garside pour les groupes des tresses dans [Gar69].

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. Une présentation algébrique a été établie par E. Artin dans [Art25], et c'est le point de départ qui sera utilisé dans ce travail. Pour nous, B_n est donc le groupe de présentation

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

Ainsi une tresse à n brins est une classe d'équivalence (infinie) de mots en les lettres $\sigma_i^{\pm 1}$. De tels mots seront appelés *mots de tresse*. Nous nous référerons souvent aux lettres σ_i comme les *générateurs d'Artin*. La correspondance standard entre les éléments de la présentation de B_n et les tresses géométriques consiste à utiliser σ_i comme un code pour la tresse géométrique où le $i$ème et le $(i+1)$ ème brins se croisent, avec la convention que le brin originellement en position $(i+1)$ passe au-dessus de l'autre.

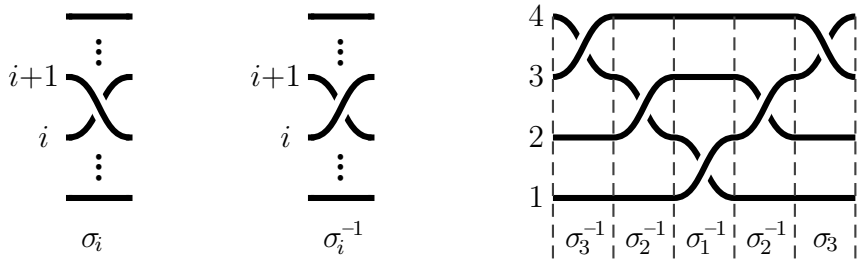


FIG. 1 : Interprétation d'un mot en les lettres $\sigma_i^{\pm 1}$ comme diagramme de tresse géométrique.

Ordre des tresses

La théorie des groupes ordonnés a environ un siècle. Le résultat le plus connu portant sur les groupes ordonnables est sans doute un théorème de O.L. Hölder [Höl01] datant de 1901, qui caractérise le groupe $(\mathbb{R}, +)$ comme l'unique groupe maximal ordonnable satisfaisant la propriété dite archimédienne.

Un ordre total $<$ défini sur un groupe G est dit *invariant à gauche* si la relation $g < h$ implique $fg < fh$ pour tout f, g et h de G. Dans [Deh94], P. Dehornoy construit un ordre total invariant à gauche sur B_n. Cet ordre est facilement décrit à l'aide de mots de tresse d'un type particulier :

> **Théorème I.3.9.** (P. Dehornoy, [Deh94]) *On pose $\beta < \beta'$ si la tresse quotient $\beta^{-1}\beta'$ peut être représentée par un mot de tresse σ-positif, c'est-à-dire, un mot de tresse dont la lettre σ_i de plus grand indice i n'apparaît que positivement, dans le sens où la lettre σ_i apparaît, mais pas σ_i^{-1}. La relation $<$ est alors un ordre total invariant à gauche sur B_n pour tout n.*

Le fait que la relation $<$ soit un ordre total invariant à gauche est conséquence des deux propriétés qui suivent. On dit qu'un mot de tresse est *σ-négatif* si son inverse est σ-positif, et qu'un mot de tresse est σ-défini s'il est soit σ-positif soit σ-négatif. En d'autres termes, un mot de tresse est σ-défini si la lettre σ_i de plus grand indice i n'apparaît que positivement ou que négativement.

Propriété A. Une tresse représentée par un mot σ-défini est non triviale.

Propriété C. Toute tresse non triviale admet un représentant σ-défini.

Ces deux propriétés on été démontrées dans [Deh94] à l'aide de méthodes d'algèbre autodistributive. Elles ont été redémontrées par D. Larue dans [Lar94] en utilisant la représentation dite d'Artin des tresses en termes d'automorphismes d'un groupe libre. Ultérieurement, en 1999, R. Fenn, M. Greene, D. Rolfsen, C. Rourke et B. Wiest ont utilisé une méthode topologique pour reconstruire un ordre invariant à gauche sur B_n vu comme groupe d'homéotopie du disque unité à n trous [FGR$^+$99]. Leur approche est une version géométrique de celle de D. Larue. Le fait remarquable est que cet ordre coïncide avec celui du théorème I.3.9. Encore plus de démonstrations des propriétés A et C ont été proposées dans d'autres travaux reposant sur des approches variées. Nous référons à [DDRW02, DDRW08].

Par ailleurs, en 2000, B. Wiest et H. Short construisent dans [SW00] une famille entière d'ordres invariants à gauche sur B_n définie à partir de la géométrie hyperbolique du recouvrement universel du disque troué, en suivant une approche remontant à W. Thuston et même à J. Nielsen [Nie27]. Nous renvoyons à [Ito08] pour une description combinatoire de certains de ces ordres. Il est maintenant connu que l'ensemble des ordres sur B_n a des propriétés tout à fait intéressantes, voir [Nav07].

Expression σ-définie

Comme mentionné précédemment, le point clé de l'existence de l'ordre est la propriété C, qui établit que toute tresse non triviale admet au moins une expression σ-définie, c'est-à-dire, une expression dans laquelle le générateur σ_i de plus grand indice i apparaît seulement positivement, ou seulement négativement. Indépendamment de toute considération d'ordre, cette propriété est un résultat fondamental des tresses (il doit être noté qu'elle ne peut pas être étendue aux groupes de tresses généralisés associés aux groupes de Coxeter de type autre que A et B, voir [Sib03]).

Durant les vingt dernières années, au moins cinq ou six démonstrations de ce résultat ont été proposées. Comme nous l'avons dit, la première par P. Dehornoy en 1992 repose sur les algèbres auto-distributives [Deh94]. La suivante, par D. Larue [Lar94], utilise la représentation d'Artin des tresses comme automorphismes du groupe libre, un argument qui a été indépendamment redécouvert part R. Fenn, M. Greene, D. Rolfsen, C. Rourke et B. Wiest [FGR$^+$99] dans un langage topologique. Une démonstration complètement différente fondée sur la géométrie du graphe de Cayley du groupe de tresse B_n et la théorie de Garside apparaît dans [Deh97a]. Il existe aussi au moins deux démonstrations reposant sur des algorithmes de relaxation, qui sont des stratégies pour simplifier de proche en proche l'image d'une (famille de) courbe(s) dessinée dans un disque et déformée par l'action d'une tresse vue comme un homéomorphisme du disque. Une est décrite par I. Dynnikov et B. Wiest dans [DW07], une autre par X. Bressaud dans [Bre08].

Toutes ces méthodes sont effectives et donnent lieu à des algorithmes. Cependant, en termes de complexité en espace et en temps, aucune n'a une compléxité meilleure qu'exponentielle. En particulier, la meilleure borne supérieure obtenue pour la longueur d'un mot σ-défini final équivalent à un mot de tresse initial de longueur ℓ est une exponentielle en ℓ. D'un autre côté, certaines méthodes sont connues comme extrêmement efficaces en pratique, et la conjecture suivante appartient au folklore du sujet :

> **Conjecture IV.0.1.** *Pour tout n, il existe une constante C_n telle que, pour tout mot de tresse w à n brins de longueur ℓ, il existe un mot σ-défini équivalent de longueur au plus $C_n\ell$.*

En d'autres termes, la conjecture affirme que toute tresse admet un représentant σ-défini quasi-géodésique.

Tresses et bon ordre

Le monoïde de tresses positives à n brins, noté B_n^+, est le sous-monoïde du groupe B_n engendré par $\sigma_1, \dots, \sigma_{n-1}$. Il est composé des tresses pouvant être représentées par un mot de tresse positif, c'est-à-dire, un mot ne contenant pas de lettre σ_i^{-1}. Par les résultats de Garside [Gar69], le monoïde B_n^+ admet la présentation donnée en (1) pour le groupe de tresses B_n, vue comme présentation de monoïde.

Restreindre l'ordre des tresses $<$ au sous-monoïde B_n^+ de B_n munit trivialement B_n^+ d'un ordre total invariant à gauche. De plus, cette restriction admet des propriétés supplémentaires remarquables.

On dit qu'un ordre total $\prec$ sur X est un *bon ordre* si toute partie non vide de X admet un plus petit élément pour $\prec$. Avec une version faible de l'axiome du choix, ceci est équivalent à dire qu'il n'existe pas de suite infinie $\prec$-décroissante dans X.

Clairement, pour $n \geqslant 2$, l'ensemble B_n muni de l'ordre standard des tresses n'est pas un bon ordre car il contient la suite infinie décroissante $1, \sigma_1^{-1}, \sigma_1^{-2}, \dots$. Cependant, en 1996, R. Laver a montré dans [Lav96] que, pour chaque n, la restriction de $<$ au monoïde B_n^+ est un bon ordre.

Une des bonnes propriétés d'un bon ordre est que, contrairement à un ordre total quelconque, un bon ordre est complètement déterminé à isomorphisme près par un seul paramètre, à savoir sa longueur, qui est habituellement spécifiée par un ordinal. Nous rappelons que les ordinaux constituent une extension de la suite des entiers naturels au-delà de l'infini. Par exemple, le premier ordinal infini ω est le plus petit majorant des entiers naturels. L'ordinal suivant est $\omega + 1$, ensuite vient $\omega + 2$, etc.

Pour ce que nous allons faire ici, il est suffisant de mentionner que les ordinaux sont naturellement munis d'un ordre total qui est un bon ordre, et d'opérations arithmétiques, addition, multiplication, exponentiation qui étendent celles des entiers naturels et partagent certaines de leurs propriétés (mais pas toutes). Pour plus de résultats sur les ordinaux, voir par exemple [Lév79]. Basée sur le théorème de Higman [Hig52], la démonstration de Laver du fait que $(B_n^+, <)$ soit bien ordonné n'est pas effective, et ne fournit aucun moyen de déterminer sa longueur. Cette dernière fut donnée par S. Burckel dans sa thèse [Bur94], puis dans [Bur97] :

Théorème I.3.17. (S. Burckel, [Bur97]) *La restriction de $<$ à B_n^+ est un bon ordre de longueur $\omega^{\omega^{n-2}}$.*

La démonstration donnée par S. Burckel repose sur un argument subtil d'induction transfinie qui est difficile à contrôler en pratique.

La forme normale alternante

Par définition, une tresse est une classe d'équivalence de mots de tresse. Diverses *formes normales* ont été décrites dans la littérature, c'est-à-dire, divers moyens de sélection, pour toute tresse, d'un mot de tresse distingué la représentant. La dite *forme normale alternante* est une telle forme normale. Elle est seulement définie pour les tresses positives et fut introduite en 2008 par P. Dehornoy dans [Deh08].

La construction de la forme normale alternante d'une tresse à n brins repose sur l'opération dite de Φ_n-éclatement qui associe à chaque tresse positive à n brins une suite finie de tresses positives à $(n-1)$ brins la déterminant complètement.

Pour donner une description plus précise, nous devons introduire une relation de divisibilité à droite dans le monoïde B_n^+. Pour β, γ dans B_n^+, on dit que γ *divise à droite* β, ou, de manière équivalente, que β est un *multiple à gauche* de γ s'il existe une tresse positive β' satisfaisant la relation $\beta = \beta' \gamma$. Il est connu que B_n^+ muni de la relation de divisibilité à droite a une structure de treillis, c'est-à-dire, que deux tresses positives quelconques admettent un unique plus grand diviseur à droite (ou pgcd à droite) et un unique plus petit multiple commun à gauche (ou ppcm à gauche). C'est l'un des ingrédients de la structure dite de *Garside* du monoïde B_n^+. Un autre ingrédient est le fait que le ppcm à gauche Δ_n des générateurs d'Artin $\sigma_1, \dots, \sigma_{n-1}$ est aussi leur ppcm à droite. Ceci implique que l'automorphisme intérieur Φ_n du groupe B_n associé à Δ_n préserve le monoïde B_n^+, et, donc, que Φ_n induit un automorphisme du monoïde B_n^+. De plus, l'automorphisme Φ_n préserve la divisibilité à gauche (et à droite), donc il préserve les opérations de pgcd et de ppcm. On vérifie facilement que Φ_n échange σ_i et σ_{n-i} pour tout i, donc, géométriquement, Φ_n agit comme une symétrie sur les diagrammes de tresses.

Proposition III.1.22. (P. Dehornoy, [Deh08]) *Pour toute tresse non triviale β de B_n^+ avec $n \geqslant 3$, il existe une unique suite finie $(\beta_b, \dots, \beta_1)$ de tresses de B_{n-1}^+ avec β_b non triviale satisfaisant $\beta = \Phi_n^{b-1}(\beta_b) \cdot \dots \cdot \Phi_n(\beta_2) \cdot \beta_1$ et telle que, pour tout k, la tresse β_k est le plus grand diviseur à droite dans B_{n-1}^+ de $\Phi_n^{b-k}(\beta_b) \cdot \dots \cdot \Phi_n(\beta_{k+1}) \cdot \beta_k$.*

Dans les conditions ci-dessus, la suite $(\beta_b, \dots, \beta_1)$ est appelée le Φ_n*-éclatement* de la tresse positive β. Les termes d'un Φ_n-éclatement sont numérotés de la droite vers la gauche afin d'insister sur le fait que la construction commence à partir de la droite et consiste à prendre le plus grand diviseur à droite à chaque étape.

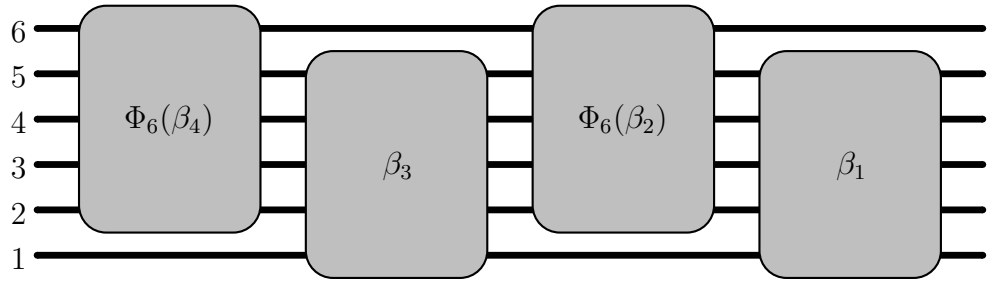


FIG. 2 : Partant d'une tresse β de B_6^+, on prend le plus grand diviseur à droite de β laissant le 6ème brin invariant, puis on prend le plus grand diviseur à droite du reste laissant le 1er brin invariant, etc. On obtient ainsi le ϕ_6-éclatement de β.

Le principal résultat de [Deh08] est une description inductive de l'ordre des tresses $<$ sur B_n^+ en termes d'ordre sur B_{n-1}^+ et de Φ_n-éclatement. Plus précisement, le résultat est le suivant :

Théorème III.1.26. (P. Dehornoy, [Deh08]) *Pour β, β' dans B_n^+, la relation $\beta < \beta'$ est satisfaite si et seulement si le Φ_n-éclatement de β est plus petit que le Φ_n-éclatement de β' vis-à-vis de l'extension `ShortLex` de l'ordre $<$ sur B_{n-1}^+.*

On rappelle que si $(X, \prec)$ est un ensemble ordonné, une suite finie s d'éléments de X est dite `ShortLex` plus petite qu'une autre suite finie s', si la longueur de s est strictement plus petite que celle de s', ou alors si les longueurs de s et s' sont égales et s est $\prec$-lexicographiquement plus petite que s', c'est-à-dire, lorsque les deux suites sont lues en partant de la gauche, le premier terme dans s qui ne coïncide pas avec son homologue dans s' est plus petit pour l'ordre $\prec$.

Il doit être noté que le lien entre le Φ_n-éclatement et l'ordre des tresses établi dans [Deh08] utilise les travaux de S. Burckel. Cette approche ne permet donc pas de décire directement le type d'ordre du bon ordre $(B_n^+, <)$, mais en donne une description alternative.

Monoïdes de tresses duaux

En 1998, J.S. Birman, K.H. Ko et S.J. Lee [BKL98] 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 de tresses dual* a été proposé ultérieurement et provient du fait que certains paramètres obtiennent des valeurs symétriques s'ils sont évalués dans B_n^+ ou dans B_n^{+*} ; une correspondance qui a été étendue par D. Bessis au contexte plus général des groupes d'Artin–Tits [Bes03].

Nous rappelons que le groupe des tresses B_n^+ est le sous-monoïde de B_n engendré par les éléments $\sigma_1, \dots, \sigma_{n-1}$, où, géométriquement, σ_i correspond au croisement des brins i et $(i+1)$. Le monoïde de tresses dual B_n^{+*} est le sous-monoïde du groupe de tresse B_n engendré par les tresses $a_{i,j}$ avec $1 \leqslant i < j \leqslant n$, où $a_{i,j}$ est définie par $a_{i,j} = \sigma_i \dots \sigma_{j-1}\ \sigma_j^{-1}\ \sigma_{j-1}^{-1} \dots \sigma_i^{-1}$. Géométriquement, $a_{i,j}$ correspond au croisement des brins i et j, le tout par-dessous les (possibles) brins intermédiaires.

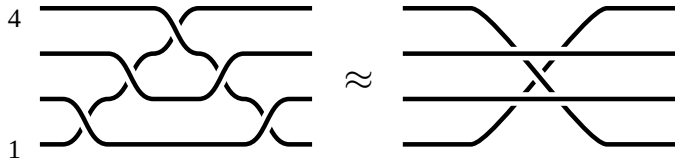


FIG. 3 : Dans la tresse géométrique représentée par $a_{1,4}$, les brins 1 et 4 se croisent en dessous des brins 2 et 3.

Par définition, σ_i est égale à $a_{i,i+1}$ et, donc, le monoïde B_n^+ est inclus dans B_n^{+*}, une inclusion stricte pour $n \geqslant 3$ car la tresse $a_{1,3}$ n'appartient pas à B_3^+.

Il est connu [BKL98] que le monoïde de tresses dual admet une structure de Garside similaire à celle de B_n^+. Ainsi, en particulier, deux éléments quelconques de B_n^{+*} admettent des ppcm et des pgcd à gauche et à droite. Le rôle de l'élément de Garside Δ_n est joué dans le cas de B_n^{+*} par la tresse δ_n définie comme étant $a_{1,2}\, a_{2,3} \dots a_{n-1,n}$, c'est-à-dire, $\sigma_1\, \sigma_2 \dots \sigma_{n-1}$.

Le lien entre le monoïde B_n^{+*} et le groupe symétrique $\mathfrak{S}_n$ a été étudié dans [Bes03] et dans [Bra01]. Des liens avec les racines n èmes de l'unité et la théorie de Springer apparaissent dans [BDM02].

Le problème de conjugaison

Le problème de conjugaison du groupe B_n est le problème de décider si deux tresses β, β' de B_n sont conjuguées, c'est-à-dire, s'il existe une tresse γ de B_n satisfaisant $\beta = \gamma^{-1}\, \beta'\, \gamma$.

Depuis les travaux de F.A. Garside [Gar69], il est connu que le problème de conjugaison a une solution algorithmique. Cependant, à ce jour, toutes les solutions connues sont exponentielles en complexité. C'est le cas pour la solution originale de F.A. Garside, comme pour toutes les améliorations successives décrites par E.A. El-Rifai et H.R. Morton dans [ERM94], par N. Franco et J. González-Meneses dans [FGM03], et par J. González-Meneses et V. Gebhardt dans [GMG08].

Toutes les solutions citées ci-dessus utilise la structure de Garside de B_n, soit celle associée au monoïde B_n^+ et à la tresse Δ_n, soit celle associée au monoïde B_n^{+*} et à la tresse δ_n.

LES RÉSULTATS DE CE TRAVAIL

Dans cette thèse nous établissons de nouveaux résultats combinatoires portant sur les tresses, et, plus spécifiquement, sur les monoides de tresses duaux B_n^{+*} et l'ordre standard des tresses. Notre principal outil est une nouvelle forme normale, appelée *forme normale tournante*.

Forme normale tournante

Le point de départ de la construction de la forme normale alternante dans le monoïde d'Artin B_n^+ est l'observation que toute tresse de B_n^+ admet un unique diviseur à droite maximal appartenant à B_{n-1}^+. Une propriété similaire est vérifiée dans le cas des monoïdes de tresses duaux B_n^{+*} et B_{n-1}^{+*}. Il est donc naturel de chercher une adaptation de la forme normale alternante à ce contexte.

Comme rappelé précédemment, le monoïde de tresses dual B_n^{+*} est muni d'une structure de Garside, dans laquelle le rôle de la tresse Δ_n est joué par δ_n. Il s'ensuit que l'analogue de Φ_n, qui est une conjugaison par Δ_n, est l'automorphisme ϕ_n de conjugaison par δ_n. Comme la tresse Δ_n^2 est un élément du centre de B_n, l'automorphisme Φ_n est une involution, qui correspond géométriquement à une symétrie des diagrammes de tresses. Par ailleurs, la plus petite puissance de δ_n appartenant au centre de B_n est δ_n^n. L'automorphisme ϕ_n est donc d'ordre n. En particulier, on trouve $\phi_n(a_{i,j}) = a_{i+1,j+1}$ pour $j \leqslant n-1$ et $\phi_n(a_{i,n}) = a_{1,i+1}$. Géométriquement, l'automorphsime ϕ_n devrait donc être vu comme une rotation, ce qui a un sens si l'on dessine les diagrammes de tresses sur un cylindre au lieu d'un rectangle plan.

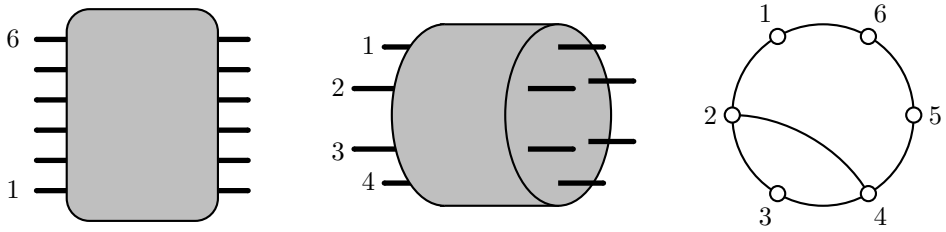


FIG. 4 : Enrouler le diagramme de tresse usuel aide à visualiser les symétries des tresses $a_{p,q}$. Sur le cercle obtenu, $a_{p,q}$ correspond naturellement à la corde reliant les points p et q.

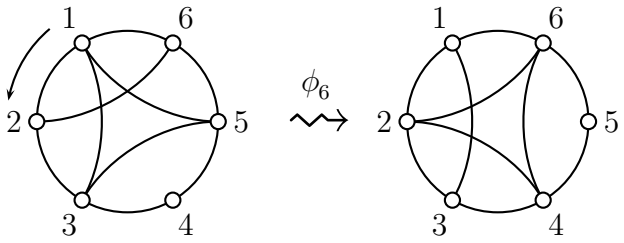


FIG. 5 : Représentation de l'automorphisme ϕ_n comme une rotation d'angle $\frac{2\pi}{n}$ dans le sens contraire des aiguilles d'une montre.

Notre premier résultat est une adaptation de la construction de la forme normale alternante aux monoïdes de tresse dual B_n^{+*}.

Proposition III.2.7. *Pour toute tresse non triviale β de B_n^{+*} avec $n \geqslant 3$, il existe une unique suite finie $(\beta_b, \dots, \beta_1)$ de tresses de B_{n-1}^{+*} avec $\beta_b \neq 1$ satisfaisant la relation $\beta = \phi_n^{b-1}(\beta_b) \cdot \dots \cdot \phi_n(\beta_2) \cdot \beta_1$, et telle que, pour chaque k, la tresse β_k est le plus grand diviseur à droite de $\phi_n^{b-k}(\beta_b) \cdot \dots \cdot \phi_n(\beta_{k+1}) \cdot \beta_k$ dans B_{n-1}^{+*}.*

Dans le conditions ci-dessus,la suite $(\beta_b, \dots, \beta_1)$ est appelée le ϕ_n-*éclatement* de la tresse β. La démonstration de ce résultat utilise les propriétés standard de B_n^{+*}, et n'est pas réellement difficile une fois que la définition correcte a été donnée.

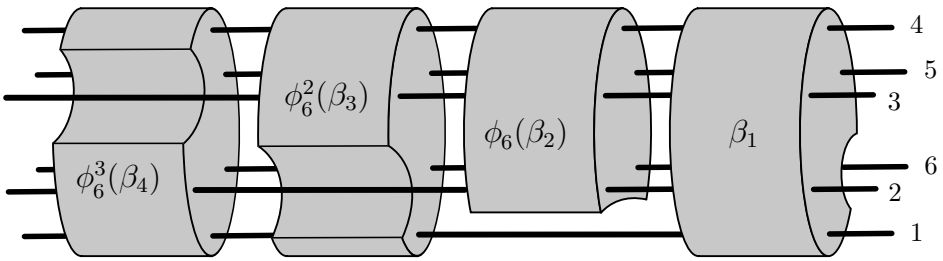


FIG. 6 : Le ϕ_6-éclatement d'une tresse de B_6^{+*}. Partant de la droite on extrait le plus grand diviseur à droite maximal qui laisse le sixième brin invariant, puis on extrait le plus grand diviseur à droite de la tresse restante laissant le premier brin invariant, etc.

Utilisant la procédure du ϕ_n-éclatement inductivement, on déduit un représentant de toute tresse de B_n^{+*} en terme (d'image) de tresses de B_2^{+*}, c'est-à-dire, de puissance de $a_{1,2}$. On définit un homomorphisme de mots de tresses duaux, encore noté ϕ_n, qui envoie une lettre $a_{i,j}$ avec $j \leqslant n-1$ sur $a_{i+1,j+1}$ et une lettre $a_{i,n}$ sur $a_{1,i+1}$.

Définition III.2.12. Pour β dans B_n^{+*}, on définit la *forme normale tournante* de β par
– l'unique puissance de $a_{1,2}$ représentant β, pour $n = 2$;
– le mot $\phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1$, où $(\beta_b, \ldots, \beta_1)$ est le ϕ_n-éclatement de β et w_k est la forme normale tournante de β_k, pour $n \geqslant 3$.

La forme normale tournante est un outil très pratique pour étudier le monoïde B_n^{+*} et, à partir de là, le groupe B_n, qui est le groupe de fractions de B_n^{+*}. Il semble que l'un des principaux avantages à utiliser la forme normale tournante à la place de la forme normale alternante est qu'il existe plus de relations reliant les $a_{i,j}$ (qui forment une famille hautement redondante de générateurs du groupe de tresses). Il s'ensuit que distinguer un représentant spécifique d'une tresse est, en un certain sens, plus difficile dans B_n^{+*} que dans B_n^+, mais, lorsqu'on y arrive, c'est potentiellement plus intéressant. Quelles que soient les raisons, le point est que nous allons être capables d'établir de nombreuses propriétés spécifiques à la forme normale tournante n'ayant pas d'homologue connu à ce jour dans le cas de la forme normale alternante.

Un résultat typique dans cette direction est la caractérisation suivante des suites de B_{n-1}^{+*} qui sont des ϕ_n-éclatements. Nous disons qu'une lettre $a_{r,s}$ de B_{n-1}^{+*} est une $a_{p,n}$-barrière si les conditions $r < p$ et $p < s$ sont vérifiées.

Théorème III.4.4. *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*
– *pour $k \geqslant 3$, la tresse β_k est non triviale,*
– *pour $k \geqslant 2$, aucune tresse non triviale de B_{n-1}^{+*} ne divise à droite $\phi_n(\beta_k)$,*
– *si, pour $k \geqslant 3$, la tresse β_k est divisible à droite par $a_{p-1,n-1}$, alors au moins une (et alors toute) expression de β_{k-1} contient une $a_{p,n}$-barrière.*

La démonstration de ce résultat nécessite la notion d'*échelle* développée à la section III.3.3 ainsi que quelques propriétés de l'algorithme bien connu du *retournement* sur le monoïde de tresse dual, redonné à la section II.3.

On appelle *mot tournant à n brins* la forme normale d'une tresse de B_n^{+*}. Une conséquence du théorème III.4.4 est le résultat suivant :

Corollaire III.4.31. *Pour tout n, la famille des mots tournants à n brins est un langage régulier.*

Plus précisement nous obtenons une construction inductive d'automates finis reconnaissant le langage des mots tounants.

Expression σ-définie

Le résultat principal de cette thèse est la démonstration de la conjecture IV.0.1 portant sur l'existence de représentant σ-défini quasi-géodésique. Pour β une tresse, nous notons par $\|\beta\|_\sigma$ la longueur géodésique de β par rapport aux générateurs d'Artin σ_i, c'est-à-dire, la longueur d'un plus court mot en les lettres $\sigma_i^{\pm 1}$ représentant β. Nous démontrons alors le résultat suivant :

> **Théorème IV.3.17.** *Toute tresse β à n brins admet une expression σ-définie de longueur au plus $6(n-1)^2\|\beta\|_\sigma$.*

Le résultat précédent est presque optimal : il est connu qu'une tresse ne peut pas admettre de représentant σ-défini géodésique, et, plus précisement que l'on ne peut pas espérer mieux qu'une borne $C_n\|\beta\|_\sigma$ avec C_n au moins linéaire en n. Plus précisément B. Wiest a montré que la tresse à n brins

$$\sigma_{n-1}\sigma_{n-2}^{-2}\sigma_{n-3}^{2}\sigma_{n-4}^{-2}\ldots\sigma_1^{2e}\sigma_2^{2e}\sigma_3^{-2e}\ldots\sigma_{n-2}^{2}\sigma_{n-1}^{-1},$$

avec $e = \pm 1$ en fonction de la parité de n, n'admet pas de représentant σ-défini de moins de $(n-2)(n-1)$ lettres. Comme le mot ci-dessus est de longueur $4(n-2)$, la constante C_n doit croître au moins linéairement en n : $C_n \geqslant (n+1)/4$.

D'ailleurs, le facteur $(n-1)^2$ du théorème IV.3.17 provient d'une étape de traduction finale des générateurs de Birman–Ko–Lee en les générateurs d'Artin. Si nous considérons le problème analogue portant sur les générateurs d'Artin $a_{i,j}$, alors, en notant $\|\beta\|_a$ la longueur géodésique de β par rapport aux générateurs de Birman–Ko–Lee, on a

> **Théorème IV.3.16.** *Toute tresse β à n brins admet une expression σ-définie de longueur au plus $3(n-1)\|\beta\|_a$.*

Le principe de l'argument est le suivant. Étant donnée une tresse β de B_n, on commence d'abord par l'exprimer comme fraction $\delta_n^{-t}\,\beta'$, où, on le rappelle, δ_n est l'élément de Garside de B_n^{+*}, et où β' est un élément de B_n^{+*}. Ceci est possible car B_n est le groupe de fraction du monoïde B_n^{+*}. Si l'exposant t est plus grand que la longueur du ϕ_n-éclatement de β', alors le facteur σ-négatif δ_n^{-t} l'emporte sur le facteur σ-positif β et un mot σ-négatif représentant β peut être facilement obtenu par un calcul direct consistant essentiellement à intercaler un δ_n^{-1} entre les termes du ϕ_n-éclatement de β'. Sinon, si l'exposant t est plus petit que la longueur du ϕ_n-éclatement de β', on détermine la forme normale tournante w de β' et on essaie d'obtenir un représentant σ-positif de β en poussant le facteur négatif δ_n^{-t} à droite au travers de w. Le problème est que certains mots σ-négatifs d'une forme particulière, appelés *mots dangereux*, apparaissent à chaque étape. Le point clé est que les mots tournants possèdent certaines propriétés syntaxiques, nous permettant de contrôler l'impact des mots dangereux. L'étape élémentaire de l'opération consiste à échanger un mot dangereux et un mot tournant. Pour cela nous définissons et utilisons l'algorithme dit de *renversement*, qui est facilement décrit à l'aide de diagrammes comme pour l'algorithme bien connu du retournement. Cependant, démontrer qu'il effectue la tâche demandée est plus délicat et nécessite l'introduction de la notion de *mur*, qui est un affaiblissement de la notion d'*échelle* introduite à la section III.3.3. Pour le moment, mentionnons qu'un mot tournant est une échelle, que le produit d'un fragment d'un mot dangereux suivi

d'une échelle donne un mur et que le produit d'un fragment d'un mot dangereux donne encore un mur.

La démonstration du théorème IV.3.17 mène alors à un algorithme effectif. L'analyse de complexité de cet algorithme donne :

> **Théorème IV.3.18.** *La complexité en temps de l'algorithme impliqué dans la démonstration du théorème IV.3.17 est quadratique : pour tout mot de tresses à n brins de longueur ℓ, le temps d'exécution de l'algorithme est en $O(\ell^2)$.*

La démonstration du théorème IV.3.17 ne s'appuyant sur aucun résultat lié à l'ordre des tresses, nous en déduisons une nouvelle démonstration de la propriété **C**, c'est-à-dire, de l'existence d'un représentant σ-défini pour toute tresse non triviale. Cette démonstration est l'une des meilleures que l'on connaisse, car pour le moment c'est la seule pour laquelle on a démontré que l'on obtenait un représentant σ-défini quasi-géodésique.

D'un autre côté, si l'on considère la propriété **C** comme acquise et que l'on souhaite obtenir une expression σ-définie courte, alors, comme suggéré par L. Paris, on peut construire un algorithme plus simple que celui du théorème IV.3.17 : en utilisant l'astuce de X. Bressaud dans son algorithme de relaxation [Bre08], on applique en parallèle l'algorithme du théorème IV.3.17 sur β et β^{-1} ; le cas facile du théorème IV.3.17 est alors suffisant pour obtenir un représentant σ-défini soit pour β soit pour β^{-1}, ce qui est suffisant pour conclure. De cette manière, on démontre :

> **Théorème IV.3.24.** *Toute tresse β à n brins admet une expression σ-définie en les lettres σ_i de longueur au plus $2(n-1)^2\|\beta\|_\sigma$ et une expression σ-définie en les lettres $a_{p,q}$ de longueur au plus $(n-1)\|\beta\|_a$.*

Type d'ordre de B_n^{+*}

Une autre conséquence du résultat de R. Laver montrant que certains sous-monoïdes de B_n sont bien ordonnés pour $<$, est que la restriction de l'ordre des tresses $<$ au monoïde B_n^{+*} est un bon ordre pour tout n. Comme dans le cas du monoïde des tresses positives B_n^+, l'approche de R. Laver ne donne aucun contrôle sur le bon ordre obtenu.

En utilisant la forme normale tournante, nous sommes capables de décrire complètement la restriction de l'ordre standard des tresses au monoïde B_n^{+*}. Le résultat technique clé établit que l'ordre sur B_n^{+*} est une extension `ShortLex` de l'ordre sur B_{n-1}^{+*}.

> **Théorème V.0.1.** *Pour β, β' dans B_n^{+*}, la relation $\beta < \beta'$ est satisfaite si et seulement si le ϕ_n-éclatement de β est plus petit que le ϕ_n-éclatement de β' par rapport à l'extension `ShortLex` de l'ordre $<$ sur B_{n-1}^{+*}.*

La démonstration de ce résultat requiert une analyse précise de la forme normale tournante et n'est pas simple. Le principe de l'argument consiste à introduire un nouvel ordre $<^*$ sur B_n^{+*}, appelé *ordre tournant*, puis à déterminer un représentant σ-positif de la tresse quotient $\beta^{-1}\beta'$ lorsque les tresses β et β' de B_n^{+*} satisfont la relation $\beta <^* \beta'$. Nous utilisons alors l'algorithme de renversement introduit à la section II.3 (qui est aussi utilisé pour la démonstration du théorème IV.3.17). Afin de simplifier le travail nous le décomposons en plusieurs étapes. Pour cela nous introduisons une suite de tresses $\widehat{\delta}_{n,b}$ jouant le rôle de séparateurs pour l'ordre $<^*$ (voir figure 7).

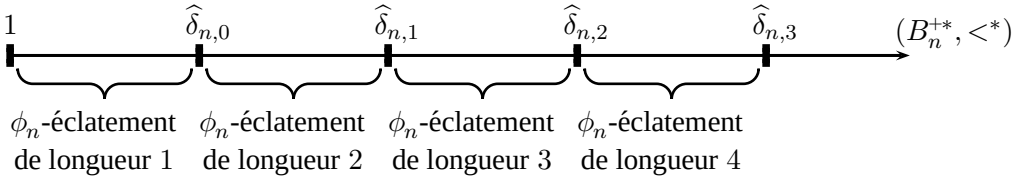


FIG. 7 : La tresse $\widehat{\delta}_{n,b}$ comme séparateur dans $(B_n^{+*}, <^*)$.

Nous démontrons le théorème V.0.1 lorsque la tresse β ou la tresse β' est un séparateur. Puis nous utilisons une induction sur le nombre de brins pour obtenir le résultat général. Nous insistons sur le fait que la démonstration donnée est complète et ne nécessite pas de résultats annexes. En particulier, contrairement au théorème I.3.17 portant sur le bon ordre $(B_n^+, <)$, elle ne requiert pas de recours aux résultats de S. Burckel ou tout autre induction transfinie.

Le théorème V.0.1 redémontre le résultat de R. Laver pour B_n^{+*}, et donne plus, à savoir une détermination de la longueur du bon d'ordre ainsi obtenu.

Corollaire V.1.13. *La restriction de $<$ à B_n^{+*} est un bon ordre de longueur $\omega^{\omega^{n-2}}$.*

Le problème de conjugaison

Jusqu'ici, il n'existait pas vraiment de tentative d'utilisation de l'ordre des tresses afin d'étudier le problème de conjugaison. Une des raisons évidentes est que l'ordre des tresses n'est pas invariant à droite, donc pas invariant par conjugaison. Une autre raison est que l'ordre des tresses est un objet compliqué, sur lequel nous n'avons seulement qu'un contrôle partiel. Ce qui est nouveau est que, avec la forme normale alternante, même plus, avec la forme normale tournante, nous avons maintenant un meilleur moyen de contrôler cet ordre et d'étudier ses connections avec d'autre structures. Ce qui suit est un regroupement d'observations vraiment préliminaires, mais apparemment prometteuses, sur le lien entre l'ordre des tresses et le problème de conjugaison des tresses. C'est un travail en commun avec V. Gebhardt.

Pour β une tresse de B_n^{+*}, on note $C^{+*}(\beta)$ la famille de toutes les tresses $\gamma^{-1}\beta\gamma$, avec γ dans B_n^{+*}, appartenant à B_n^{+*}. Comme la restriction de l'ordre standard des tresses à B_n^{+*} est un bon ordre, l'ensemble non vide $C^{+*}(\beta)$ contient un unique élément $<$-minimal qui est noté $\mu^*(\beta)$ dans la suite.

En utilisant la structure de Garside de B_n^{+*}, on vérifie facilement que deux tresses β et β' de B_n^{+*} sont conjuguées si et seulement si la fonction μ^* prend la même valeur en β et β', et que construire un algorithme calculant la fonction μ^* sur B_n^{+*} donne une solution au problème de conjugaison sur B_n, avec la même complexité dès que la dernière est au moins quadratique. Réciproquement, la solution au problème de conjugaison décrite dans [GMG08] peut être utilisée en pratique pour calculer la fonction μ^*, en temps exponentiel.

Notre présent travail, qui est encore en cours, consiste à essayer de calculer, ou du moins d'étudier la fonction μ^* en utilisant la forme normale tournante. L'expérimentation sur ordinateur est facile, spécialement dans le cas de B_3^+, et amène à quelques conjectures liant la fonction μ^* et la forme normale tournante. Pour le moment, le seul résultat non trivial que nous avons est le suivant :

Proposition V.3.11. *Pour toute tresse β de B_3^{+*}, on a $b(\beta) - 5 \leqslant b(\mu(\beta)) \leqslant b(\beta)$, où $b(\gamma)$ désigne la longueur du ϕ_3-éclatement de γ.*

Ce résultat est loin d'être une description complète de μ^*, mais il restreint sévèrement l'intervalle où $\mu^*(\beta)$ peut exister : la conjugaison ne peut pas trop changer la longueur des ϕ_n-éclatements.

La prochaine étape devrait établir un lien entre les valeurs de μ^* pour des tresses suffisamment proches—ce qui pourrait donner un procédé de calcul par induction. Aucun résultat ne méritant d'être mentionné n'a été démontré pour le moment, mais, comme conclusion, nous mentionnons la conjecture suivante soutenue par l'expérimentation sur ordinateur :

Conjecture V.3.12. *Pour toute tresse β de B_3^{+*}, on a $\mu(\delta_3^3\,\beta) = \delta_3^3\,a_{1,2}^{-3}\,\mu(\beta)\,a_{1,2}^3$.*

Nous rappelons que δ_3^3 est égale à Δ_3^2, un générateur du centre de B_3. Nous conjecturons aussi une formule similaire, $\mu(\Delta_3^2) = \Delta_3^2\sigma_1^{-2}\,\mu(\beta)\sigma_1^2$, où μ est une adaptation de μ^* à B_n^+, mais, pour les raisons listées précédemment, il semble plus évident de démontrer la conjecture pour B_3^{+*} que pour B_3^+.

ORGANISATION DU TEXTE

La rédaction de la thèse suit l'ordre des résultats décrits ci-dessus. Le chapitre I est introductif et est consacré à des rappels sur les groupes des tresses et l'ordre qu'on peut y définir. En particulier, on rappelle ce qu'est une présentation, un ordre invariant à gauche, un bon ordre, etc. Le chapitre II est aussi introductif et est consacré à l'introduction et à l'étude des monoïdes de tresses duaux. En particulier, on décrit la structure de Garside de B_n^{+*} en terme de partitions non croisées et on montre que B_n est le groupe de fractions de B_n^{+*} à l'aide du procédé dit de *retournement*. Le chapitre III est consacré à la forme normale tournante. On commence d'abord par en donner une construction à partir de l'opération dite du ϕ_n-éclatement. Ensuite, on établit certaines contraintes portant sur les mots tournants. Enfin, on donne une caractérisation des mots tournants, en particulier on montre qu'ils forment un langage régulier. Le chapitre IV est consacré à la démonstration de la conjecture assurant l'existence pour toute tresse d'un représentant σ-défini quasi-géodésique. Dans le chapitre V, on étudie la restriction de l'ordre des tresses aux monoïdes de tresses duaux.

English introduction

In this thesis we investigate some combinatorial properties of braid groups. More specifically, we study the Birman–Ko–Lee braid monoids (or dual braid monoids) and the standard braid ordering (or Dehornoy ordering).

GENERAL FRAMEWORK AND PREVIOUSLY KNOWN RESULTS

We first briefly review the existing literature about braid groups, with a special emphasis on the algebraic aspects that will be developed in our work.

History of braid groups

It seems that the first reference where braid groups are explicitly considered and investigated is a text by E. Artin that was published in 1925 [Art25] and reappeared in a slightly different form in [Art47]. However, the notion of a braid and several related ideas can be traced back to the XIXth century, in works by A. Hurwitz, F. Klein, H. Poincaré, B. Riemann, and certainly some other authors. It has been mentioned that a braid scheme can be found in a notebook of C.F. Gauß [Gau].

Braids have been the subject of many research works in the recent years, in particular because they are sufficiently simple to allow relatively simple proofs and, at the same time, they are complicated enough to give rise to deep results. A major breakthrough has been the discovery by V. Jones around 1984 [Jon87] of a deep connection between braid groups, operator theory, statistical mechanics, and other notions from physics. More recently, D. Krammer [Kra00, Kra02] and S. Bigelow [Big01] proved they are linear, *i.e.*, they admit a faithful representation in a finite-dimensional vector space.

On the other hand, many generalizations of braid groups have been fruitfully introduced. From 1966, J. Tits defined and investigated a braid group for each Coxeter group in [Tit66]. This study was then pursued by P. Deligne in [Del72] and E. Brieskorn together with K. Saito in [BS72]. In 1998, M. Broué, G. Malle and R. Rouquier extended the framework further by investigating braid groups associated with complex reflection groups [BMR98]. In 1999, P. Dehornoy and L. Paris introduced the notion of a Garside group [DP99], an abstract version of the approach developed by F. A. Garside for braid groups in [Gar69].

Originally, the group B_n of n-strand braids was defined as the group of isotopy classes of n-strand geometric braids. An algebraic presentation was established by Artin in [Art25], which is the startpoint of this work. So, for us, B_n will be the group that admits the presentation

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

So an n-strand braid is an equivalence class consisting of (infinitely many) words in the letters $\sigma_i^{\pm 1}$. Such words will be called *braid words*. We shall often refer to the letters σ_i as to the

Artin generators. The standard correspondence between the elements of the presented group B_n and geometric braids consists in using σ_i as a code for the geometric braid where the ith and the $(i+1)$st strands cross, with the strand originally at position $(i+1)$ in front of the other.

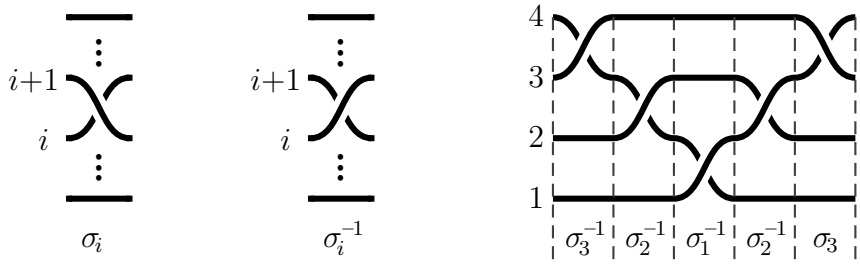


Figure 8 : Interpretation of a word in the letters $\sigma_i^{\pm 1}$ as a geometric braid diagram.

Braid ordering

The theory of orderable groups has been developed for about a century. The most famous result about orderable groups is probably a theorem in 1902 by O.L. Hölder [Höl01] that characterizes the additive group $(\mathbb{R}, +)$ as the unique maximal orderable group satisfying the Archimedian property.

A group G is called *left-orderable* if there exists a linear ordering $<$ of G that is left-invariant, *i.e.*, $g < h$ implies $fg < fh$ for all f, g, and h in G. As for the braid group B_n, the ordering discovered by Dehornoy in [Deh94] is easily described in terms of braid words of a particular type:

> **Theorem I.3.9.** (P. Dehornoy, [Deh94]) *Let us say that $\beta < \beta'$ holds if the quotient-braid $\beta^{-1}\beta'$ can be represented by a σ-positive braid word,* i.e., *a braid word in which the generator σ_i with maximal i occurs positively only, in the sense that σ_i occurs, but σ_i^{-1} does not. Then the relation $<$ is a left-invariant linear ordering on B_n for all n.*

The fact that the relation $<$ is a left-invariant linear ordering relies on the following two properties. We say that a braid word is *σ-negative* if its inverse is σ-positive, and that a braid word is *σ-definite* if it is either σ-positive or σ-negative. In other words a braid word is σ-definite if the generator σ_i with the highest index i occurs positively only, or negatively only.

Property A. A braid that admits a σ-definite expression is non-trivial.

Property C. Every non-trivial braid admits a σ-definite expression.

Both properties were established in [Deh94] using methods of self-distributive algebra. They were given a new proof by D. Larue in [Lar94] using the so-called Artin representation of braids in terms of automorphisms of a free group. Subsequently, by 1999, R. Fenn, M. Greene, D. Rolfsen, C. Rourke, and B. Wiest used topological methods in [FGR$^+$99] to reconstruct an order on B_n viewed as the mapping class group of an n-punctured disk. Their method is a geometrical version of Larue's approach, and the remarkable point is that the ordering it leads to coincides with the one of Theorem I.3.9. Still many more proofs of Properties A and C have been proposed in further works, based on various approaches. We refer to [DDRW02, DDRW08].

On the other hand, in 2000, B. Wiest and H. Short constructed in [SW00] a whole family of left-invariant linear orderings on B_n relying on the hyperbolic geometry of the universal cover of the punctured disk, following an approach that goes back to W. Thurston and even to J. Nielsen in [Nie27]. We refer to [Ito08, Ito09] for a combinatorial description of some of these orders. It is now known that the space of all left-invariant orderings on B_n has quite interesting properties, see [Nav07].

Sigma-definite expressions

As mentioned above, the key point in the existence of the standard braid order is Property **C**, which states that every non-trivial braid admits at least one σ-definite expression, *i.e.*, an expression in which the generator σ_i with the highest index i occurs positively only, or negatively only. Independently of any order question, this property is a fundamental result about braids (it may be noted that it does not extend to generalized braid groups associated with Coxeter groups of types other than A and B, see [Sib03]).

In the past twenty years, at least five or six different proofs of this result have been proposed. They rely on very different approaches. As we say, the first one, by P. Dehornoy in 1992, uses self-distributive algebra. The next one, by D. Larue [Lar94], uses the Artin representation of braids as automorphisms of a free group, an argument that was subsequently rediscovered independently by R. Fenn, M. Greene, D. Rolfsen, C. Rourke and B. Wiest [FGR$^+$99] in a more topological setting. A completely different proof relying on the geometry of the Cayley graph of B_n appears in [Deh97a]. There also exist at least two proofs based on relaxation algorithms, which are strategies designed to progressively make simpler and simpler a (family of) curve(s) drawn in a disk and deformed under the action of a braid viewed as a homeomorphism of that disk. One is described by I. Dynnikov and B. Wiest in [DW07], another by X. Bressaud in [Bre08].

All the above methods are effective and lead to practical algorithms. However, in terms of time and space complexity, none has been proved to be simpler than exponential. In particular, the only proved upper bound for the length of the final σ-definite word equivalent to an initial word of length ℓ is exponential in ℓ. On the other hand, some methods are known to be extremely efficient in practice, and the following conjecture belongs to the folklore of the domain:

> **Conjecture IV.0.1.** *For each n, there exists a constant C_n such that, for each n-strand braid word w of length ℓ, there exists an equivalent σ-definite word of length at most $C_n\ell$.*

In other words, the conjecture claims that every braid admits a quasi-geodesic expression that is σ-definite.

The well-order property

The monoid of positive n-strand braids, denoted B_n^+, is the submonoid of the group B_n generated by σ_1, ..., σ_{n-1}. It consists of those braids that can be represented by a positive braid word, *i.e.*, a word containing no letter σ_i^{-1}. By the results of F.A Garside [Gar69], the monoid B_n^+ admits, as a monoid, the presentation (2) given above to introduce the braid group B_n.

Restricting the standard braid ordering to the submonoid B_n^+ of B_n obviously yields a left-invariant linear ordering of B_n^+. Moreover, this restriction enjoys remarkable additional properties.

A linear order $\prec$ on a set X is said to be a *well-order* if every non-empty subset of X admits a minimal element with respect to $\prec$. Up to a weak form of the axiom of choice, this is equivalent to saying that there is no infinite $\prec$-descending sequence in X.

Clearly, for $n \geqslant 2$, the set B_n equipped with the standard braid order is not a well-order, since it contains the infinite descending sequence $1, \sigma_1^{-1}, \sigma_1^{-2}$, ... However, in 1996, R. Laver showed in [Lav96] that, for each n, the restriction of the braid order to the monoid B_n^+ is a well-order.

One of the nice properties of well-orders is that, contrary to an arbitrary linear order, a well-order is completely determined by a unique parameter, namely its length, which is usually specified using an ordinal. We recall that ordinals make an extension of the sequence of natural numbers in the transfinite realm. For instance, the first infinite ordinal ω is the least upper bound of the natural numbers. The next ordinal is $\omega + 1$, then comes $\omega + 2$, etc. For our current purpose, it is enough to mention that the ordinals are equipped with a canonical linear order that is a well-order, and with arithmetic operations, addition, multiplication, exponentiation, that extend those of natural numbers and share some (but not all) of their properties. For more results about ordinals, see for instance [Lév79].

Based on Higman's lemma, Laver's proof for the result that $(B_n^+, <)$ is a well-order is non-effective, and it gives no way of determining the length. The latter was determined by S. Burckel in his PhD thesis [Bur94], and in the subsequent journal article [Bur97]:

Theorem I.3.17. (S. Burckel, [Bur97]) *The restriction of the braid order $<$ to B_n^+ is a well-order of length $\omega^{\omega^{n-2}}$.*

Burckel's proof relies on a transfinite inductive argument that is extremely tricky and remains very difficult to control in practice.

The alternating normal form

By definition, a braid is an equivalence class of braid words. Various *normal forms* have been described in literature, *i.e.*, various ways of selecting, for each braid, a distinguished word that represents it. The so-called *alternating normal form* is one such normal form. It is defined for positive braids only. It was introduced in 2008 by P. Dehornoy in [Deh08].

The construction of the alternating normal form relies on an operation called Φ_n-*splitting* that associates to each positive n-braid a finite sequence of positive $(n-1)$-strand braids that determines it completely.

To give a precise description, we have to introduce the right-divisibility relation in the monoid B_n^+. For β, γ in B_n^+, we say that γ is a *right-divisor* of β, or, equivalently, that β is a *left-multiple* of γ if there exists a positive braid β' in B_n^+ satisfying $\beta = \beta' \gamma$. It is known that B_n^+ equipped with the right-divisibility relation has the structure of a lattice, *i.e.*, any two positive braids admit a unique greatest common right-divisor (or right-gcd) and a unique least common left-multiple (or left-lcm). This is one of the ingredients of the so-called *Garside structure* of the monoid B_n^+. Another ingredient is the result that the left-lcm Δ_n of the Artin generators $\sigma_1, ..., \sigma_{n-1}$ is also their right-lcm. This implies that the inner automorphism Φ_n of the group B_n associated with Δ_n preserves the monoid B_n^+, and, therefore, Φ_n induces an isomorphism of the monoid B_n^+. Moreover, Φ_n preserves (left- and) right-divisibility, hence it

preserves the operations of gcd's and lcm's. One easily checks that Φ_n exchanges σ_i and σ_{n-i} for each i, so, geometrically, Φ_n corresponds to a symmetry in terms of braid diagrams.

Proposition III.1.22. (P. Dehornoy, [Deh08]) *For each non-trivial braid β of B_n^+ with $n \geqslant 3$, there exists a unique finite sequence $(\beta_b, \dots, \beta_1)$ of braids of B_{n-1}^+ with $\beta_b \neq 1$ satisfying the relation $\beta = \Phi_n^{b-1}(\beta_b) \cdot \dots \cdot \Phi_n(\beta_2) \cdot \beta_1$ and such that, for each k, the braid β_k is the maximal right-divisor of $\Phi_n^{b-k}(\beta_b) \cdot \dots \cdot \Phi_n(\beta_{k+1}) \cdot \beta_k$ that belongs to B_{n-1}^+.*

Under the above hypotheses, the sequence $(\beta_b, \dots, \beta_1)$ is called the Φ_n-*splitting* of the positive braid β. The entries of a Φ_n-splitting are numbered from right to left in order to emphasize the fact that the construction starts from the right and relies on taling the maximal right-divisor at each step.

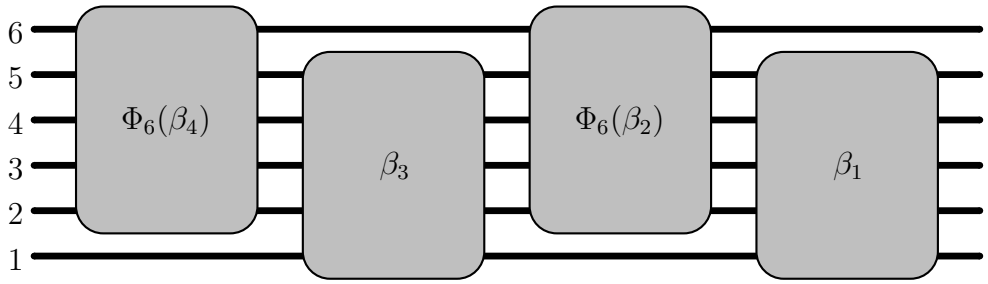


Figure 9 : Starting from a braid β of B_6^+, we extract the maximal right-divisor of β keeping the sixth strand unbraided, then we extract the maximal right-divisor of the remaining braid keeping the first strand unbraided, etc.

The main result of [Deh08] is an inductive description of the braid order on B_n^+ in terms of order on B_{n-1}^+ and of Φ_n-splittings. The precise result is as follows.

Theorem III.1.26. (P. Dehornoy, [Deh08]) *For β, β' in B_n^+, the relation $\beta < \beta'$ is true if and only if the Φ_n-splitting of β is smaller than the Φ_n-splitting of β' with respect to the* `ShortLex`*-extension of the order on B_{n-1}^+.*

We recall that, if $(X, \prec)$ is an ordered set, and s, s' are finite sequences of elements of X, then s is said to be `ShortLex`-smaller than s' if the length of s is smaller than the length of s', or the lengths are equal and s is smaller than s' for the lexicographical extension of $\prec$, *i.e.*, starting from the left, the first entry of s that is not equal to its counterpart in s' is $\prec$-smaller.

It may be noted that the connection between the Φ_n-splitting and the braid order established in [Deh08] relies on Burckel's results. Therefore, this approach does not reprove the latter, but rather gives an alternative description of these results.

Dual braid monoids

In 1998, J.S. Birman, K.H. Ko, and S.J. Lee [BKL98] introduced and investigated for each n a new submonoid B_n^{+*} of B_n. This monoid is known as the *Birman–Ko–Lee* monoid. The name "*dual braid monoid*" was subsequently proposed because several numerical parameters

obtain symmetric values when evalutated in B_n^+ and in B_n^{+*}, a correspondence that was extended to the context of more general Artin–Tits groups by D. Bessis in 2003 [Bes03].

We recall that the positive braid monoid B_n^+ is the submonoid of B_n generated by the elements σ_1, ..., σ_{n-1}, where, geometrically, σ_i corresponds to the crossing of the ith and $(i+1)$st strands. The dual braid monoid B_n^{+*} is the submonoid of B_n that is generated by the braids $a_{i,j}$ with $1 \leqslant i < j \leqslant n$, where $a_{i,j}$ is defined by $a_{i,j} = \sigma_i \dots \sigma_{j-1}\ \sigma_j\ \sigma_{j-1}^{-1} \dots \sigma_i^{-1}$. In geometrical terms, the braid $a_{i,j}$ corresponds to a crossing of the ith and jth strand, both passing behind the (possible) intermediate strands. By definition, σ_i equals $a_{i,i+1}$ and, therefore, the monoid B_n^+ is

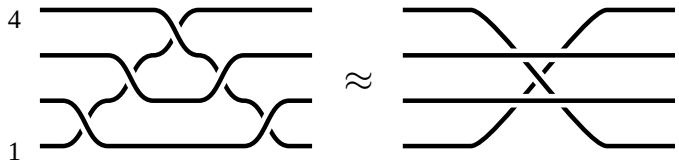


Figure 10 : In the geometric braid $a_{1,4}$, the strands 1 and 4 cross under the strands 2 and 3.

included in the monoid B_n^{+*}, a proper inclusion for $n \geqslant 3$ since the braid $a_{1,3}$ does not belong to the monoid B_3^+.

It is known [BKL98] that the dual braid monoid B_n^{+*} admits a Garside structure similar to that of B_n^+. So, in particular, any two elements of B_n^{+*} admit left- and right-gcd's and lcm's. The role of the Garside element Δ_n is played in the case of B_n^{+*} by the element δ_n defined to be $a_{1,2}\, a_{2,3} \dots a_{n-1,n}$, *i.e.*, $\sigma_1\, \sigma_2 \dots \sigma_{n-1}$.

The connection between the monoid B_n^{+*} and the symmetric group $\mathfrak{S}_n$ has been investigated further in [Bra01] and in [Bes03]. Connections with the nth roots of unity and Springer's theory appear in [BDM02].

The Conjugacy Problem

The Conjugacy Problem of the braid group B_n is the problem of deciding whether two braids β, β' of B_n are conjugate, *i.e.*, whether there exists a braid γ in B_n satisfying $\beta' = \gamma^{-1}\, \beta\, \gamma$.

After the work of F.A. Garside [Gar69], it is known that the Conjugacy Problem is algorithmically solvable. At the moment, all known solutions are exponential in complexity. This is the case for Garside's original solution, as well as for the many successive improvements described by E.A. El-Rifai and H. R. Morton in [ERM94], by N. Franco and J. González-Meneses in [FGM03], and by J. González-Meneses and V. Gebhardt in [GMG08].

All the above solutions rely on the Garside structure of the braid group B_n, either the one associated with the monoid B_n^+ and Δ_n, or the one associated with the dual monoid B_n^{+*} and δ_n.

RESULTS OF THIS WORK

Here we establish new combinatorial results involving braids and, more specifically, the dual braid monoids B_n^{+*} and the standard braid order. Our main tool is a new normal form, called the *rotating normal form*.

The rotating normal form

The starting point for the construction of the alternating normal form in the monoid B_n^+ is the observation that every braid of B_n^+ admits a unique maximal right-divisor lying in B_{n-1}^+. A similar property holds in the case of the dual braid monoids B_n^{+*} and B_{n-1}^{+*}. It is therefore quite natural to look for a counterpart to the alternating normal form.

As recalled above, the dual braid monoid B_n^{+*} is equipped with a Garside structure, in which the role of Δ_n is played by δ_n. It follows that the counterpart to the automorphism Φ_n, which is a conjugacy by Δ_n, is now played by an automorphism denoted ϕ_n which is a conjugacy by δ_n. As is well-known, Δ_n^2 belongs to the center of B_n, and the autormorphism Φ_n is an involution, which corresponds geometrically to the fact that Φ_n induces a symmetry on braid diagrams. By contrast, the smallest power of δ_n that lies in the center of B_n is δ_n^n, so that the automorphism ϕ_n has order n. In particular, we find $\phi_n(a_{i,j}) = a_{i+1,j+1}$ for $j \leqslant n-1$ and $\phi_n(a_{i,n}) = a_{1,n+1}$. Geometrically, ϕ_n should be viewed as a rotation, which makes sense provided braid diagrams are drawn on a cylinder rather than on a plane rectangle.

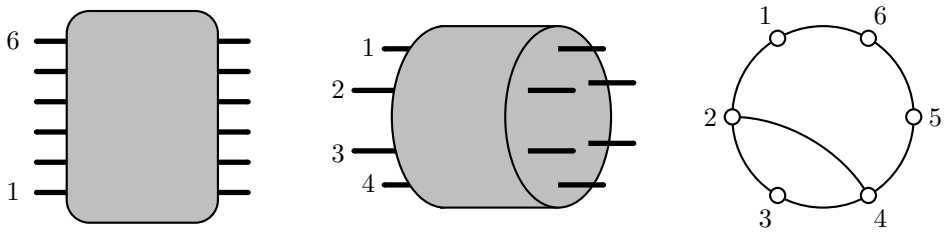


Figure 11 : Rolling up the usual braid helps us to vizualize the symmetries of the braids $a_{p,q}$. On the resulting cylinder, $a_{p,q}$ naturally corresponds to the chord connecting the vertices p and q.

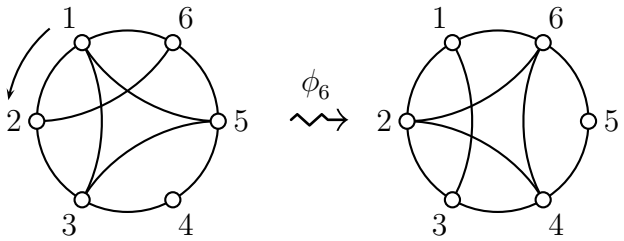


Figure 12 : Representation of the automorphism ϕ_n as a reverse clockwise rotation of the marked circle by $\frac{2\pi}{n}$.

Our first result is a counterpart to the construction of the alternating form in the dual braid monoid B_n^{+*}.

Proposition III.2.7. *For every non-trivial braid β of B_n^{+*} with $n \geqslant 3$, there exists a unique finite sequence $(\beta_b, \dots, \beta_1)$ of braids of B_{n-1}^{+*} with $\beta_b \neq 1$ satisfying the relation $\beta = \phi_n^{b-1}(\beta_b) \cdot \dots \cdot \phi_n(\beta_2) \cdot \beta_1$ and such that, for each k, the braid β_k is the maximal right-divisor of the braid $\phi_n^{b-k}(\beta_b) \cdot \dots \cdot \phi_n(\beta_{k+1}) \cdot \beta_k$ lying in B_{n-1}^{+*}.*

Under the above hypotheses,the sequence$(\beta_b, \dots, \beta_1)$ is called the ϕ_n-*splitting* of the braid β.

The proof of this result uses the standard Garside properties of B_n^{+*}, and it is not really difficult once the correct definition has been formulated.

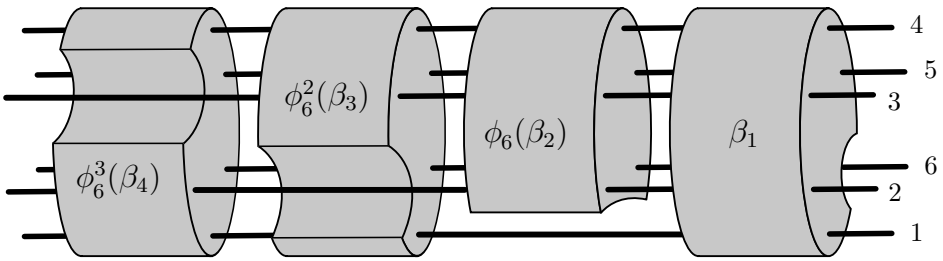


Figure 13 : The ϕ_6-splitting of a braid of B_6^{+*}. Starting from the right, we extract the maximal right-divisor that keeps the sixth strand unbraided, then extract the maximal right-divisor that keeps the first strand unbraided, etc.

Using the ϕ_n-splitting procedure inductively, we deduce an expression of each braid of B_n^{+*} in terms of (images of) braids of B_2^{+*}, *i.e.*, of powers of $a_{1,2}$. We define a word homomorphism, still denoted ϕ_n that maps the letter $a_{i,j}$ with $j \leqslant n-1$ to $a_{i+1,j+1}$ and the letter $a_{i,n}$ to $a_{1,i+1}$.

Definition III.2.12. For β in B_n^{+*}, we define *the rotating normal form* of β by
– for $n = 2$, the unique power of $a_{1,2}$ representing β;
– for $n \geqslant 3$, the word $\phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1$, where $(\beta_b, \ldots, \beta_1)$ is the ϕ_n-splitting of β and w_k is the rotating normal form of β_k.

The rotating normal form turns out to be a very convenient tool for investigating the dual braid monoid B_n^{+*}—and, from there, the braid group B_n which is a group of fractions for B_n^{+*}. It seems that one of the main advantages of using the monoid B_n^{+*} and the rotating normal form when compared with using the monoid B_n^+ and the alternating normal form is that many relations connect the generators $a_{i,j}$ (which make a highly redundant family of generators for the braid group). It follows that distinguishing a specific expression is, in some sense, more difficult in B_n^{+*} than in B_n^+, but, then, it is also potentially more powerful. Whatever the reasons are, the point is that we shall be able to establish for the rotating normal form many specific properties which have no known counterpart in the case of the alternating normal form.

A typical result in this direction is the following characterization of those sequences in B_{n-1}^{+*} that are ϕ_n-splittings. Let us say that a letter $a_{r,s}$ is a $a_{p,n}$-barrier if we have both $r < p$ and $p < s$.

Theorem III.4.4. *A finite sequence $(\beta_b, \ldots, \beta_1)$ of braids in B_{n-1}^{+*} is the ϕ_n-splitting of a braid in B_n if and only if the following conditions are satisfied:*
– *we have $\beta_k \neq 1$ for $k \geqslant 3$;*
– *no non-trivial braid of B_{n-1}^{+*} right-divides $\phi_n(\beta_k)$ for $k \geqslant 2$;*
– *for each $k \geqslant 3$, if β_k is right-divisible by $a_{p-1,n-1}$, then some/any expression of β_{k-1} contains an $a_{p,n}$-barrier.*

The proof of this result requires using the notion of a *ladder* that is developed in Section III.3.3, as well as some (rather standard) properties of the so-called reversing method for the Birman-Ko-Lee presentations of the dual braid monoids, which are stated in Section II.3.

Let us call *n-strand rotating word* every word on the letters $a_{i,j}$ that is the rotating normal form of braid of B_n^{+*}. Theorem III.4.4 implies:

Corollary III.4.31. *For each n, the family of all n-strand rotating words is a regular language.*

More precisely, we obtain an inductive construction of a finite state automaton that recognizes the language of rotating words.

Sigma-definite expressions

The main result of this thesis is a proof of Conjecture IV.0.1, which is about the existence of a quasi-geodesic σ-definite expression. For a braid β, let us denote by $\|\beta\|_\sigma$ the geodesic length of β with respect to the Artin generators σ_i, *i.e.*, the length of the shortest expression of β by a word in the letters $\sigma_i^{\pm 1}$. Then we prove

Theorem IV.3.17. *Every n-strand braid β admits a σ-definite expression of length at most $6(n-1)^2\|\beta\|_\sigma$.*

The above result is essentially optimal: it is known that a braid does not need to admit a geodesic σ-definite expression, and, more precisely, that one could not hope for better than an upper bound $C_n\|\beta\|_\sigma$ with C_n at least linear in n. More precisely B. Wiest has shown that the n-strand braid

$$\sigma_{n-1}\sigma_{n-2}^{-2}\sigma_{n-3}^{2}\sigma_{n-4}^{-2}\ldots\sigma_1^{2e}\sigma_2^{2e}\sigma_3^{-2e}\ldots\sigma_{n-2}^{2}\sigma_{n-1}^{-1},$$

with $e = \pm 1$ in function of the parity of n, admits no σ-definite expression of length smaller than $(n-2)(n-1)$. As the above word has length $4(n-2)$, the constant C_n must increase linearly in n: $C_n \geqslant (n+1)/4$.

By the way, the quadratic factor $(n-1)^2$ in Theorem IV.3.17 comes from a final translation step from the Birman–Ko–Lee generators to the Artin ones. If we consider the analogous problem involving the generators $a_{i,j}$, then, denoting by $\|\beta\|_a$ the geodesic length of β with respect to the Birman–Ko-Lee generators, we have:

Théorème IV.3.16. *Every n-strand braid β admits a σ-definite expression of length at most $3(n-1)\|\beta\|_a$.*

The principle of the proof of Theorem IV.3.17 is as follows. We start with an arbitrary braid β of B_n, and aim at finding a σ-definite expression of β. We proceed in several steps. The first step consists in expressing β as a fraction $\delta_n^{-t}\,\beta'$, where we recall δ_n to be the standard Garside element of B_n^{+*}, and where β' belongs to B_n^{+*}. This is possible because B_n is a group of fractions for B_n^{+*}.

If the exponent t is larger than the length of the ϕ_n-splitting of β', then the σ-negative factor δ_n^{-t} wins against the σ-positive factor β, and it is easy to obtain a σ-negative word representing β by a direct computation that amounts to placing one factor δ_n^{-1} between any two adjacent entries of the ϕ_n-splitting of β'.

Otherwise, if the exponent t is at most equal to the length of the ϕ_n-splitting of β', one determines the rotating normal form w of β', and one tries to obtain a σ-positive word representing β by pushing the negative factor δ_n^{-t} to the right through w. The problem is that certain σ-negative words with a particular form, hereafter called *dangerous*, appear at each step of the process. The crucial point is to use the specific properties of rotating normal words to keep the dangerous fragments under control. The basic step consists in swapping a dangerous word and a rotating normal word. To this end, we introduce a procedure called reversing, which is similar to (but different from) the standard subword reversing method mentioned above. Technically, the hard point is to prove that the reversing procedure actually fulfills all requirements it is supposed to. This is done by introducing the notion of *wall*, which is a weakening of the ladders of Section III.3.3. The three main results are that every rotating normal word is a ladder, that the product of a (fragment of) dangerous word and a ladder is a wall, and that the product of a (fragment of) a wall and a ladder is again a wall. The proof of Theorem IV.3.17 is effective, and it leads to a tractable algorithm. The complexity analysis of the algorithm gives:

Theorem IV.3.18. *The time complexity of the algorithm involved in the proof of Theorem IV.3.17 is quadratic: for each n-strand braid word w of length ℓ, the total running time of the algorithm on w lies in $O(\ell^2)$.*

As was said above, the proof of Theorem IV.3.17 is completely self-contained. So, in particular, it provides one more proof of Property **C**, *i.e.*, the existence of a sigma-definite expression for each non-trivial braid. One may argue that this proof is the best one known so far, since it is the only one that provably leads to an (almost) optimal σ-definite expression.

On the other hand, if one takes Property **C** for granted and one only wishes to obtain a short σ-definite expression, then, as was suggested by L. Paris, one can design a new algorithm that is simpler than the one of Theorem IV.3.18: using the trick of X. Bressaud in its relaxation algorithm [Bre08], one runs the algorithm of Theorem IV.3.18 on β and β^{-1} in parallel; the easy case of Theorem IV.3.17 is then sufficient to provide a σ-definite expression either for β or for β^{-1}, which in turn is enough to conclude. In this way, one proves:

Theorem IV.3.16. *Every n-strand braid β admits a σ-definite expression in the letters σ_i of length at most $2(n-1)^2\|\beta\|_\sigma$ and a σ-definite expression in the lettres $a_{p,q}$ of length at most $(n-1)\|\beta\|_a$.*

The well-order on B_n^{+*}

Another consequence of Laver's result is that the restriction of the braid order to the dual braid monoid B_n^{+*} is a well-order. As in the case of the monoid B_n^+, Laver's approach gives no control of the well-order so obtained.

By using the rotating normal form, we shall be able to completely describe this restriction of the standard braid order to the monoid B_n^{+*}. The key technical result states that the order on B_n^{+*} is a `ShortLex`-extension of the order on B_{n-1}^{+*}.

Theorem V.0.1. *For β, β' in B_n^{+*}, the relation $\beta < \beta'$ is true if and only if the ϕ_n-splitting of β is smaller than the ϕ_n-splitting of β' with respect to the `ShortLex`-extension of the order $<$ on B_{n-1}^{+*}.*

The proof of this result requires a precise analysis of the rotating normal form and the argument is not simple. However, we insist that the proof given below is complete and self-contained. In particular, contrary to Theorem I.3.17 about the order on B_n^+, it requires no use of Burckel's results or of any transfinite induction.

The principle of the argument consists in introducing the so-called *rotating ordering* $<^*$ on B_n^{+*} that corresponds to the expected inductive characterization of the braid ordering, and to establish enough properties of $<^*$ to finally deduce that it coincides with the standard braid ordering by determining a σ-positive expression for the quotient-braid $\beta^{-1}\beta'$ whenever $\beta <^* \beta'$ holds. To this end, as in the proof of Theorem IV.3.17, we use the reversing method of Section II.3.

To make the argument more easily understandable, we split the proof into several steps, and we introduce certain braids $\widehat{\delta}_{n,b}$ that play the role of landmarks (or separators) with respect to the order $<^*$ (see figure 14).

Theorem V.0.1 is first established in the case when β or β' is a separator $\widehat{\delta}_{n,b}$, using an induction on the length of the ϕ_n-splittings of the involved braids. The general case then follows using an induction on the braid index.

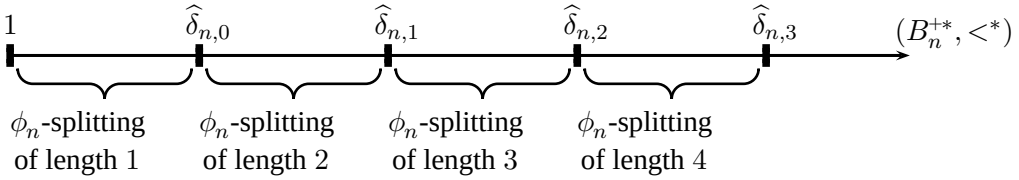


Figure 14 : The braid $\widehat{\delta}_{n,b}$ as a separator in $(B_n^{+*}, <^*)$.

Theorem 1 easily gives a new proof of Laver's result for B_n^{+*}, and even more, namely a determination of the length of the well-order so obtained.

Corollary V.1.13. *The restriction of the standard braid order to B_n^{+*} is a well-order of length $\omega^{\omega^{n-2}}$.*

The Conjugacy Problem

So far there have been no real attempts to use the standard braid order to investigate conjugacy in braid groups. One obvious reason is that the braid order is not right-invariant, hence not invariant under conjugacy, making most of the naive attempts unfruitful. Another related reason is that the braid order is a complicated object, of which we have only a very partial control. What is new is that, with the alternating normal form, and even more, with the rotating normal form, we now have a much better way to control this braid order and investigate its connection with other structures. What follows is a report on very preliminary, but seemingly promising, observations about the connection between the braid ordering and the braid Conjugacy Problem. This is a joint work with V. Gebhardt.

For β a braid in B_n^{+*}, let us denote by $C^{+*}(\beta)$ the family of all braids $\gamma^{-1}\beta\gamma$, γ in B_n^{+*}, that lie in B_n^{+*}. As the restriction of the standard braid order to B_n^{+*} is a well-order, the non-empty set $C^{+*}(\beta)$ contains a unique $<$-minimal element, which will be denoted $\mu^*(\beta)$ hereafter.

Using the Garside structure of B_n^{+*}, one easily sees that two braids β, β' of B_n^{+*} are conjugate if and only if the function μ^* takes the same value on β and β', and deduce that any algorithm computing the function μ^* on B_n^{+*} leads to a solution of the Conjugacy Problem on B_n, with the same algorithmic complexity whenever the latter is at least quadratic. Conversely, the solution to the Conjugacy Problem described in [GMG08] can be used to practically compute the function μ^*, in exponential time.

Our current work, which is still in progress, consists in trying to compute or, at least, to investigate the function μ^* using the rotating normal form. Computer experiments are easy, especially in the case of B_3^{+*}, and they lead to several conjectures connecting μ^* and the rotating normal form. At the moment, the only non-trivial result we have is the following one:

Proposition V.3.11. *For every braid β in B_3^{+*}, we have $b(\beta)-5 \leqslant b(\mu^*(\beta)) \leqslant b(\beta)$, where $b(\gamma)$ denotes the length of the ϕ_3-splitting of γ.*

This result is far from a complete determination of the function μ^*, but it severely restricts the interval where $\mu^*(\beta)$ may live: conjugacy cannot change the length of the ϕ_n-splitting too much.

The next step should consist in connecting the values of μ^* on some closely connected braids—so possibly resulting in an inductive computation process. No result worth mentioning has been proved so far, but, as a conclusion, we shall mention the following conjecture, which is vastly supported by computer experiments:

Conjecture V.3.12. *For each braid β in B_3^{+*}, we have $\mu^*(\delta_3^3\,\beta) = \delta_3^3\,a_{1,2}^{-3}\,\mu^*(\beta)\,a_{1,2}^3$.*

We recall that δ_3^3 equals Δ_3^2, a generator of the center of B_3. We also conjecture a similar formula, $\mu(\Delta_3^2\,\beta) = \sigma_2\,\sigma_1^2\,\sigma_2\,\mu(\beta)\,\sigma_1^2$, where μ is the counterpart of μ^* involving B_n^+ instead of B_n^{+*}, but, for the reasons listed above, it seems more likely that the B_3^{+*} conjecture will be more easily proved than its B_3^+ counterpart.

ORGANIZATION OF THE TEXT

The text of the thesis follows the order of the results decribed above. Chapter I is introductory and is devoted to recall the basic defintion of the braid groups B_n and of the braid ordering. In particular, we recall what the presentation of a group is, a left invariant ordering is, a well-ordering is, etc. Chapter II is also introductory and is devoted to the construction and the investigation of the dual braid monoid B_n^{+*}. In particular, we describe the Garside structure of B_n^{+*} in terms of non-crossing partitions and we prove that B_n is the group of fractions of B_n^{+*} using the returning process. Chapter III is devoted to the rotating normal form. We start by giving a construction of this new normal form from the ϕ_n-splitting operation. Next, we establish some constraints satisfied by rotating normal words. Finally, we give a characterization of rotating normal words. In particular, we show that they make a regular language. In Chapter IV we prove the conjecture stating that each braid admits a quasi-geodesic representative. In Chapter V, we investigate the restriction of the standard braid ordering to the dual braid monoids.

I. Groupes de tresses

Dans ce chapitre préparatoire, nous introduisons les groupe de tresses et rappelons les propriétés qui servent de base à cette thèse : présentation de groupes et de monoïdes, ordre des tresses, etc. Tous les résultats mentionnés ici sont classiques et sont souvent donnés sans démonstration ou seulement avec une idée de celle-ci. C'est aussi l'occasion de bien définir le contexte dans lequel on travaillera par la suite.

L'organisation de ce premier chapitre est la suivante : dans la première section, nous rappelons la construction géométrique du groupe de tresses donnée par E. Artin dans [Art25], ainsi qu'une interprétation topologique de ce groupe initiée par J.S Birman dans [Bir74]. Dans la section 2, nous rappelons ce qu'est une présentation de monoïdes et de groupes et donnons une présentation du groupe de tresses B_n, nous redonnons aussi les notions élémentaires portant sur les mots. Finalement, à la section 4, nous rappelons la construction de l'ordre standard des tresses introduit par P. Dehornoy dans [Deh94], ainsi qu'une liste non exhaustive de ses propriétés.

1 Le groupe de tresses B_n

Le groupe de tresses B_n a été initialement introduit d'un point de vue géométrique par E. Artin dans [Art25]. Dans [Art47], E. Artin revient sur les points laissés avec une démonstration intuitive.

1.1 Tresses géométriques

On rappelle ici la définition géométrique du groupe de tresses B_n. On note D^2 le disque unité fermé centré en 0 du plan euclidien $\mathbb{R}^2$ identifié à la droite complexe $\mathbb{C}$, et par P_n l'ensemble de n points marqués distincts de D^2 régulièrement espacés sur l'axe imaginaire.

Définition 1.1. Un *brin de tresse géométrique à n brins* est un plongement continu br de l'intervalle $[0,1]$ dans le cylindre $[0,1] \times D^2$ satisfaisant les propriétés suivantes :
– (i) pour tout t dans $[0,1]$, le point $\mathrm{br}(t)$ appartient à $\{t\} \times D^2$,
– (ii) le point $\mathrm{br}(0)$ appartient à $\{0\} \times P_n$,
– (iii) le point $\mathrm{br}(1)$ appartient à $\{1\} \times P_n$.

Intuitivement, l'ensemble $[0,1] \times D^2$ est un cylindre de $\mathbb{R}^3$. Par convention, on visualise l'intervalle $[0,1]$ horizontalement. Ainsi chaque copie de D^2 se trouve dans un plan Euclidien orthogonal à l'axe des abscisses et les éléments de P_n sont disposés selon l'axe des ordonnées. Un brin de tresse géométrique à n brins est alors un brin « matériel » allant de la gauche vers la droite de manière continue, sans rebroussement reliant un point de $\{0\} \times P_n$ à un point de $\{1\} \times P_n$.

Définition 1.2. Une *tresse géométrique à n brins* est l'ensemble de n brins de tresses géométriques à n brins ne s'intersectant pas.

Les n brins constituant une tresse géométrique tr à n brins ne s'intersectant pas, pour tout élément p de P_n, il existe un unique brin br de tr tel que $\mathrm{br}(0)$ soit $(0, p)$; de même il existe un unique brin br de tr tel que $\mathrm{br}(1)$ soit $(1, p)$. Ainsi chaque point de $\{0\} \times P_n$ est envoyé sur un point de $\{1\} \times P_n$ par la tresse géométrique tr.

Les éléments de P_n sont naturellement ordonnés : on note p_1 le point de P_n le plus bas, c'est-à-dire, celui d'ordonnée minimale lorsque $[0, 1] \times D^2$ est vu dans $\mathbb{R}^3$; on note p_2 le deuxième point le plus bas de P_n, etc. On appelle *k ème brin, ou brin k* d'une tresse géométrique l'unique brin br de tr satisfaisant $\mathrm{br}(0) = p_k$.

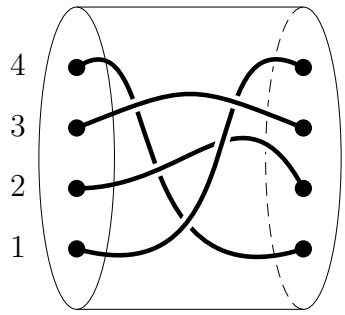


FIG. 1.1 : Exemple de tresse géométrique à 4 brins : les gros points noirs correspondent aux éléments de P_4 (on représente le point p_k par k). Le brin 1 passe devant les brins 4 et 2 puis derrière le brin 3, etc.

Afin de pouvoir définir une structure de groupe sur les tresses nous devons identifier les tresses géométriques à n brins qui sont topologiquement équivalentes. Tout d'abord redonnons la définition d'isotopie d'homéomorphismes d'espaces topologiques.

Définition 1.3. Soient X et Y deux espaces topologiques. Les homéomorphismes f et g de X dans Y sont dits *isotopes* s'il existe une application continue F de $[0, 1] \times X$ dans Y telle que :
– pour tout x dans X, on ait $F(x, 0) = f(x)$ et $F(x, 1) = g(x)$,
– pour tout t dans $[0, 1]$, l'application $x \mapsto F(x, t)$ soit un homéomorphisme de X dans Y.

Nous pouvons maintenant définir l'isotopie de tresses géométriques à n brins.

Définition 1.4. Deux tresses géométriques tr_1 et tr_2 sont dites *isotopes*, et on note $\mathrm{tr}_1 \approx \mathrm{tr}_2$, s'il existe un homéomorphisme h de $D^2 \times [0, 1]$ dans lui même isotope à l'identité envoyant tr_1 sur tr_2 tel que sa restriction à $\{0\} \times D^2$ et à $\{1\} \times D^2$ soit l'identité.

D'une manière plus intuitive, deux tresses sont isotopes l'une à l'autre si on peut transformer l'une en l'autre en bougeant les brins de manière continue, sans intersection et en laissant les extrémités fixes.

1.2 Structure de groupe

On peut naturellement définir un produit sur l'ensemble des tresses géométriques à n brins en utilisant la concaténation : étant données deux tresses géométriques tr_1 et tr_2 à n brins, on écrase l'image de tr_1 sur le cylindre $[0, \frac{1}{2}] \times D^2$, l'image de tr_2 sur le cylindre $[\frac{1}{2}, 1] \times D^2$ et, mettant bout à bout les cylindres obtenus, on définit une nouvelle tresse géométrique à n brins notée $\mathrm{tr}_1 \cdot \mathrm{tr}_2$. Le produit ainsi défini sur les tresses géométriques, ne permet pas d'obtenir une

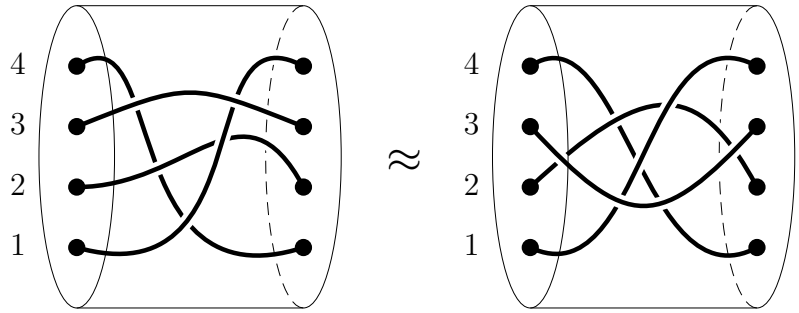


FIG. 1.2 : Isotopie entre deux tresses géométriques à 4 brins : on peut passer de l'une à l'autre à l'aide de déformations continues des brins en laissant les extrémités, c'est-à-dire, les gros points, fixes.

structure de groupe. En effet pour toutes tresses géométriques tr_1 et tr_2 à n brins distinctes, les tresses géométriques produits $\mathrm{tr}_1 \cdot \mathrm{tr}_2$ et $\mathrm{tr}_2 \cdot \mathrm{tr}_1$ sont distinctes, ce qui empêche l'existence d'un élément neutre. L'idée est alors de considérer les classes d'isotopies des tresses géométriques.

Définition 1.5. Une *tresse à n brins* est la classe d'isotopie d'une tresse géométrique à n brins. On note B_n l'ensemble des tresses à n brins.

Le produit de tresses géométriques à n brins étant clairement compatible avec la relation d'isotopie, il induit un produit sur B_n. Pour β, γ deux éléments de B_n, on note $\beta \cdot \gamma$ la tresse produit de β et γ. Contrairement aux cas des tresses géométriques on a le résultat suivant, donné sans démonstration :

Lemme 1.6. *Pour tout $n \geqslant 2$, la loi produit $\cdot$ définit une structure de groupe sur B_n.*

L'élément neutre de la loi produit $\cdot$ est la classe d'isotopie de la tresse géométrique où tous les brins sont des segments horizontaux. L'inverse de la classe d'isotopie d'une tresse géométrique tr est la classe d'isotopie de la réflexion de tr par rapport au disque $\left\{\frac{1}{2}\right\} \times D^2$.

Dans la suite on fera référence à B_n comme le groupe des tresses à n brins muni de l'opération produit $\cdot$ induite par la concaténation de tresses géométriques.

1.3 Tresses et groupe d'homéotopie

Nous avons vu précédemment comment définir les tresses comme objets géométriques plongés dans $\mathbb{R}^3$. Dans cette section nous allons donner une définition plus topologique du groupe de tresses.

Définition 1.7. Soit $\mathcal{S}$ une surface compacte orientée et $\mathcal{P}$ un ensemble fini de points intérieurs de $\mathcal{S}$. Le *groupe d'homéotopie* $\mathcal{MCG}(\mathcal{S}, \mathcal{P})$ de la surface $\mathcal{S}$ relativement à $\mathcal{P}$ est le groupe d'isotopie des homéomorphismes de $\mathcal{S}$ préservant l'orientation, fixant le bord $\partial\mathcal{S}$ point par point et laissant $\mathcal{P}$ globalement invariant.

La notion d'isotopie ici est légèrement différente de celle donnée à la définition 1.3. En effet, en reprenant les notations de la définition 1.3 nous ne demandons pas seulement que pour tout t dans $[0, 1]$ l'application $x \mapsto F(x, t)$ soit un homéomorphisme de $\mathcal{S}$, mais aussi qu'elle préserve l'orientation, laisse fixe $\partial\mathcal{S}$ point par point et laisse $\mathcal{P}$ globalement invariant. Le produit que l'on considère ici sur $\mathcal{MCG}(\mathcal{S}, \mathcal{P})$ est la loi de composition des homéomorphismes.

On rappelle que D^2 désigne le disque unité fermé centré en 0 de $\mathbb{R}^2$ identifié à la droite complexe $\mathbb{C}$, et que P_n désigne n points distincts intérieurs à D^2 régulièrement espacés sur l'axe imaginaire. On oriente le disque D^2 dans le sens contraire des aiguilles d'une montre.

Théorème 1.8. (J.S. Birman, [Bir74]) *Le groupe $\mathcal{MCG}(D^2, P_n)$ est isomorphe à B_n.*

De manière intuitive un élément de $\mathcal{MCG}(D^2, P)$ peut être considéré comme le film de n points qui bougent les uns autour des autres dans le disque D^2. Si au lieu de faire dérouler ce film dans le temps on le fait se dérouler le long de l'axe des abscisses, on obtient une tresse géométrique.

2 Présentation de B_n

Le but de cette section est de donner une définition du groupe de tresses B_n par générateurs et relations. Nous commençons d'abord par des rappels sur les mots et les monoïdes.

2.1 Présentation de monoïde et de groupe

Un *monoïde* est un ensemble muni d'une loi de composition interne associative admettant un élément neutre. Évidemment tout groupe est un monoïde. Mais la réciproque est fausse. Par exemple, l'ensemble $\mathbb{N}$ muni de l'addition est un monoïde d'élément neutre 0, mais pas un groupe.

Parmi les monoïdes, certains ont un rôle particulier : les *monoïdes libres*.

Définition 2.1. Soit $\mathcal{S}$ un ensemble non vide. Un *mot* sur $\mathcal{S}$ est une suite finie w d'éléments de $\mathcal{S}$, c'est à dire qu'il existe un entier ℓ positif tel que w soit une application de $\{1, \dots, \ell\}$ dans $\mathcal{S}$. L'entier ℓ est appelé *longueur* de w et est noté $|w|$. L'ensemble des mots sur $\mathcal{S}$ est noté $\mathcal{S}^*$.

Souvent, on dit que l'ensemble $\mathcal{S}$ est un *alphabet* et que ses éléments sont des *lettres*.

Dans cette thèse, on sera amené à utiliser des alphabets différents en même temps. Ainsi, afin d'éviter toute confusion, on utilisera les notations suivantes :

Notation 2.2. Soit $\mathcal{S}$ un ensemble non vide. On appelle *$\mathcal{S}$-lettre* tout élément de $\mathcal{S}$. On appelle *$\mathcal{S}$-mot* tout élément de $\mathcal{S}^*$, c'est-à-dire, un mot sur $\mathcal{S}$.

Soit $\mathcal{S}$ un alphabet. Pour u et w deux $\mathcal{S}$-mots, on définit le *produit* de u et v, noté $u \cdot v$ ou encore uv, le mot w de longueur $|u| + |v|$ défini par

$$w(i) = \begin{cases} u(i) & \text{pour } i \leqslant |u|, \\ v(i - |u|) & \text{pour } |u| + 1 \leqslant i \leqslant |u| + |v|. \end{cases} \tag{1.1}$$

L'unique $\mathcal{S}$-mot de longueur 0 est noté ε. Un mot w de longueur ℓ sera noté $w(1) \dots w(\ell)$ à la place de la suite $(w(1), \dots, w(\ell))$. Cette convention explique la notation uv pour le produit des mots u et v.

Proposition 2.3. *Pour un alphabet $\mathcal{S}$, l'ensemble $\mathcal{S}^*$ muni du produit de mots est un monoïde d'élément neutre ε.*

Le monoiïde introduit à la propsition précédente est appelé *monoïde libre sur $\mathcal{S}$*.

Soit $\mathcal{S}$ un alphabet. Une relation d'équivalence $\equiv$ sur $\mathcal{S}$ est appelée *congruence* si elle est compatible avec le produit de mots, c'est-à-dire, si les relations $u \equiv v$ et $u' \equiv v'$ impliquent la relation $u\,u' \equiv v\,v'$.

Définition 2.4. Soient $\mathcal{S}$ un alphabet et $\mathcal{R}$ un sous-ensemble de $\mathcal{S}^* \times \mathcal{S}^*$. Deux $\mathcal{S}$-mots sont dits *$\mathcal{R}$-équivalents,* et on note $u \equiv_{\mathcal{R}} v$, s'il existe une suite de $\mathcal{S}$-mots $(w_0, \dots, w_n)$ avec $w = w_0$ et $w' = w_n$ telle que pour tout k dans $\{0, \dots, n-1\}$ il existe une paire (x, y) de $\mathcal{R}$ et deux $\mathcal{S}$-mots u et v satisfaisant $\{w_k, w_{k+1}\} = \{uxv, uyv\}$.

Exemple 2.5. Considérons l'alphabet $\mathcal{S} = \{a, b\}$ et $\mathcal{R}$ le singleton $\{(ab, ba)\}$. Alors les mots $abba$ et $baab$ sont $\mathcal{R}$-équivalents. En effet, la suite (w_0, w_1, w_2) avec

$$w_0 = abba,\ w_1 = baba \text{ et } w_2 = baab,$$

en témoigne : on a $\{w_0, w_1\} = \{\varepsilon \cdot ab \cdot ba, \varepsilon \cdot ba \cdot ba\}$ et $\{w_1, w_2\} = \{ba \cdot ab \cdot \varepsilon, ba \cdot ba \cdot \varepsilon\}$.

On vérifie facilement que la relation $\equiv_{\mathcal{R}}$ est une congruence sur $\mathcal{S}^*$. Ainsi le produit de mots induit une loi de monoïde sur le quotient $\mathcal{S}^* / \equiv_{\mathcal{R}}$. De même, on peut montrer que tout monoïde est isomorphe à un quotient du monoïde $\mathcal{S}^*$ pour un certain alphabet $\mathcal{S}$, ce qui explique le terme « libre » pour désigner le monoïde $\mathcal{S}^*$.

Définition 2.6. Soit $\mathcal{S}$ un alphabet non vide et $\mathcal{R}$ un sous-ensemble de $\mathcal{S}^* \times \mathcal{S}^*$, on note

$$\langle \mathcal{S} \mid \mathcal{R} \rangle^+$$

le monoïde quotient $\mathcal{S}^* / \equiv_{\mathcal{R}}$, c'est le monoïde présenté par l'ensemble de générateurs $\mathcal{S}$ soumis aux relations $\mathcal{R}$.

On dit qu'un monoïde admet la présentation $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$ s'il est isomorphe au monoïde quotient $\mathcal{S}^* / \equiv_{\mathcal{R}}$.

Afin de simplifier les notations, dans une présentation, on notera les ensemble $\mathcal{S}$ et $\mathcal{R}$ sous forme de listes, c'est-à-dire, qu'on omet les accolades.

Exemple 2.7.
– Le monoïde $(\mathcal{S}, \cdot, \varepsilon)$ admet la présentation $\langle \mathcal{S} \mid \ \rangle^+$,
– Le monoïde $(\mathbb{N}^2, +, 0)$ admet la présentation $\langle a, b \mid ab = ba \rangle^+$,
– Le monoïde $(\mathbb{Z}/6\mathbb{Z}, +, 0)$ admet la présentation $\langle a, b \mid aa = \varepsilon, ab = ba, bbb = \varepsilon \rangle^+$.

Une présentation est un moyen performant d'étudier un monoïde, mais encore faut-il pouvoir reconnaître des éléments égaux. En effet, étant donnés deux $\mathcal{S}$-mots, peut-on décider si la relation $u \equiv_{\mathcal{R}} v$ est satisfaite ? Autrement dit, peut-on reconnaître si deux $\mathcal{S}$-mots représentent le même élément dans le monoïde $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$: c'est ce qu'on appelle *problème du mot*. Cette question a première vue anodine n'a pas de réponse en général. En effet en 1947, E.L. Post a montré dans [Pos47] qu'un problème proche de celui du mot est indécidable. Puis, de manière indépendante, A.A. Markov a démontré le résultat suivant :

Théorème 2.8. (A.A. Markov, [Mar47]) *Il existe une présentation de monoïde finie (en les générateurs et en les relations) pour laquelle le problème du mot est indécidable.*

Un groupe est un monoïde particulier où tout élément admet un inverse. Une congruence sur un groupe G est une relation d'équivalence sur G qui est compatible avec le produit et l'inverse, tandis qu'une congruence de monoïde est supposée être seulement compatible avec le produit.

Lemme 2.9. *Supposons que G soit un groupe et $\equiv$ une congruence de monoïde sur G. Alors G est aussi une congruence de groupe.*

Démonstration. Supposons $g \equiv g'$. Alors, comme $\equiv$ est compatible avec le produit, en multipliant à gauche par g^{-1} et à droite par g'^{-1} on a $g^{-1}g'g'^{-1} \equiv g^{-1}gg'^{-1}$, donc $g^{-1} \equiv g'^{-1}$. □

Définition 2.10. Soit $\mathcal{S}$ un alphabet non vide et $\mathcal{R}$ un sous-ensemble de $(\mathcal{S}\cup\mathcal{S}^{-1})^* \times (\mathcal{S}\cup\mathcal{S}^{-1})^*$, on note $\langle \mathcal{S} \mid \mathcal{R} \rangle$ le groupe qui, comme monoïde, admet la présentation

$$\left\langle (\mathcal{S} \cup \mathcal{S}^{-1})^* \mid \mathcal{R} \cup \{(ss^{-1}, \varepsilon), (s^{-1}s, \varepsilon) \mid s \in \mathcal{S}\} \right\rangle^+.$$

Exemple 2.11.
– Le groupe $(\mathbb{Z}, +, 0)$ admet la présentation $\langle a \mid \ \rangle$,
– Le groupe $(\mathbb{Z}^2, +, 0)$ admet la présentation $\langle a, b \mid ab = ba \rangle$,
– Le groupe $\mathfrak{S}_3$ admet la présentation $\langle a, b \mid aba = bab, aa = \varepsilon, bb = \varepsilon \rangle$.
L'exemple de $\mathfrak{S}_3$ est intéressant car le monoïde de même présentation est aussi $\mathfrak{S}_3$. En effet les relations $aa = \varepsilon$ et $bb = \varepsilon$ impliquent l'existence d'inverses pour a et b, à savoir a et b eux-mêmes.

2.2 Cas des groupes de tresses

Dans cette section, nous allons donner une présentation du groupe de tresses à n brins B_n. Nous rappelons que les éléments de B_n sont des classes d'isotopie de tresses géométriques à n brins. Dans le but de pouvoir décrire facilement B_n, nous allons exhiber des éléments particuliers de ces classes d'isotopie.

Un diagramme de tresses est une succession dans le plan $\mathbb{R}^2$ de la gauche vers la droite de diagrammes élémentaires $\mathcal{D}_i^+$ et $\mathcal{D}_i^-$ définis à la figure 1.3. Une tresse géométrique est dite *régulière* si, lorsqu'on la projette sur le plan (x, y) suivant l'axe z, on obtient un diagramme de tresses.

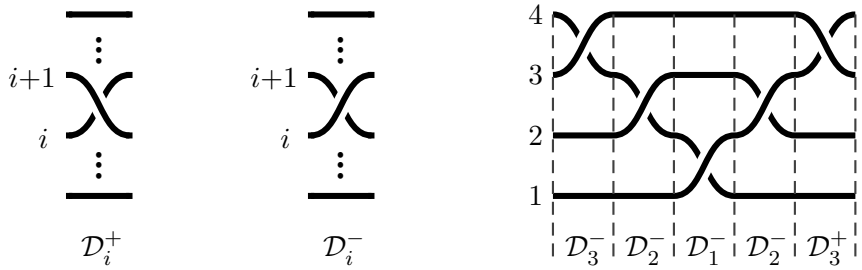


FIG. 1.3 : De la gauche vers la droite : diagramme élémentaire $\mathcal{D}_i^+$, diagramme élémentaire $\mathcal{D}_i^-$, exemple de diagramme de tresses. Les traits verticaux permettent de mieux visualiser l'agencement des diagrammes élémentaires.

Proposition 2.12. (E. Artin, [Art47]) *Toute tresse géométrique est isotope à une tresse régulière.*

Idée de la démonstration. Soit tr une tresse géométrique à n brins. Tout d'abord, il faut s'assurer que la projection de tr suivant l'axe des z soit informative. En effet, il peut arriver qu'il existe deux brins br_1 et br_2 de tr définis par

$$\mathrm{br}_1(t) = (x_1(t), y_1(t), z_1(t)), \quad \mathrm{br}_2(t) = (x_2(t), y_2(t), z_2(t)),$$

vérifiant $x_1(t) = x_2(t)$ et $y_1(t) = y_2(t)$ pour tout t dans un sous-intervalle I de $[0, 1]$. Dans ce cas, les projections des brins br_1 et br_2 seront confondues sur l'intervalle I. Pour éviter ce

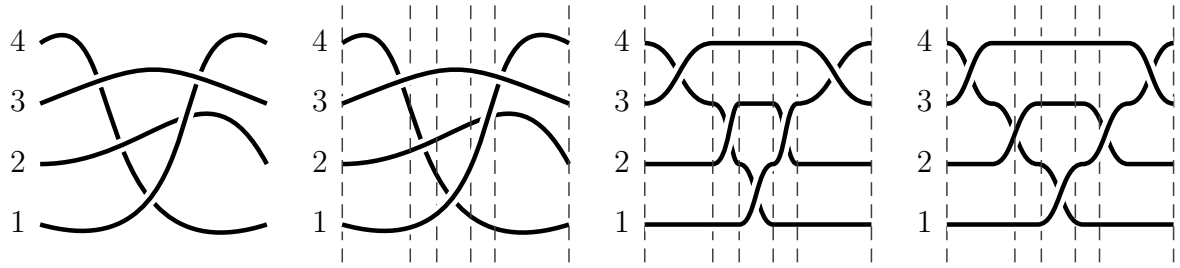


FIG. 1.4 : Obtention d'un diagramme de tresses à partir de la projection d'une tresse géométrique. Les lignes verticales en pointillés marquent la séparation entre les bandes, voir idée de la démonstration du lemme 2.12.

problème, nous allons déformer par isotopie la tresse tr. Tout d'abord nous déformons tr par isotopie afin qu'aucun brin n'ait de point d'intersection avec le bord $[0,1] \times \partial D^2$. Comme, par définition, les brins de tr sont compacts, il existe alors une constante strictement positive δ telle que chaque brin de tr soit à une distance d'au moins δ des autres brins et du bord $[0,1] \times \partial D^2$. Alors, si les projections de deux brins sont confondues sur un sous-intervalle I de $[0,1]$, il suffit d'en pousser continûment un vers le haut d'une distance d'au plus une fraction convenable de δ, et l'autre vers le bas. On recommence cette opération autant de fois que nécessaire.

Toujours grâce à un argument de compacité des brins, on montre que la projection de la tresse obtenue contient un nombre fini de croisements, noté k, et aucune portion de brin n'est confondue. Maintenant si deux croisements ont lieu à la même abscisse, on en déplace un vers la gauche et l'autre vers la droite par isotopie. On découpe alors la projection de la tresse obtenue en bandes verticales, notées $b_1, \dots, b_k$, de telle manière que chaque bande contienne exactement un croisement. Puis, en commençant par la bande la plus à gauche, nous déformons la tresse qu'elle contient afin d'obtenir un diagramme élémentaire. Enfin, nous dilatons ou rétractons chacune des bandes et la portion de tresse qu'elle contient, afin que toutes les bandes soient de même largeur (voir figure 1.4). □

On note σ_i une tresse géométrique dont la projection est le diagramme $\mathcal{D}_i^+$. De même, on note σ_i^{-1} une des tresses géométriques dont la projection est le diagramme $\mathcal{D}_i^-$. Le lemme 2.12 garantit que le groupe de tresses B_n est engendré par les tresses σ_i pour $i \leqslant n-1$. Les tresses σ_i ont été introduites par Artin dans [Art25] et [Art47] et sont souvent appelées *générateurs d'Artin* du groupe de tresses B_n. Clairement la tresse σ_i^{-1} est l'inverse de la tresse σ_i dans B_n. Quelles sont les autres relations satisfaites par les tresses σ_i ?

Lemme 2.13. *Les relations suivantes sont satisfaites dans B_n :*

$$\sigma_i \, \sigma_j = \sigma_j \, \sigma_i \qquad \textit{pour } |i-j| \geqslant 2 \tag{1.2}$$

$$\sigma_i \, \sigma_j \, \sigma_i = \sigma_j \, \sigma_i \, \sigma_j \quad \textit{pour } |i-j| = 1 \tag{1.3}$$

Démonstration. Les relations (1.2) et (1.3) se lisent très bien sur des diagrammes de tresses, voir figure 2.2. □

Dire que B_n satisfait les relations du lemme 2.13 n'implique pas que celles-ci donnent lieu à une présentation de B_n. Il pourrait très bien exister d'autres relations dans B_n qui ne soient pas conséquences des relations (1.2) et (1.3). Cependant de telles relations n'existent pas :

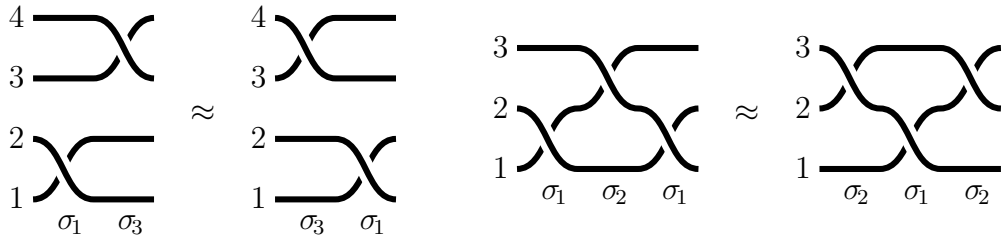


FIG. 1.5 : Illustration des relations (1.2) et (1.3) entre les générateurs d'Artin σ_i.

Théorème 2.14. (E. Artin, [Art47]) *Le groupe de tresses B_n admet la présentation suivante :*

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\,\sigma_j = \sigma_j\,\sigma_i & \textit{pour } |i-j| \geqslant 2 \\ \sigma_i\,\sigma_j\,\sigma_i = \sigma_j\,\sigma_i\,\sigma_j & \textit{pour } |i-j| = 1 \end{array} \right\rangle. \tag{1.4}$$

La démonstration de ce résultat consiste à montrer que si deux tresses géométriques sont isotopes, alors on peut passer d'un diagramme d'une tresse régulière isotope à l'une, au diagramme d'une tresse régulière isotope à l'autre, seulement à l'aide des relations du lemme 2.13.

Notation 2.15. Notons Σ_n l'ensemble $\{\sigma_1, \sigma_1^{-1}, \dots, \sigma_{n-1}, \sigma_{n-1}^{-1}\}$ et $\equiv$ la congruence de groupe engendrée par les relations de la présentation (1.4).

D'après le théorème 2.14, toute tresse de B_n peut être vue comme classe d'équivalence de Σ_n-mots pour la relation $\equiv$. C'est cette vision du groupe B_n qu'on aura à partir de maintenant. Pour simplifier les notations, un mot sur l'alphabet Σ_n sera souvent appelé *mot de tresse*. On dit qu'un mot de tresse *représente* la tresse β s'il est dans la classe d'équivalence associée à la tresse β.

Exemple 2.16. Montrons que les mots de tresses $\sigma_2^{-1}\,\sigma_1\,\sigma_2$ et $\sigma_1\,\sigma_2\,\sigma_1^{-1}$ sont équivalents. Comme la relation $\equiv$ est une congruence de groupe, de la relation $\sigma_1\,\sigma_2\,\sigma_1 \equiv \sigma_2\,\sigma_1\,\sigma_2$, on obtient

$$\sigma_2^{-1}\,\sigma_1\,\sigma_2\,\sigma_1 \equiv \sigma_1\sigma_2,$$

puis $\sigma_2^{-1}\,\sigma_1\,\sigma_2 \equiv \sigma_1\,\sigma_2\,\sigma_1^{-1}$.

2.3 Monoïde de tresses positives

Une fois qu'on a une présentation, le premier problème qu'on se pose est : peut-on résoudre le problème du mot pour cette présentation ? Le théorème 2.8 montre que cette question n'a pas de solution générale. Cependant, dans le cas des groupes de tresses, E. Artin a donné une solution au problème du mot dans [Art25, Art47]. Nous ne détaillons pas cette solution ici.

En 1969, F.A. Garside a donné une autre solution au problème du mot pour le groupe de tresse B_n [Gar69]. Pour cela il utilise ce que l'on appelle le *monoïde de tresses positives* et la forme normale dite de Garside sur ce monoïde, qui permet d'isoler un mot de tresse unique parmi tous les représentants d'une tresse donnée. Dans cette section nous nous intéressons au monoïde de tresses positives.

Définition 2.17. On appelle *monoïde de tresses positives à n brins* et on note B_n^+, le monoïde de présentation

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\,\sigma_j = \sigma_j\,\sigma_i & \text{pour } |i-j| \geqslant 2 \\ \sigma_i\,\sigma_j\,\sigma_i = \sigma_j\,\sigma_i\,\sigma_j & \text{pour } |i-j| = 1 \end{array} \right\rangle^+. \tag{1.5}$$

On remarque que la présentation donnée pour B_n^+ est la même que celle de B_n, à l'exception que c'est une présentation de monoïde et non une présentation de groupe.

Notation 2.18. Notons Σ_n^+ l'ensemble $\{\sigma_1, \dots, \sigma_{n-1}\}$ et $\equiv^+$ la congruence de monoïde engendrée par les relations de la présentation (1.5).

Un mot sur l'alphabet $\{\sigma_1, \dots, \sigma_{n-1}\}$ est appelé *mot de tresse positif*. Un mot de tresse positif étant un mot de tresse particulier, on peut naturellement se demander quels sont les liens entre les relations $\equiv^+$ et la restriction de $\equiv$ aux mots de tresse positifs. Clairement, on a

$$\text{pour } u, v \text{ mots de tresse positifs, } u \equiv^+ v \text{ implique } u \equiv v. \tag{1.6}$$

Qu'en est-il de la réciproque ? En général, il n'y a aucune raison pour qu'elle soit vraie :

Exemple 2.19. Soit M le monoïde de présentation $\langle a, b \mid ab = a \rangle^+$ et G le groupe de présentation $\langle a, b \mid ab = a \rangle$. On définit les relations $\equiv_M$ et $\equiv_G$ associées respectivement à la présentation de M et de G.

Alors on a $b \equiv_G \varepsilon$ mais pas $b \equiv_M \varepsilon$. En effet la relation $ab \equiv_G a$ implique $a^{-1}ab \equiv_G a^{-1}a$ puis $b \equiv_G \varepsilon$. D'autre part, comme b ne contient aucun facteur intervenant dans les relations de M, il est seul dans sa $\equiv_M$-classe d'équivalence.

Heureusement, dans le cas des tresses, la réciproque à (1.6) est vraie. Pour le démontrer on utilise le résultat suivant :

Théorème 2.20. (O. Ore, [Ore31]) *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 avec les propriétés suivantes :*
– *(i) il existe un morphisme injectif ψ de M dans G,*
– *(ii) tout élément de G, peut être exprimé comme fraction $\psi(a)^{-1}\psi(b)$ avec a et b dans M.*
De plus si $\langle \mathcal{S}, \mathcal{R} \rangle^+$ est une présentation de M, alors $\langle \mathcal{S}, \mathcal{R} \rangle$ est une présentation de G.

D'abord, donnons une définition des termes utilisés dans l'énoncé du théorème 2.20.

Définition 2.21. On dit qu'un monoïde est *simplifiable à gauche* (*resp.* à droite) si la relation $au = av$ (*resp.* $ua = va$) implique $u = v$ dans M. Un monoïde simplifiable à gauche et à droite est dit *simplifiable*.

Nous allons maintenant définir deux relations de divisibilité dans un monoïde M.

Définition 2.22. Soient M un monoïde et x, y deux éléments de M.
– On dit que x *divise à gauche* y ou bien encore que y est un *multiple à droite* de x, noté $x \preccurlyeq y$, s'il existe z de M satisfaisant $y = xz$.
– On dit que y *divise à droite* x ou bien encore que x est un *multiple à gauche* de y, noté $x \succcurlyeq y$, s'il existe z de M satisfaisant $x = zy$.

F.A. Garside a montré que le monoïde de tresses positives B_n^+ satisfait les conditions du théorème 2.20 :

Théorème 2.23. (F.A. Garside, [Gar69]) *Le monoïde B_n^+ est simplifiable et admet des multiples communs à droite.*

Une question est : peut-on résoudre le problème du mot dans B_n^+ ? La réponse est oui. En effet, comme les relations de la présentation 1.5 préservent la longueur des mots, deux mots équivalents sont de même longueur. Soient u et v deux mots de tresses positifs de même longueur ℓ. Pour décider si u et v sont équivalents, on calcule la classe d'équivalence $Cl(u)$ du mot u en appliquant successivement les relations (1.2) et (1.3). Comme l'alphabet Σ_n^+ est de cardinal $(n-1)$, la classe $Cl(u)$ a au plus $(n-1)^\ell$ éléments ; elle est donc finie et calculable. Enfin, il suffit de vérifier si v appartient à $Cl(u)$ pour conclure.

D'autre méthodes plus efficaces existent pour résoudre le problème du mot de B_n^+. Dans son article [Gar69], F.A. Garside calcule un représentant distingué dans chaque classe d'équivalence de mots positifs : la *forme normale de Garside*.

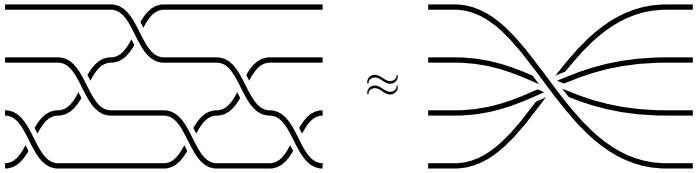


FIG. 1.6 : Diagramme de la tresse Δ_4 définie par $\Delta_4 = \sigma_1\sigma_2\sigma_3 \cdot \sigma_1\sigma_2 \cdot \sigma_1$ et son interprétation comme demi-tour des brins.

Cette forme est étroitement liée à la tresse Δ_n définie par :

$$\Delta_n = (\sigma_1 \cdot \ldots \cdot \sigma_{n-1}) \cdot (\sigma_1 \cdot \ldots \cdot \sigma_{n-2}) \cdot \ldots \cdot (\sigma_1 \cdot \sigma_2) \cdot \sigma_1, \tag{1.7}$$

c'est la tresse de B_n^+ où chaque paire de brins se croise une et une seule fois, correspondant à un demi-tour des brins.

La tresse Δ_n a de nombreuses propriétés intéressantes vis-à-vis de la structure de groupe de B_n, en particulier on a :

Proposition 2.24. (F.A. Garside, [Gar69]) *Un multiple commun à gauche et à droite des tresses $\sigma_1, \ldots, \sigma_n$ est Δ_n. De plus Δ_n^2 est dans le centre de B_n^+.*

On en déduit alors que pour toute tresse β de B_n il existe un entier p et une tresse positive β^+ avec $\beta = \Delta_n^{-2p}\,\beta^+$. Dans la suite on notera la tresse Δ_n et le mot de tresse positif du membre droit de (1.7) par le même symbole Δ_n. On espère que le contexte sera assez clair pour ne pas créer de confusion.

Nous pouvons maintenant donner une solution au problème de mot sur B_n. Soient u et v deux mots de tresse. On compte le nombre de lettres négatives k_u et k_v apparaissant dans u et v et on note k le maximum des deux. On calcule alors deux mots de tresses positifs u^+ et v^+ vérifiant (on peut le faire facilement) :

$$u \equiv \Delta_n^{-2k} u^+ \quad \text{et} \quad v \equiv \Delta_n^{-2k} v^+.$$

Les mots u^+ et v^+ sont des mots positifs, on peut donc décider si la relation $u^+ \equiv v^+$ est satisfaite ou pas et ainsi décider si $u \equiv v$ l'est.

Pour le moment, nous ne donnons pas plus de détails sur la structure dite de Garside de B_n^+ et ne donnons pas de démonstration de la proposition 2.23. Le chapitre II.2 est consacré à l'étude d'un autre sous-monoïde du groupe de tresses, admettant lui aussi une structure de Garside.

3 Ordre des tresses

Dans cette section nous allons définir un ordre sur les groupes des tresses. D'abord commençons par quelques définitions classiques sur les ordres.

Un *ordre strict* sur un ensemble X, est une relation binaire $\prec$ sur X qui est anti-réflexive, c'est-à-dire que la relation $x \prec x$ n'est jamais satisfaite, et transitive, c'est-à-dire que les relations $x \prec y$ et $y \prec z$ impliquent $x \prec z$.

Exemple 3.1. Pour x, y éléments de $\mathbb{N}$, on pose $x \prec y$ si x est un diviseur de y différent de y. Par définition, pour tout x de $\mathbb{N}$, la relation $x \prec x$ ne peut pas être satisfaite : la relation $\prec$ est anti-réflexive. Maintenant supposons $x \prec y$ et $y \prec z$, alors il existe w et w' deux éléments de $\mathbb{N}$ différents de 1 tels qu'on ait $x \cdot w = y$ et $y \cdot w' = z$. Ceci implique $x \cdot w \cdot w' = z$, c'est-à-dire, $x \prec z$: la relation $\prec$ est transitive. Ainsi $\prec$ est un ordre strict sur $\mathbb{N}$.

Un *ordre total* sur un ensemble X est un ordre strict $\prec$ tel que pour tout élément x, y de X, on ait soit $x = y$, soit $x \prec y$, soit $y \prec x$. L'ordre strict $\prec$ donné à l'exemple 3.1 n'est pas total. En effet, aucune des relations $2 = 3$, $2 \prec 3$ et $3 \prec 2$ n'est satisfaite. En revanche, l'ordre usuel de $\mathbb{N}$ est un ordre total.

Définir un ordre total sur le groupe des tresses B_n n'est pas chose difficile. L'alphabet Σ_n étant fini, l'ensemble des mots de tresse est dénombrable (comme ensemble de suites à support fini sur un ensemble dénombrable), ce qui implique que B_n est dénombrable. Ainsi il existe une injection ψ de B_n dans $\mathbb{N}$. Définissons la relation $\prec_\psi$ sur B_n par :

$$x \prec_\psi y \quad \text{si et seulement si} \quad \psi(x) < \psi(y).$$

Comme $<$ est un ordre total sur $\mathbb{N}$, il en est de même pour $\prec_\psi$ (l'injectivité est nécessaire pour montrer que $\prec_\psi$ est anti-réflexive).

On ne va donc pas seulement introduire un ordre total sur B_n mais aussi demander que cet ordre ait de bonnes propriétés vis-à-vis de la structure de groupe de B_n.

3.1 L'ordre de Dehornoy

Nous allons maintenant introduire l'ordre standard des tresses, qui est souvent appelé ordre de Dehornoy.

Définition 3.2. Un ordre total $\prec$ sur un groupe G est dit *invariant à gauche* (*resp.* à droite) si la relation $g \prec h$ implique $fg \prec fh$ (*resp.* $gf \prec hf$) pour tout f, g, h de G. Un ordre total $\prec$ sur un groupe G est dit *bi-invariant* s'il est invariant à la fois à gauche et à droite.

Par exemple, l'ordre des entiers est un ordre total bi-invariant. Malheureusement le groupe de tresses B_n n'admet pas d'ordre total bi-invariant.

Proposition 3.3. *Il n'existe pas d'ordre total bi-invariant sur B_n pour $n \geqslant 3$.*

Démonstration. En rajoutant σ_1 à gauche des termes de la relation $\sigma_1 \sigma_2 \sigma_1 \equiv \sigma_2 \sigma_1 \sigma_2$, on obtient $\sigma_1 \sigma_1 \sigma_2 \sigma_1 \equiv \sigma_1 \sigma_2 \sigma_1 \sigma_2$, impliquant $\sigma_1 \Delta_3 \equiv \Delta_3 \sigma_2$. De même en rajoutant σ_1 à droite dans la même relation on obtient $\Delta_3 \sigma_1 \equiv \sigma_2 \Delta_3$. Ainsi on a :

$$\Delta_3 \sigma_1 \Delta_3^{-1} \equiv \sigma_2 \quad \text{et} \quad \Delta_3 \sigma_2 \Delta_3^{-1} \equiv \sigma_1.$$

Supposons que $\prec$ soit un ordre bi-invariant sur B_n avec $\sigma_1 \prec \sigma_2$. Alors par bi-invariance de $\prec$, on devrait avoir $\Delta_3\,\sigma_1\Delta_3^{-1} \prec \Delta_3\,\sigma_2\Delta_3^{-1}$, c'est-à-dire, $\sigma_2 \prec \sigma_1$. Puis par transitivité de $\prec$, on aurait $\sigma_1 \prec \sigma_1$, ce qui est en contradiction avec le fait que $\prec$ soit anti-réflexive. On aboutit à la même contradiction si l'on suppose initialement $\sigma_2 \prec \sigma_1$. Ainsi on ne peut pas définir d'ordre bi-invariant sur B_n pour $n \geqslant 3$. □

Pour $n = 2$, le groupe B_n est isomorphe à $\mathbb{Z}$ et est donc naturellement muni d'un ordre bi-invariant. Maintenant la question est : existe-t-il un ordre invariant à gauche sur B_n ? Définir un ordre invariant à gauche sur un groupe G est équivalent à y définir un cône positif.

Définition 3.4. Un sous-ensemble P de G est appelé *cône positif* sur G si P est clos par multiplication et si G est la réunion disjointe de P, P^{-1} et $\{1\}$.

Voyons comment définir un ordre total invariant à gauche sur un groupe G à partir d'un cône positif de G et réciproquement.

Lemme 3.5. *Soit G un groupe.*
- (i) *Supposons que la relation $\prec$ soit un ordre total invariant à gauche sur G. Alors l'ensemble $\{g \in G \mid 1 \prec g\}$ est un cône positif de G , et $g \prec h$ est équivalent à $g^{-1}h \in P$.*
- (ii) *Supposons que P soit un cône positif sur G. Alors la relation $g \prec h$ équivalente à $g^{-1}h \in P$ est un ordre total invariant à gauche sur G et P correspond aux éléments plus grands que* 1.

Démonstration. Montrons (i). Posons $P = \{g \in G \mid 1 \prec g\}$ et montrons que P est un cône positif sur G. Comme $\prec$ est anti-réflexive, l'élément 1 n'appartient ni à P ni à P^{-1} (car on a $1^{-1} = 1$). De plus, comme $\prec$ est total, pour tout élément g de G, on a soit $g = 1$, soit $1 \prec g$, soit $g \prec 1$. Par invariance à gauche de $\prec$, la relation $g \prec 1$ implique $g^{-1}\,g \prec g^{-1}$, c'est-à-dire, la relation $1 \prec g^{-1}$. Ainsi G est réunion disjointe de $\{1\}$, P et P^{-1}. Soient g et h deux éléments de P. On a donc $1 \prec g$ et $1 \prec h$. Par invariance à gauche de $\prec$, on obtient $h \prec gh$. Puis la transitivité de $\prec$ avec les relations $1 \prec h$ et $h \prec gh$ implique $1 \prec gh$, c'est-à-dire, $gh \in P$. La relation $g \prec h$ est équivalente à $1 \prec g^{-1}h$ par invariance à gauche de $\prec$.

Montrons (ii). Notons $g \prec h$ la relation $g^{-1}h \in P$. Comme 1 n'est pas un élément de P, la relation $\prec$ est anti-réflexive. Supposons qu'on ait $f \prec g$ et $g \prec h$. Par définition de $\prec$, cela revient à $f^{-1}g \in P$ et $g^{-1}h \in P$. Comme P est stable par multiplication on a $f^{-1}h \in P$, c'est-à-dire que la relation $f \prec h$ est satisfaite. Soient g et h deux éléments de G. De $G = P^{-1} \sqcup \{1\} \sqcup P$, on déduit que $g^{-1}h$ appartient soit à P, soit à P^{-1}, ou bien est l'élément neutre. Ainsi $\prec$ est un ordre total. Supposons $g \prec h$ et soit f un élément de G. De $g^{-1}h \in P$ on déduit $g^{-1}f^{-1}fh \in P$, c'est-à-dire, $(fg)^{-1}(fh) \in P$, ce qui implique $fg \prec fh$. On a donc montré que $\prec$ est un ordre total invariant à gauche. □

Exemple 3.6. L'ordre standard des entiers naturels $\mathbb{Z}$ est associé au cône des entiers positifs : la relation $i < j$ est satisfaite si et seulement si $-i + j$ est strictement positif, c'est-à-dire, si on a $j - i > 0$.

Nous allons maintenant définir un cône positif sur B_n. Naïvement on pourrait penser au monoïde de tresses positives, comme pour le cas des entiers. Malheureusement, il existe des tresses qui ne sont ni triviales (pas emmêlée), ni positives, ni les inverses de tresses positives. L'idée est de prendre une famille un peu plus grande que les tresses positives.

Définition 3.7. – Un mot de tresse est dit *σ-positif* si la lettre σ_i de plus grand indice i n'apparaît que positivement, c'est à dire que σ_i^{-1} n'est pas présent.
– Une tresse est dite *σ-positive* si elle peut être représentée par un mot σ-positif.

Par exemple le mot $\sigma_2^{-1}\sigma_1\sigma_2$ n'est pas σ-positif : la lettre de plus grand indice, σ_2, apparaît positivement et négativement. Par contre le mot $\sigma_1\sigma_2\sigma_1^{-1}$ qui lui est équivalent (voir exemple 2.16), est σ-positif : la lettre σ_2 n'apparaît que positivement. Ainsi la tresse $\sigma_2^{-1}\sigma_1\sigma_2$ est σ-positive. C'est l'ensemble des tresses σ-positives que l'on va prendre comme cône positif.

Définition 3.8. Pour β, γ éléments de B_n, on dit que la relation $\beta < \gamma$ est vraie si la tresse $\beta^{-1}\gamma$ est σ-positive.

La relation $<$ est le premier ordre total invariant à gauche défini sur le groupe de tresses B_n :

Théorème 3.9. (P. Dehornoy, [Deh94]) *Pour tout n, la relation $<$ est un ordre total invariant à gauche sur B_n.*

Ce théorème est une conséquence des deux propriétés suivantes :

Propriété A. (Acyclicité) Une tresse σ-positive est non triviale.

Propriété C. (Comparaison) Une tresse est soit triviale, soit σ-positive, soit l'inverse d'une tresse σ-positive.

*Démonstration du théorème 3.9 à partir des propriétés **A** et **C**.* Soit P l'ensemble des tresses σ-positives de B_n. Par le lemme 3.5 il suffit alors de montrer que P est un cône positif. Soient β et γ deux tresses σ-positives. Alors il existe deux mots de tresses σ-positifs u et v représentant respectivement β et γ. Clairement le mot w, produit des mots u et v, est σ-positif. Il s'ensuit que la tresse $\beta\,\gamma$ est σ-positive, et donc que P est stable par multiplication. La propriété **C** implique que B_n est inclus dans $P^{-1} \cup \{1\} \cup P$. Comme l'inverse de 1 est 1, la propriété **A** implique que 1 n'appartient ni à P, ni à P^{-1}. Il nous reste à montrer que l'intersection de P et P^{-1} est vide. Supposons qu'il existe une tresse β dans l'intersection de P et P^{-1}. Alors β et β^{-1} seraient dans P, et, par stabilité par multiplication, on aurait que 1 appartient à P, ce qui est faux. □

Pour la propriété **A**, nous renvoyons aux livres [DDRW02] et [DDRW08], qui présentent différentes manières de la démontrer. Dans cette thèse nous redonnons une démonstration de la propriété **C** à la section V.1.3. D'autres démonstrations existent dans les livres cités ci-dessus.

Exemple 3.10. Pour i et j dans $\{1, \dots, n\}$, la relation $\sigma_i < \sigma_j$ est équivalente à $i < j$. En effet, si on a $i < j$ alors la tresse $\sigma_i^{-1}\sigma_j$ est σ-positive car le générateur de plus grand indice, à savoir j, n'apparaît que positivement.

3.2 Tresses et bon ordre

On dit qu'un ordre total $\prec$ sur un ensemble X est un *bon ordre* si toute partie non vide de X admet un plus petit élément. Le groupe B_n muni de l'ordre $<$ n'est pas un bon ordre. En effet l'ensemble $\{\sigma_1^{-k} \mid k \geqslant 0\}$ n'admet pas de plus petit élément. Dans cette section, nous allons montrer que la restriction de l'ordre $<$ à certains sous-monoïdes de B_n est un bon ordre, c'est le cas de B_n^+.

On commence par donner une autre caractérisation des ensembles bien ordonnés.

Proposition 3.11. *Soit $<$ un ordre total sur un ensemble X, alors on a équivalence entre*
– (i) $(X, <)$ est un bon ordre.
– (ii) il n'existe pas de suite infinie strictement décroissante sur $(X, <)$.

Démonstration de $(i) \Rightarrow (ii)$ de la proposition 3.11 . Soit $(y_k)_{k\geqslant 1}$ une suite infinie d'éléments appartenant à X. On pose $Y = \{y_k \mid k \geqslant 1\}$. Comme Y est un sous-ensemble de X, qui est bien ordonné pour $<$ par hypothèse, Y admet un plus petit élément pour l'ordre $<$. Notons ℓ l'indice de ce plus petit élément. Par construction on a alors $y_{\ell+1} \geqslant y_\ell$, et la suite $(y_k)_{k\geqslant 1}$ n'est pas infinie décroissante. □

La démonstration de $(ii) \Rightarrow (i)$ nécessite l'axiome du choix (ou plus exactement un axiome plus faible qui est une conséquence de celui du choix). Nous rappelons donc cet axiome à l'aide de la notion de *fonction de choix*.

Définition 3.12. Soit X un ensemble. On appelle *fonction de choix* sur X toute application f de $\mathcal{P}(X) \setminus \{\emptyset\}$ dans X qui vérifie $f(Y) \in Y$ pour toute partie Y de X.

L'axiome du choix est alors l'assertion : « Il existe une fonction de choix sur tout ensemble ». A l'aide de cet axiome nous pouvons maintenant terminer la démonstration de la proposition 3.11.

Démonstration de $(ii) \Rightarrow (i)$ de la proposition 3.11 . Supposons qu'il existe un sous-ensemble non vide Y de X qui n'admette pas de plus petit élément pour $<$. Pour tout y de Y, on note I_y l'ensemble $\{z \in Y \mid z < y\}$. D'après l'hypothèse faite sur Y, l'ensemble I_y est non vide pour tout y dans Y. Notons f une fonction de choix sur X, l'axiome du choix en assurent l'existence. On a alors $f(I_y) \in I_y$, donc en particulier $f(I_y) < y$, pour tout y de Y . On définit alors une suite d'éléments de Y par induction en posant $y_1 = f(Y)$ et $y_{k+1} = f(I_{y_k})$. Par construction de I_y, la suite $(y_k)_{k\geqslant 1}$ est infinie décroissante, ce qui est en contradiction avec (ii). L'ensemble Y admet donc un plus petit élément. □

Revenons maintenant aux tresses. En 1996, R. Laver a montré dans [Lav96] que la restriction de $<$ sur le monoïde de tresses positives est un bon ordre. Le point difficile est de démontrer le théorème suivant :

Théorème 3.13. (R. Laver, [Lav96]) *Pour toute tresse β de B_n, la tresse $\beta^{-1}\,\sigma_i\,\beta$ est σ-positive.*

La démonstration donnée par Laver utilise des considérations d'algèbre auto-distributive et demeure très compliquée malgré la simplicité de l'énoncé. D'autres démonstrations de ce résultat sont données dans [DDRW02] et [DDRW08].

On remarque que le théorème 3.13 reste vrai si on remplace la tresse σ_i par n'importe quel conjugué d'une tresse σ_i :

Corollaire 3.14. *Soit α un conjugué de σ_i. Alors, toute tresse de la forme $\beta^{-1}\,\alpha\,\beta$ est σ-positive.*

Démonstration. Soit γ une tresse vérifiant $\alpha = \gamma^{-1}\sigma_i\gamma$. La tresse $\beta^{-1}\alpha\beta$ est alors égale à la tresse $(\gamma\beta)^{-1}\sigma_i(\gamma\beta)$, qui, par le théorème 3.13, est σ-positive. □

A ce stade, le lien entre le théorème 3.13 et le fait que la restriction de $<$ au monoïde de tresses positives est un bon ordre n'est pas évident. Pour l'établir, nous avons besoin du résultat suivant :

Théorème 3.15. (G. Higman, [Hig52]) *Tout ensemble infini de mots sur un alphabet fini, contient nécessairement deux mots w et w' tels que w' peut être obtenu à partir de w par insertion de lettres.*

La démonstration du théorème 3.15 nécessite des notions d'algèbre abstraite. Nous ne donnons pas plus de détails ici et référons à l'article original.

Voici le principal résultat de cette section :

Théorème 3.16. (R. Laver, [Lav96]) *La restriction de $<$ à tout sous-monoïde de B_n engendré par un nombre fini de conjugués de σ_i est un bon ordre.*

Démonstration. Soit M un sous-monoïde de B_n engendré par un ensemble $\{\alpha_1, \dots, \alpha_i\}$ de conjugués de σ_i, noté $\mathcal{S}$. Soit $(\beta_k)_{k\geqslant 1}$ une suite infinie d'éléments de B_n. Pour tout k, choisissons un mot w_k représentant la tresse β_k. Il n'y a qu'un nombre fini de mots d'une longueur donnée sur $\mathcal{S}$. On peut donc extraire une sous suite $(w_{k_i})_{i\geqslant 1}$ pour laquelle les longueurs ne décroissent pas. Si l'ensemble W, défini par $W = \{w_{k_1}, w_{k_2}, ...\}$, est fini, il existe i et j tels qu'on ait la relation $w_{k_i} = w_{k_j}$ et donc $\beta_{k_i} = \beta_{k_j}$; la suite $(\beta_k)_{k\geqslant 1}$ n'est donc pas décroissante. Supposons maintenant que W soit infini. Par le théorème 3.15, il existe i et j tel que w_{k_j} soit obtenu à partir de w_{k_i} en insérant des lettres de $\mathcal{S}$. Par construction de $(w_{k_i})_{i\geqslant 1}$, on a alors $i < j$. D'autre part, le théorème 3.13 implique $\beta_{k_i} < \beta_{k_j}$. Ainsi la suite $(\beta_k)_{k\geqslant 1}$ n'est pas décroissante. □

Une conséquence du théorème 3.16 est que le monoïde B_n^+ muni de l'ordre $<$ est un bon ordre. On peut alors se demander quelle est la longueur de $(B_n^+, >)$. Malheureusement, la méthode utilisée pour la démonstration du théorème 3.16, ne permet pas de répondre. Cependant, S. Burckel a démontré dans sa thèse le résultat suivant :

Théorème 3.17. (S. Burckel, [Bur94]) *Le type d'ordre de $(B_n^+, <)$ est $\omega^{\omega^{n-2}}$.*

La démonstration donnée par S. Burckel repose sur un argument subtil d'induction qui est difficile à contrôler en pratique.

3.3 Applications de l'existence de l'ordre

Dans cette section nous donnons des propriétés du groupe de tresses B_n qui peuvent être démontrées à partir de l'existence d'un ordre invariant à gauche.

La première montre que B_n est un groupe sans torsion ; c'est-à-dire qu'il n'existe pas de tresse β différente de la tresse triviale vérifiant $\beta^k = 1$ avec $k \geqslant 1$.

Proposition 3.18. *Le groupe de tresses B_n est sans torsion.*

Démonstration. Soit β une tresse non triviale de B_n. Comme $<$ est un ordre total, l'une des deux relations $1 < \beta$ et $\beta < 1$ est satisfaite. Supposons qu'on ait $1 < \beta$ (l'autre cas se traite de la même manière). Par invariance à gauche de $<$, on a $\beta < \beta^2$. Ainsi, par induction, on obtient

$$1 < \beta < \beta^2 < \dots < \beta^{k-1} < \beta^k < \dots .$$

Il n'existe donc pas d'entier k strictement positif satisfaisant $\beta^k = 1$. □

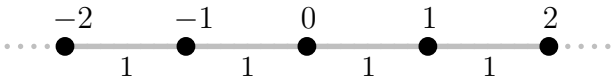


FIG. 1.7 : Graphe de Cayley de $(\mathbb{Z}, +)$ par rapport à $\{1\}$.

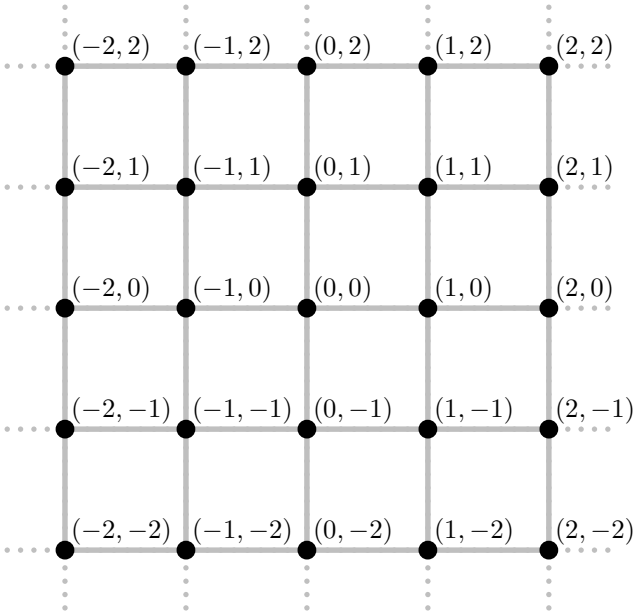


FIG. 1.8 : Graphe de Cayley de $(\mathbb{Z}^2, +)$ par rapport à $\{(0,1),(1,0)\}$: le générateur $(1,0)$ est représenté par une arête horizontale tandis que $(0,1)$ est représenté par une arête verticale.

Une autre application de l'ordre de des tresses repose sur le graphe de Gayley du groupe de tresse.

Le choix d'un système de générateurs $\mathcal{S}$ pour un groupe G donne une notion de distance sur ce groupe, où deux éléments distincts sont à distance 1 si on peut passer de l'un à l'autre par multiplication ou division à droite par un élément de $\mathcal{S}$. En connectant les éléments de G qui sont à distance 1 par une arête étiquetée par le générateur correspondant, on obtient le *graphe de Cayley de G par rapport à $\mathcal{S}$*.

Soit G un groupe donné par une présentation finie $\langle \mathcal{S}, \mathcal{R} \rangle$. Notons $F(\mathcal{S})$ le groupe libre engendré par $\mathcal{S}$. Alors tout $\mathcal{S}$-mot w représentant l'élément neutre de G admet une écriture

$$w = \prod_{i=1}^{n} v_i r_i^{\pm 1} v_i^{-1}, \tag{1.8}$$

avec $r_i \in \mathcal{R}$ et $v_i \in F(\mathcal{S})$ pour tout i. Dans le graphe de Cayley de G relativement à $\mathcal{S}$, l'écriture de (1.8) correspond à la sous-division d'un lacet étiquetté par w par des lacets étiquettés r_i, les mots v_i correspondent au déplacement d'un lacet codant une relation de $\mathcal{R}$ à partir du point base. Pour plus de détails, nous référons à [ECH+92].

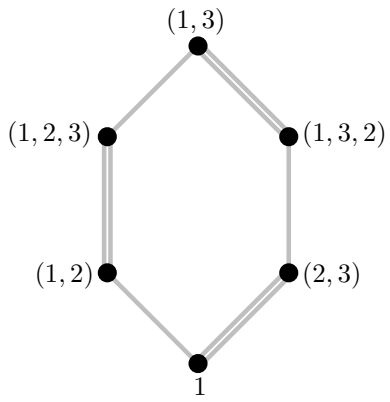


FIG. 1.9 : Graphe de Cayley de $(\mathfrak{S}_3, \cdot)$ par rapport à $\{(1,2),(2,3)\}$: le générateur $(1,2)$ est représenté par une arête simple tandis que $(2,3)$ est représenté par une arête double.

Définition 3.19. Soient G un groupe donné par une présentation finie $\langle \mathcal{S}, \mathcal{R} \rangle$.
– Pour w un $\mathcal{S}$-mot représentant l'élément neutre de G, on appelle *aire* de w et on note aire(w) le plus petit n pour lequel l'écriture (1.8) existe.
– On appelle *fonction isopérimétrique* de $\langle \mathcal{S}, \mathcal{R} \rangle$, la fonction définie par

$$\psi(i) = \max\{\text{aire}(w) \mid \ell(w) \leqslant i; w \equiv_{\mathcal{R}} 1\},$$

où 1 est l'élément neutre du groupe G.

Bien sûr, la fonction isopérimétrique dépend de la présentation de groupe donné, mais si ψ et ψ' sont deux fonctions isopérimétriques associées à deux présentations différentes du même groupe G, alors il existe deux constantes k et k' tel qu'on ait $\psi(i) \leqslant k\psi'(k'i)$. Ainsi si ψ est majoré par un polynôme ou une exponentielle, c'est le cas pour ψ'. Dans ce cas, on dit que le groupe G admet une *inégalité isopérimétrique* respectivement polynomiale ou exponentielle.

Une conséquence indirecte du fait que B_n soit sans torsion est un résultat sur la compléxité minimale de l'inégalité isopérimétrique dans B_n. D'abord donnons une définition des groupes hyperboliques au sens de Gromov.

Définition 3.20. Un groupe G finiment présenté est dit *hyperbolique* s'il admet une inégalité isopérimétrique linéaire.

En 1987, M. Gromov a donné dans [Gro87] la caractérisation suivante des groupes hyperboliques :

Théorème 3.21. (M. Gromov, [Gro87]) *Pour un groupe G finiment présenté, il y a équivalence entre :*
– (i) *G est hyperbolique.*
– (ii) *G a une inégalité isopérimétrique sous-quadratique.*

Le groupe des tresses admettant une présentation finie, on peut se demander s'il est hyperbolique. Le groupe $(B_2, \cdot)$ est isomorphe à $(\mathbb{Z}, +)$, qui est hyperbolique. Pour $n \geqslant 3$, la situation est différente. Gromov a montré dans [Gro87] qu'un groupe ayant $\mathbb{Z} \times \mathbb{Z}$ comme sous-groupe ne peut pas être hyperbolique. Nous utilisons le fait que B_n soit sans torsion pour démontrer le résultat suivant :

Lemme 3.22. *Pour $n \geqslant 3$, le groupe $\mathbb{Z} \times \mathbb{Z}$ est un sous-groupe de B_n.*

Démonstration. Pour $n \geqslant 3$, le groupe G engendré par σ_1 et Δ_3^2 est un sous-groupe de B_n. Par la proposition 2.24, les tresses σ_1 et Δ_3^2 commutent. Ainsi l'application η définie par

$$\begin{aligned} \eta : \mathbb{Z} \times \mathbb{Z} &\to G \\ (p,\ q) &\mapsto \sigma_1^p\, \Delta_3^q, \end{aligned}$$

est un morphisme de groupe surjectif. Supposons que la tresse β égale à $\sigma_1^p\, \Delta_3^q$ soit triviale. Comme Δ_3 contient au moins une lettre σ_2, la tresse β est σ_2-positive pour $q \geqslant 1$. On doit donc avoir $q = 0$, puis $p = 0$. Ainsi η est injective et G est isomorphe à $\mathbb{Z} \times \mathbb{Z}$. □

Ainsi le groupe B_n n'est pas hyperbolique pour $n \geqslant 3$, et donc l'inégalité isopérimétrique y est au moins quadratique.

Pour plus de détails sur les groupes hyperbobliques, nous renvoyons à [Gd90, Gro87, BRS07].

II. Monoïde de tresses dual

Dans ce chapitre, nous présentons un nouveau monoïde de tresses, noté B_n^{+*}, initialement introduit par J.S. Birman, K.H. Ko et S.J. Lee [BKL98], nommé monoïde de Birman–Ko–Lee, ou monoïde de tresses dual : le terme dual a été introduit par D. Bessis dans [Bes03] et est dû à une symétrie d'invariants numériques entre le monoïde de tresses positives B_n^+ et le monoïde B_n^{+*}.

1 Une autre présentation de B_n

À la section I.I.2.2, nous avons donné une présentation du groupe de tresses. Par ailleurs la même présentation vue comme présentation de monoïde nous a permis de définir un sous-monoïde de B_n, à savoir le monoïde de tresses positives. Le but de cette section est de donner une présentation différente du groupe de tresses B_n.

1.1 Générateurs de Birman–Ko–Lee

A la section I.I.2.2, nous avons vu que le groupe de tresses B_n était engendré par les générateurs dit d'Artin, notés $\sigma_1, \dots, \sigma_{n-1}$. La tresse σ_i correspond au croisement des brins i et $i+1$. Maintenant, nous allons introduire de nouvelles tresses correspondant au croisement de brins non forcément adjacents.

Définition 1.1. Pour $1 \leqslant p \leqslant q$, on pose

$$a_{p,q} = \sigma_p \dots, \sigma_{q-2}\ \sigma_{q-1}\ \sigma_{q-2}^{-1} \dots \sigma_p^{-1} \tag{2.1}$$

La tresse $a_{p,q}$ correspond au croisement du q-ème brin au dessus du p-ème en dessous des brins intermédiaires (s'il y en a).

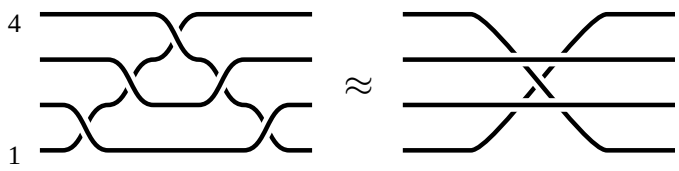


FIG. 2.1 : Dans la tresse $a_{1,4}$, les brins 1 et 4 se croisent en dessous des brins 2 et 3.

Remarque 1.2. Dans [BKL98], Birman, Ko et Lee définissent la tresse $a_{p,q}$ en posant :

$$a_{p,q} = \sigma_{q-1} \dots \sigma_{p+1}\ \sigma_p\ \sigma_{p+1}^{-1} \dots \sigma_{q-1}^{-1}.$$

Dans leur version, $a_{p,q}$ correspond aussi au croisement du q ème brin au dessus du p ème brin, mais en dessus des brins intermédiaires. Les deux versions donnent lieu à des propriétés semblables, mais la version que nous utilisons se comporte mieux vis-à-vis de l'ordre.

D'après la définition des tresses $a_{p,q}$, on a $\sigma_i = a_{i,i+1}$. Ainsi cette nouvelle famille de tresses inclut la famille des générateurs d'Artin, comme le laissait penser l'interprétation géométrique.

Notation 1.3. Notons A_n^+ l'ensemble $\{a_{p,q} \mid 1 \leqslant p < q \leqslant n\}$, et A_n l'ensemble $A_n^+ \sqcup (A_n^+)^{-1}$.

Un mot sur l'alphabet A_n est appelé A_n*-mot*, un mot sur l'alphabet A_n^+ est appelé A_n^+*-mot* ou *mot de tresse dual*. Comme Σ_n^+ est inclus dans A_n, les mots de tresses positifs sont des mots de tresses duaux.

Les tresses de A_n^+ engendrent B_n, car c'est déjà le cas pour celles de Σ_n^+. On note $[p, q]$ l'intervalle $\{p, \dots, q\}$ de $\mathbb{N}$, et on dit que $[p, q]$ est *niché* dans $[r, s]$ si la relation $r < p < q < s$ est satisfaite. Nous allons maintenant démontrer le résultat suivant :

Proposition 1.4. (Birman, Ko, Lee, [BKL98]) *Le groupe de tresses B_n est présenté par l'ensemble de générateurs A_n soumis aux relations :*

$$a_{p,q}\, a_{r,s} = a_{r,s}\, a_{p,q} \qquad \textit{pour } [p, q] \textit{ et } [r, s] \textit{ nichés ou disjoints}, \tag{2.2}$$

$$a_{p,q}\, a_{q,r} = a_{q,r}\, a_{p,r} = a_{p,r}\, a_{p,q} \qquad \textit{pour } 1 \leqslant p < q < r \leqslant n. \tag{2.3}$$

L'ensemble A_n a de bonnes propriétés vis-à-vis de la rotation des indices, qui sont mieux visualisées lorsque la tresse $a_{p,q}$ est représentée sur un cylindre. En effet, il est naturel de représenter la tresse $a_{p,q}$ par une corde reliant les points p et q d'un cercle avec n points marqués. Cette manière de voir n'est pas qu'une astuce. Pour plus de détails, consulter [BDM02].

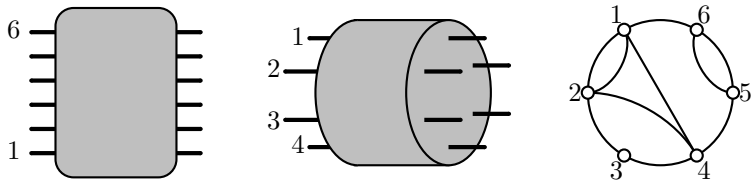


FIG. 2.2 : Enrouler le diagramme de tresse usuel aide à visualiser les symétries des tresses $a_{p,q}$. Sur le cercle obtenu, $a_{p,q}$ correspond naturellement à la corde reliant les points p et q.

Donnons maintenant un sens aux relations (2.2) et (2.3) lorsque $a_{p,q}$ est représentée par une corde. La condition « $[p, q]$ et $[r, s]$ nichés ou disjoints » de la relation (2.2) est équivalente au fait que la corde reliant p à q et la corde reliant r à s ne s'intersectent pas, même aux extrémités. Ainsi les tresses $a_{p,q}$ et $a_{r,s}$ commutent si et seulement si les cordes associées n'ont pas de points en commun ou si elles sont confondues. Par exemple, on a $a_{1,4}\, a_{2,6} = a_{2,6}\, a_{1,4}$ (voir figure 2.2). La relation (2.3) est un peu plus délicate à interpréter. Comme elle fait intervenir trois entiers distincts, elle se lit naturellement dans un triangle de cordes. Son interprétation est : dans un triangle de cordes, le produit de deux arêtes adjacentes lues dans le sens contraire des aiguilles d'une montre ne dépend pas du point d'origine choisi. Par exemple, on a

$$a_{2,4}\, a_{1,4} = a_{1,4}\, a_{1,2} = a_{1,2}\, a_{2,4} \text{ (voir figure 2.2)}.$$

1.2 Les tresses $d_{p,q}$

D'après la définition 1.1 les tresses $a_{p,q}$ sont les conjugués de σ_{q-1} par des tresses produits de σ_i. Ces dernières jouant un rôle important dans cette thèse nous leur donnons un nom et nous leur consacrons cette sous-section.

Définition 1.5. Pour $1 \leqslant p \leqslant q$, on pose

$$d_{p,q} = \sigma_p \dots \sigma_{q-1}. \tag{2.4}$$

Géométriquement, la tresse $d_{p,q}$ correspond au décalage vers le bas des brins $p+1$ jusqu'à q par dessus le brin p, qui, lui, se retrouve en position q. Une conséquence immédiate de la définition 1.1 est la relation suivante qui établit le lien entre $d_{p,q}$ et $a_{p,q}$:

$$a_{p,q} = d_{p,q-1}\, \sigma_{q-1}\, d_{p,q-1}^{-1} = d_{p,q}\, d_{p,q-1}^{-1}. \tag{2.5}$$

Ainsi $d_{p,q-1}$ est le conjuguant de σ_{q-1} définissant la tresse $a_{p,q}$.

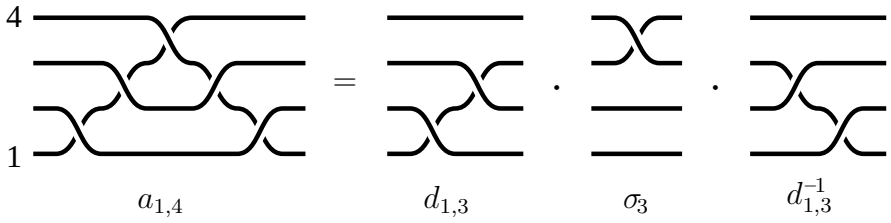


FIG. 2.3 : Décomposition de la tresse $a_{1,4}$ en $d_{1,3} \cdot \sigma_3 \cdot d_{1,3}^{-1}$.

Le premier intérêt d'introduire ces nouvelles tresses est de simplifier les calculs permettant d'établir les relations (2.2) et (2.3) entre les tresses $a_{p,q}$. Le lemme suivant donne les relations qui nous seront utiles dans ce sens.

Lemme 1.6. *Les relations suivantes sont satisfaites*

$$d_{p,r} = d_{p,q}\, d_{q,r} \qquad \textit{pour } p \leqslant q \leqslant r, \tag{2.6}$$

$$d_{p,q}\, d_{r,s} = d_{r,s}\, d_{p,q} \qquad \textit{pour } p \leqslant q < r \leqslant s, \tag{2.7}$$

$$d_{p,q}^{\pm 1}\, d_{r,s} = d_{r,s}\, d_{p-1,q-1}^{\pm 1} \qquad \textit{pour } r < p \leqslant q < s. \tag{2.8}$$

Démonstration. La relation (2.6) est une conséquence immédiate de l'écriture de $d_{p,q}$ en terme des σ_i donnée en (2.4). Pour la relation (2.7), on remarque que le générateur σ_i de plus grand indice apparaissant dans l'expression de $d_{p,q}$ donnée en (2.4) est σ_{q-1} tandis que celui de plus petit indice apparaissant dans celle de $d_{r,s}$ est σ_r. Comme $q < r$ implique $q-1 \leqslant r-2$, on peut appliquer la relation (I.1.2) de commutation de la présentation d'Artin et ainsi obtenir le résultat. Montrons maintenant la relation (2.8). Pour $r < p < s$ et $e = \pm 1$, établissons

$$\sigma_p^e\, d_{r,s} = d_{r,s}\, \sigma_{p-1}^e. \tag{2.9}$$

Comme p est compris strictement entre r et s, en utilisant (2.6) on décompose la tresse $d_{r,s}$ en le produit $d_{r,p-1}\, \sigma_{p-1}\, \sigma_p\, d_{p+1,s}$. La relation (2.7) implique que σ_p et $d_{r,p-1}$ commutent :

$$\sigma_p^e\, d_{r,s} = d_{r,p-1}\, \sigma_p^e\, \sigma_{p-1}\, \sigma_p\, d_{p+1,s}.$$

Par la relation (I.1.3) de la présentation d'Artin, on a la relation $\sigma_p\, \sigma_{p-1}\, \sigma_p = \sigma_{p-1}\, \sigma_p\, \sigma_{p-1}$, et donc $\sigma_p^{-1}\, \sigma_{p-1}\, \sigma_p = \sigma_{p-1}\, \sigma_p\, \sigma_{p-1}^{-1}$. En appliquant l'une ou l'autre des deux relations en fonction de la valeur de e, on obtient :

$$\sigma_p^e\, d_{r,s} = d_{r,p-1}\sigma_{p-1}\, \sigma_p\, \sigma_{p-1}^e\, d_{p+1,s}.$$

La relation (2.7) permet de faire commuter les tresses σ_{p-1}^e et $d_{p+1,s}$:

$$\sigma_p^e \; d_{r,s} = d_{r,p-1}\sigma_{p-1} \; \sigma_p \; d_{p+1,s}\sigma_{p-1}^e.$$

En regroupant les différents morceaux à l'aide de la relation (2.6), on obtient (2.9). La relation (2.8) est une conséquence immédiate de (2.9) et de l'écriture (2.4) de la tresse $d_{p,q}$. □

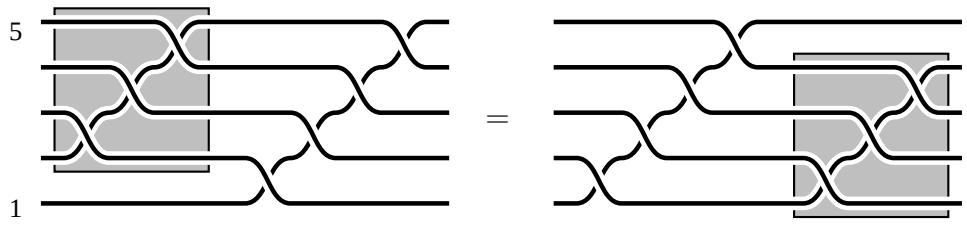


FIG. 2.4 : Illustration de la relation (2.8) : passage de la tresse $d_{2,5}$ (posée sur un carré grisé) au travers de la tresse $d_{1,5}$.

D'autres relations portant sur les tresses $d_{p,q}$ apparaîtrons dans la suite. Nous avons choisi de ne pas les donner ici et de ne les introduire qu'au moment opportun.

1.3 Relations entre les tresses $a_{p,q}$

A partir des relations satisfaites par les tresses $d_{p,q}$, nous pouvons maintenant donner la démonstration de la proposition 1.4.

Démonstration de la proposition 1.4 . Tout d'abord vérifions que les relations (2.2) et (2.3) sont respectées dans B_n une fois qu'on a remplacé les tresses $a_{p,q}$ par leurs expressions comme Σ_n-mots par la définition 1.1. La tresse $a_{p,q}$ est un produit de σ_i avec i appartenant à $[p, q-1]$. Si les intervalles $[p, q]$ et $[r, s]$ sont disjoints alors les intervalles $[p, q-1]$ et $[r, s-1]$ sont au moins à distance 2. Ainsi tout σ_i apparaissant dans l'expression de $a_{p,q}$ commute avec les σ_j apparaissant dans l'expression de $a_{r,s}$.

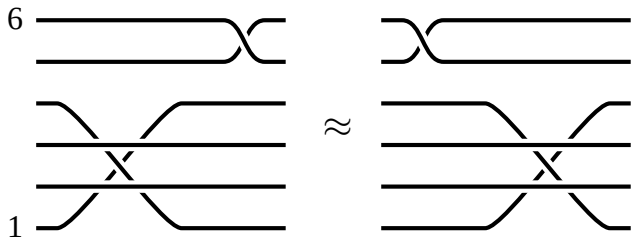


FIG. 2.5 : Illustration de la relation (2.2) lorsque $[p, q]$ et $[r, s]$ sont disjoints.

Supposons maintenant que l'intervalle $[p, q]$ soit niché dans $[r, s]$. La relation (2.5), implique que la tresse $a_{p,q} \; a_{r,s}$ s'écrit $d_{p,q} \; d_{p,q-1}^{-1} \; d_{r,s} \; d_{r,s-1}^{-1}$. La relation (2.8) permet alors de faire passer les tresses $d_{p,q-1}^{-1}$ et $d_{p,q}$ au travers de $d_{r,s}$:

$$a_{p,q} \; a_{r,s} = d_{r,s} \; d_{p-1,q-1} \; d_{p-1,q-2}^{-1} \; d_{r,s-1}^{-1}.$$

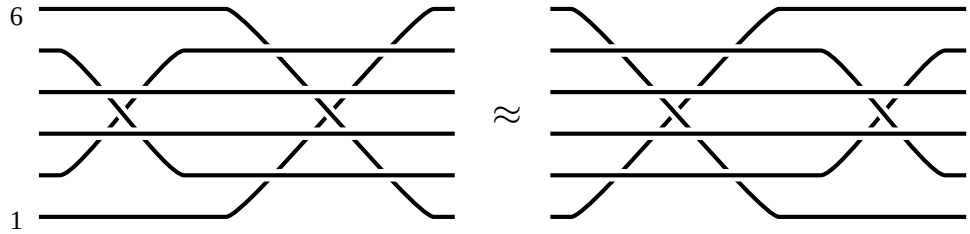


FIG. 2.6 : Illustration de la relation (2.2) lorsque $[p, q]$ est niché dans $[r, s]$.

Comme on a $r < p < q \leqslant s-1$, on utilise deux fois l'inverse de la relation (2.8) pour obtenir

$$a_{p,q}\, a_{r,s} = d_{r,s}\, d_{r,s-1}^{-1}\, d_{p,q}\, d_{p,q-1}^{-1} = a_{r,s}\, a_{p,q}.$$

Montrons que la relation (2.3) est satisfaite. Pour cela on va montrer que les trois tresses de la relation sont égales à $d_{q+1,r}^{-1}\, d_{p,r}\, d_{p,q-1}^{-1}$.
La relation (2.1) permet d'écrire $a_{p,q}\, a_{q,r}$ comme le produit $d_{p,q}\, d_{p,q-1}^{-1}\, d_{q,r}\, d_{q,r-1}^{-1}$. Par la relation (2.7) la tresse $d_{p,q-1}^{-1}$ commute avec $d_{q,r}$ et $d_{q,r-1}^{-1}$:

$$a_{p,q}\, a_{q,r} = d_{p,q}\, d_{q,r}\, d_{q,r-1}^{-1}\, d_{p,q-1}^{-1} = d_{p,r}\, d_{q,r-1}^{-1}\, d_{p,q-1}^{-1},$$

où à l'aide de la relation (2.6) on a regroupé les tresses $d_{p,q}$ et $d_{q,r}$ pour obtenir la deuxième égalité. La relation (2.8) implique $d_{p,r}\, d_{q,r-1}^{-1} = d_{q+1,r}^{-1}\, d_{p,r}$, et on obtient l'égalité souhaitée. A partir de l'égalité $a_{q,r}\, a_{p,r} = d_{q,r}\, d_{q,r-1}^{-1}\, d_{p,r}\, d_{p,r-1}^{-1}$, on utilise la relation (2.8) pour faire passer $d_{q,r-1}^{-1}$ au travers de $d_{q,r}$ et obtenir

$$a_{q,r}\, a_{p,r} = d_{q+1,r}^{-1}\, d_{q,r}\, d_{p,r}\, d_{p,r-1}^{-1}.$$

En utilisant la relation (2.8) pour faire passer $d_{q,r}$ au travers de $d_{p,r}$, on arrive à

$$a_{q,r}\, a_{p,r} = d_{q+1,r}^{-1}\, d_{p,r}\, d_{q-1,r-1}\, d_{p,r-1}^{-1} = d_{q+1,r}^{-1}\, d_{p,r}\, d_{p,q-1}^{-1},$$

la deuxième égalité étant une conséquence de (2.4) et de réductions libres. La relation (2.1) implique $a_{p,r}\, a_{p,q} = d_{p,r}\, d_{p,r-1}^{-1}\, d_{p,q}\, d_{p,q-1}^{-1}$. En utilisant la relation (2.8) on fait passer $d_{p,r-1}^{-1}$ puis $d_{p,q}$ au travers de $d_{p,r}$, pour obtenir

$$a_{p,r}\, a_{p,q} = d_{p+1,r}^{-1}\, d_{p,r}\, d_{p,q}\, d_{p,q-1}^{-1} = d_{p+1,r}^{-1}\, d_{p+1,q+1}\, d_{p,r}\, d_{p,q-1}^{-1}.$$

Enfin, à l'aide des expressions de $d_{p+1,r}^{-1}$ et $d_{p,q}$, on obtient l'égalité souhaitée.

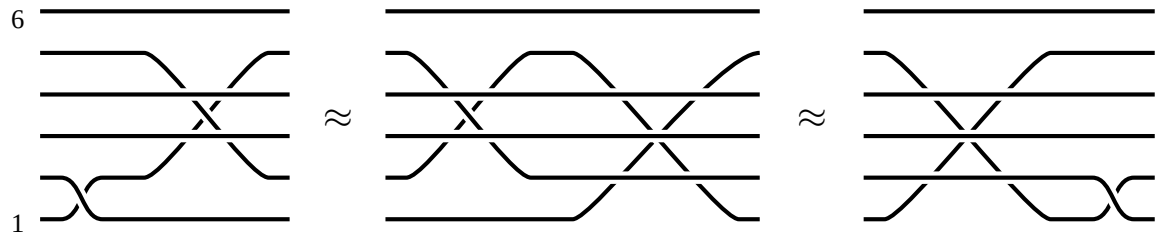


FIG. 2.7 : Illustration de la relation (2.3).

Comme $a_{i,i+1}$ est égale à σ_i, pour montrer que B_n est présenté par les générateurs A_n soumis aux relations (2.2) et (2.3), il suffit d'établir que les relations suivantes sont conséquences des relations (2.2) et (2.3).

$$a_{i,i+1}\, a_{j,j+1} = a_{j,j+1}\, a_{i,i+1} \qquad \text{pour } |i-j| \geqslant 2 \qquad (2.10)$$

$$a_{i,i+1}\, a_{j,j+1}\, a_{i,i+1} = a_{j,j+1}\, a_{i,i+1}\, a_{j,j+1} \qquad \text{pour } |i-j| = 1 \qquad (2.11)$$

$$a_{i,j} = (a_{i,i+1} \dots a_{j-2,j-1})\, a_{j-1,j}\, (a_{j-2,j-1}^{-1} \dots a_{i,i+1}^{-1}) \qquad \text{pour } 1 \leqslant i < j \leqslant n \qquad (2.12)$$

Les intervalles $[i, i+1]$ et $[j, j+1]$ étant disjoints, la relation (2.2) implique (2.10). Pour (2.11), on peut supposer par symétrie $j = i+1$. En utilisant successivement la relation (2.3) sur les mots $a_{i,i+1}\, a_{i+1,i+2}$ et $a_{i,i+2}\, a_{i,i+1}$, on obtient

$$a_{i,i+1}\, a_{i+1,i+2}\, a_{i,i+1} = a_{i+1,i+2}\, a_{i,i+2}\, a_{i,i+1} = a_{i+1,i+2}\, a_{i,i+1}\, a_{i+1,i+2},$$

ce qui implique (2.11). Montrons la relation (2.12). Pour $j = i+1$, elle devient $a_{i,j} = a_{i,j}$, qui est évidemment vraie. Supposons $j > i+1$. On utilise la relation (2.3) pour transformer successivement $a_{j-k-1,j-k}\, a_{j-k,j}$ en $a_{j-k-1,j}\, a_{j-k-1,j-k}$ pour $k = 1, \dots, j-(i+1)$:

$$\begin{aligned}(a_{i,i+1} \dots a_{j-2,j-1})\, a_{j-1,j}\, (a_{j-2,j-1}^{-1} \dots a_{i,i+1}^{-1}) &= (a_{i,i+1} \dots a_{j-3,j-2})\, a_{j-2,j}\, (a_{j-3,j-2}^{-1} \dots a_{i,i+1}^{-1}) \\ &= (a_{i,i+1} \dots a_{j-4,j-3})\, a_{j-3,j}\, (a_{j-4,j-3}^{-1} \dots a_{i,i+1}^{-1}) \\ &= \dots = (a_{i,i+1})\, a_{i+1,j}\, (a_{i,i+1}^{-1}) = a_{i,j}.\end{aligned}$$

Ceci termine la démonstration. □

Définition 1.7. On appelle *monoïde de tresses dual* à n brins et on note B_n^{+*}, le monoïde de présentation :

$$\left\langle A_n \;\middle|\; \begin{array}{ll} a_{p,q}\, a_{r,s} = a_{r,s}\, a_{p,q} & \text{pour } [p,q] \text{ et } [r,s] \text{ nichés ou disjoints,} \\ a_{p,q}\, a_{q,r} = a_{q,r}\, a_{p,r} = a_{p,r}\, a_{p,q} & \text{pour } 1 \leqslant p < q < r \leqslant n \end{array} \right\rangle^{+}. \qquad (2.13)$$

On note $\equiv^{+*}$ la relation de A_n^* engendrée par (2.2) et (2.3). Les relations (2.2) et (2.3) préservant la longueur, deux mots équivalents sont de même longueur. On définit alors la longueur d'une tresse β de B_n^{+*}, notée $|\beta|$, comme la longueur d'un mot représentant β. Pour un monoïde, posséder une longueur est une propriété forte. Ceci implique par exemple que 1 est le seul élément inversible.

Proposition 1.8. *Le monoïde B_n^{+*} ne contient pas d'inversible autre que* 1.

Démonstration. Supposons que β soit un élément inversible de B_n^{+*}. Il existe alors une tresse γ vérifiant $\beta\gamma = 1$ et donc $|\beta\gamma| = 0$. Ainsi on a $|\beta| + |\gamma| = 0$, impliquant $|\beta| = |\gamma| = 0$. □

Nous venons de montrer que le groupe de tresses admet la présentation $\langle A_n \mid \mathcal{R} \rangle$, où $\mathcal{R}$ désigne les relations (2.2) et (2.3). Le monoïde B_n^{+*} étant de présentation $\langle A_n \mid \mathcal{R} \rangle^{+}$, on peut alors se demander s'il satisfait les conditions de Ore (théorème I.2.20).

2 Partitions non croisées et simples de B_n^{+*}

Tout d'abord, remarquons qu'il existe un morphisme naturel π de B_n^{+*} dans $\mathfrak{S}_n$ envoyant $a_{p,q}$ sur la transposition (p, q). Bien sûr, le morphisme π n'est pas injectif. Cependant il permet l'étude de B_n^{+*} à l'aide du groupe symétrique $\mathfrak{S}_n$.

De telles considérations ont été faites par F.A. Garside, dans le contexte du monoïde de tresses positives [Gar69]. Ceci lui a permis de donner une solution algorithmiquement efficace au problème du mot et une solution au problème de conjuguaison. L'élément clé dans [Gar69] est la construction d'un certain ensemble de tresses positives, dites *simples*, qui sont en bijection avec les éléments de $\mathfrak{S}_n$. Plus précisément, il existe un ordre $\preccurlyeq^R$ sur $\mathfrak{S}_n$ tel que l'ensemble des simples munis de la division à droite soit isomorphe à l'ensemble ordonné $(\mathfrak{S}_n, \preccurlyeq^R)$.

J.S. Birman, K.H. Ko et S.J. Lee ont montré que l'on peut définir une notion analogue de simples sur le monoïde B_n^{+*}. Ce point a été ensuite redémontré de manière indépendante par T. Brady dans [Bra01] et par D. Bessis dans [Bes03] (dans un contexte plus général).

Le but de cette section est de définir et décrire les simples de B_n^{+*}. Dans un premier temps nous définissons un ordre $\preccurlyeq^T$ qui jouera le même rôle que $\preccurlyeq^R$ dans la cas de B_n^+. Puis nous introduirons les partitions non croisées de $\{1, \dots, n\}$ qui permettent une description efficace de $(\mathfrak{S}_n, \preccurlyeq^T)$. Enfin nous donnerons une définition des simples pour B_n^{+*}.

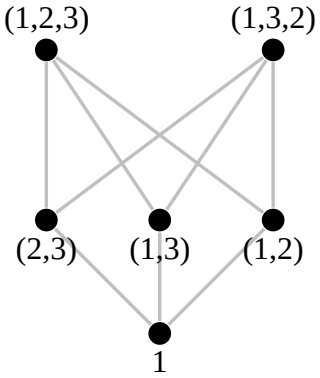
2.1 Un ordre partiel sur $\mathfrak{S}_n$

Cette partie reprend en partie l'article de T. Brady [BRS07]. Soit T_n l'ensemble des transpositions de $\mathfrak{S}_n$. Pour τ dans $\mathfrak{S}_n$, on appelle *longueur de transposition* de τ, notée $\ell_n^T(\tau)$, la distance de l'élément neutre de $\mathfrak{S}_n$ à τ dans le graphe de Cayley de $\mathfrak{S}_n$ relativement à T_n. En d'autres mots, $\ell_n^T(\tau)$ est le nombre minimal de transpositions nécessaires à l'écriture de la permutation τ. Pour tout τ et τ' dans $\mathfrak{S}_n$, on a alors la relation

$$\ell_n^T(\tau\,\tau') \leqslant \ell_n^T(\tau) + \ell_n^T(\tau'). \tag{2.14}$$

Tout produit de $\ell_n^T(\tau)$ transpositions représentant τ est appelé *expression régulière* de τ.

Exemple 2.1. Dans $\mathfrak{S}_3$ les permutations sont $(1,2)$, $(2,3)$ et $(1,3)$. Le graphe de Cayley de $\mathfrak{S}_3$ relativement à T_3 est :



On a $\ell^T(1) = 0$, $\ell^T((1,2)) = \ell^T((1,3)) = \ell^T((2,3)) = 1$ et $\ell^T((1,2,3)) = \ell^T((1,3,2)) = 2$.

Le résultat suivant décrit le comportement de $\ell_n^T(.)$ vis-à-vis de la multiplication à gauche et à droite par une transposition.

Lemme 2.2. *Pour τ une permutation de $\mathfrak{S}_n$ et t une transpostion de $\mathfrak{S}_n$, on a*

$$\ell_n^T(t \cdot \tau) = \ell_n^T(\tau) \pm 1 \quad \textit{et} \quad \ell_n^T(\tau \cdot t) = \ell_n^T(\tau) \pm 1.$$

Démonstration. Par la relation (2.14), on a $\ell_n^T(t \cdot \tau) \leqslant 1 + \ell_n^T(\tau)$. S'il existait une expression régulière $t_1 \cdot \ldots \cdot t_\ell$ de $t \cdot \tau$ avec $\ell \leqslant \ell_n^T(t) - 2$ alors $t \cdot t_1 \cdot \ldots \cdot t_\ell$ serait une expression de τ de longueur

inférieur ou égale à $\ell_n^T(t)-1$, ce qui est impossible. On a donc $\ell_n^T(\tau)-1 \leqslant \ell_n^T(t\cdot\tau) \leqslant \ell_n^T(\tau)+1$. La premutation $t\cdot\tau$ étant de signature différente de celle τ on ne peut pas avoir $\ell_n^T(t\tau)=\ell_n^T(\tau)$. Un argument symétrique traite le cas de $\ell_n^T(\tau\cdot t)$. □

Le résultat suivant permet à partir d'une expression régulière d'en obtenir d'autres, il sera souvent utilisé dans les démonstrations faisant intervenir des expressions régulières.

Lemme 2.3. *Pour $t_1\cdot\ldots\cdot t_\ell$ une expression régulière de τ de $\mathfrak{S}_n$ et $1\leqslant i_1<\ldots<i_k\leqslant\ell$ une suite d'entiers, il existe une expression régulière de τ commençant par $t_{i_1}\cdot\ldots\cdot t_{i_k}$.*

Démonstration. Pour t et t' deux transpositions de $\mathfrak{S}_n$, il existe une transposition t'' vérifiant la relation $tt'=t''t$: si on a $t'=(r,s)$, alors on prend $t''=(t(r),t(s))$. Ainsi, on peut pousser la transposition t_{i_1} vers la gauche dans l'expression régulière $t_1\cdot\ldots\cdot t_\ell$ sans en changer la longueur. On recommence en poussant t_{i_2} vers la gauche jusqu'à la droite de t_{i_1}, etc. □

Une permutation τ de $\mathfrak{S}_{n-1}$, peut être vue comme une permutation de $\mathfrak{S}_n$ laissant n fixe. Quels sont alors les liens entre $\ell_{n-1}^T(\tau)$ et $\ell_n^T(\tau)$? Le résultat suivant va nous permettre de répondre à la question.

Proposition 2.4. *Si une permutation τ fixe p, alors toute expression régulière de τ ne contient pas de transposition de la forme (p,q).*

Démonstration. Soit τ une permutation fixant p et $t_1\cdot\ldots\cdot t_k$ une expression régulière de τ. Supposons par l'absurde que t_i soit de la forme (p,q_1). D'après le lemme 2.3, il existe une expression régulière $t_1^{(1)}\cdot\ldots\cdot t_k^{(1)}$ de τ avec $t_1^{(1)}=(p,q_1)$. Posons $\tau^{(1)}=t_2^{(1)}\cdot\ldots\cdot t_k^{(1)}$. Comme τ fixe p on a $\tau^{(1)}(p)=q_1$. Il s'ensuit qu'il existe $i\geqslant 2$ tel que $t_i^{(1)}$ soit (p,q_2) pour un certain q_2. Il existe alors une expression régulière $t_1^{(2)}\cdot\ldots\cdot t_k^{(2)}$ de τ avec $t_1^{(2)}=(p,q_1)$ et $t_2^{(2)}=(p,q_2)$. Posons $\tau^{(2)}=t_3^{(2)}\cdot\ldots\cdot t_k^{(2)}$. En fonction de la valeur de q_2, la permutation $\tau^{(2)}$ peut fixer p ou non. On continue ce procédé jusqu'à obtenir

$$\tau=(p,q_1)\cdot\ldots\cdot(p,q_\ell)\cdot\tau^{(\ell)},$$

où $\tau^{(\ell)}$ fixe p. Si les entiers q_i sont deux à deux distincts, on a

$$(p,q_1)\cdot\ldots\cdot(p,q_\ell)=(p,q_\ell,q_{\ell-1},\ldots,q_1),$$

impliquant $\tau(p)=q_\ell$, ce qui est impossible. Ainsi il existe i et j vérifiant $q_i=q_j$ avec $i<j$. Le lemme 2.3 assure alors qu'il existe une expression régulière $t_1'\cdot\ldots\cdot t_k'$ de τ avec $t_1'=t_2'=(p,q_i)$. On obtient donc $\tau=t_3'\cdot\ldots\cdot t_k'$. il s'en suit que l'expression $t_1\cdot\ldots\cdot t_k$ de τ n'est pas régulière. □

Une des conséquences de la proposition 2.4 est l'égalité $\ell_{n-1}^T(\tau)=\ell_n^T(\tau)$ pour τ dans $\mathfrak{S}_{n-1}$. On peut donc enlever l'indice n du symbole ℓ_n^T et utiliser ℓ^T sans risque de confusion.

Nous allons maintenant établir plusieurs résultats permettant de donner la longueur d'une permutation à partir de sa décomposition en cycles à supports disjoints.

Lemme 2.5. (T. Brady, [Bra01]) *Si $c_1,\ldots,c_k$ sont des cycles à supports disjoints, on a*

$$\ell^T(c_1\cdot\ldots\cdot c_k)=\ell^T(c_1)+\ldots+\ell^T(c_k). \tag{2.15}$$

Démonstration. Posons $\tau = c_1 \cdot ... \cdot c_k$. Montrons d'abord que toute transposition d'une expression régulière de τ a son support inclus dans celui d'un c_i. Notons $S_1, ..., S_k$ les supports des cycles $c_1, ..., c_k$. Soit $t_1 \cdot ... \cdot t_\ell$ une expression régulière de τ. Supposons par l'absurde que le support de t_i ne soit pas inclus dans un S_j. Quitte à renommer les cycles, on peut supposer que t_i soit la transposition (p, q_1) avec $p \in S_1$ et $q_1 \in S_1$. Par le lemme 2.3, il existe une expression régulière $t_1^{(1)} \cdot ... \cdot t_\ell^{(1)}$ de τ avec $t_1^{(1)} = (p, q_1)$. Posons $\tau^{(1)} = t_2^{(1)} \cdot ... \cdot t_\ell^{(1)}$. Si $\tau^{(1)}$ ne fixe pas p, il existe $i \geqslant 2$ tel que $t_i^{(1)}$ soit de la forme (p, q_2) pour un certain q_2. Par le lemme 2.3, il existe une expression régulière $t_1^{(2)} \cdot ... \cdot t_\ell^{(2)}$ de τ avec $t_1^{(2)} = (p, q_1)$, $t_2^{(2)} = (p, q_2)$. Posons

$$\tau^{(2)} = t_2^{(2)} \cdot ... \cdot t_\ell^{(2)}.$$

Notons $S^{(2)}$ l'ensemble S_j contenant q_2. La permutation $\tau^{(2)}$ peut alors fixer p ou non. On continue ce procédé jusqu'à obtenir l'expression régulière

$$(p, q_1) \cdot ... \cdot (p, q'_\ell) \cdot \tau^{(\ell')}$$

de τ où $\tau^{(\ell)}$ fixe p. Si les q_j sont deux à deux distincts, on a

$$(p, q_1) \cdot ... \cdot (p, q_{\ell'}) = (p, q_{\ell'}, q_{\ell'-1}, ..., q_1),$$

impliquant $\tau(q_1) = p$, ce qui est impossible d'après l'hypothèse faite sur t_i. Ainsi il existe j et j' vérifiant $q_j = q_{j'}$ avec $j < j'$. Le lemme 2.3 assure alors qu'il existe une expression régulière

$$t'_1 \cdot ... \cdot t'_\ell$$

de τ avec $t'_1 = t'_2 = (p, q_i)$. On obtient alors $\tau = t'_3 \cdot ... \cdot t'_\ell$, et, donc, $t_1 \cdot ... \cdot t_\ell$ ne peut pas être une expression régulière de τ.

Nous pouvons maintenant terminer la démonstration. Notons I_i l'ensemble des indices j tels que le support de t_j soit inclus dans celui de c_i. Par ce qui précéde, on a

$$\ell = \mathrm{card}(I_1) + ... + \mathrm{card}(I_k),$$

ce qui implique

$$\prod_{j \in I_i} \tau_j = c_i.$$

On a donc $\ell(c_i) \leqslant \mathrm{card}(I_i)$. Ainsi nous avons obtenu la relation $\ell \geqslant \ell(c_1) + ... + \ell(c_k)$. Par ailleurs la relation (2.14) donne $\ell \leqslant \ell(c_1) + ... + \ell(c_k)$; on a donc l'égalité souhaitée. □

Grâce au lemme 2.5 nous pouvons calculer la longueur de transposition d'une permutation à partir de celles de ses cycles à supports disjoints. Il nous faut maintenant donner la longueur de transposition d'un cycle.

Proposition 2.6. (T. Brady, [Bra01]) *Si c est un cycle de longueur k, alors on a $\ell^T(c) = k-1$.*

Démonstration. Posons $c = (p_1, ..., p_k)$. Montrons $\ell^T(c) = k-1$ par induction sur k. C'est évidemment vrai pour $k = 2$. Soit $t_1 \cdot ... \cdot t_\ell$ une expression régulière de c (en particulier on a $\ell = \ell^T(c)$). Posons $(p_i, p_j) = \tau_1$ avec $i < j$. On a alors :

$$\tau_1 \cdot c = (p_i, p_j)(p_1, ..., p_k) = (p_1, ..., p_{i-1}, p_j, p_{j+1}, ..., p_k) \cdot (p_i, p_{i+1}, ..., p_{j-2}, p_{j-1}).$$

Le lemme 2.5 combiné à l'hypothèse d'induction donne alors

$$\ell^T(\tau_1 \cdot c) = (i - 1 + k - j + 1) - 1 + (j - 1 - i + 1) - 1,$$

c'est-à-dire, $\ell^T(\tau_1 \cdot c) = k - 2$. On a donc montré $\ell - 1 = k - 2$, ce qui implique $\ell = k-1$. □

Nous pouvons maintenant calculer la longueur de transposition d'une permutation à partir de sa décomposition en cycles à supports disjoints :

Corollaire 2.7. (T. Brady, [Bra01]) *Si τ est une permutation de $\mathfrak{S}_n$ qui se décompose en k cycles à supports disjoints (les cycles de longueur 1 sont aussi comptés), alors on a $\ell^T(\tau) = n - k$.*

Démonstration. Soit $c_1 \cdot ... \cdot c_k$ une décomposition de τ en produit de cycles à supports disjoints. Notons ℓ_i la longueur du cycle c_i. Comme même les cycles de longueur 1 apparaissent dans cette décomposition, on a $\ell_1 + ... + \ell_k = n$. Le lemme 2.5 implique

$$\ell^T(\tau) = \ell^T(c_1) + ... + \ell^T(c_k).$$

Ainsi, par la proposition 2.6, on a

$$\ell^T(\tau) = (\ell_1 - 1) + ... + (\ell_k - 1),$$

et donc $\ell^T(\tau) = n - k$. □

Exemple 2.8. Considérons la permutation τ de $\mathfrak{S}_9$ définie par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 1 & 5 & 9 & 2 & 7 & 6 & 4 \end{pmatrix}.$$

Une décomposition de τ en produit de cycles à supports disjoints est

$$(1,3) \cdot (2,8,6) \cdot (4,5,9) \cdot (7).$$

La longueur de transposition de τ est donc 5 ($9 - 4 = 5$). L'expression

$$(1,3) \cdot (2,8) \cdot (8,6) \cdot (4,5) \cdot (5,9)$$

de τ est donc régulière.

La longueur de transposition nous permet de définir une relation binaire $\preccurlyeq^T$ sur $\mathfrak{S}_n$ de la façon suivante :

Définition 2.9. Pour τ et τ' éléments de $\mathfrak{S}_n$, on pose $\tau \preccurlyeq^T \tau'$ si on a $\ell^T(\tau') = \ell^T(\tau) + \ell^T(\tau^{-1}\tau')$,

Une autre manière d'interpréter la relation $\preccurlyeq^T$ est : on a $\tau \preccurlyeq^T \tau'$ si et seulement s'il existe un chemin dans le graphe de Cayley de $\mathfrak{S}_n$ relativement à T_n de longueur $\ell^T(\tau')$ allant de 1 à τ' et passant par τ, ce qui signifie qu'il existe une expression régulière de τ' commençant par une expression régulière de τ.

Exemple 2.10. On reprend l'exemple 2.1. Tous les éléments de $\mathfrak{S}_3$ inférieurs ou égaux à la permutation $(1,2,3)$ vis à vis de $\preccurlyeq^T$ sont 1, $(1,2)$, $(1,3)$, $(2,3)$ et $(1,2,3)$.

À la section I.3, nous avons défini un ordre strict sur un ensemble X comme étant une relation binaire sur X anti-réflexive et transitive. Un *ordre non strict* $\preccurlyeq$ sur un ensemble X est une relation binaire réfléxive ($x \preccurlyeq x$), antisymétrique ($x \preccurlyeq y$ et $y \preccurlyeq x$ implique $x = y$) et transitive ($x \preccurlyeq y$ et $y \preccurlyeq z$ implique $x \preccurlyeq z$).

Proposition 2.11. *La relation $\preccurlyeq^T$ est un ordre non strict sur $\mathfrak{S}_n$.*

Démonstration. La longueur de transposition de l'identité étant nulle on a $\tau \preccurlyeq^T \tau$, c'est-à-dire, la réfléxivité de $\preccurlyeq^T$.

Montrons que la relation $\preccurlyeq^T$ est antisymétrique. Soient τ et τ' des éléments de $\mathfrak{S}_n$ vérifiant les relations $\tau \preccurlyeq^T \tau'$ et $\tau' \preccurlyeq^T \tau$. Par définition de $\preccurlyeq^T$, on a

$$\ell^T(\tau') = \ell^T(\tau) + \ell^T(\tau^{-1}\tau') \quad \text{et} \quad \ell^T(\tau) = \ell^T(\tau') + \ell^T({\tau'}^{-1}\tau)$$

En substituant la seconde égalité dans la première, on obtient

$$\ell^T(\tau') = \ell^T(\tau') + \ell^T({\tau'}^{-1}\tau) + \ell^T(\tau^{-1}\tau').$$

Il s'ensuit que $\ell^T({\tau'}^{-1}\tau)$ et $\ell^T(\tau^{-1}\tau')$ vallent 0. Or l'identité est la seule permutation de longueur de transposition nulle, ce qui implique $\tau = \tau'$.

Montrons que la relation $\preccurlyeq^T$ est transitive. Soient τ, τ' et τ'' des éléments de $\mathfrak{S}_n$ vérifiant les relations $\tau \preccurlyeq^T \tau'$ et $\tau' \preccurlyeq^T \tau''$. Par définition de $\preccurlyeq^T$, on a

$$\ell^T(\tau') = \ell^T(\tau) + \ell^T(\tau^{-1}\tau') \quad \text{et} \quad \ell^T(\tau'') = \ell^T(\tau') + \ell^T({\tau'}^{-1}\tau'').$$

En substituant la première relation dans la seconde, on obtient

$$\ell^T(\tau'') = \ell^T(\tau) + \ell^T(\tau^{-1}\tau') + \ell^T({\tau'}^{-1}\tau'').$$

La relation (2.14) implique $\ell^T(\tau^{-1}\tau'') \leqslant \ell^T(\tau^{-1}\tau') + \ell^T({\tau'}^{-1}\tau'')$, et donc

$$\ell^T(\tau'') \geqslant \ell^T(\tau) + \ell^T(\tau^{-1}\tau'').$$

Encore par la relation (2.14), on a $\ell^T(\tau'') \leqslant \ell^T(\tau) + \ell^T(\tau^{-1}\tau'')$. Ainsi on a

$$\ell^T(\tau'') = \ell^T(\tau) + \ell^T(\tau^{-1}\tau'').$$

La relation $\tau \preccurlyeq^T \tau''$ est donc vérifiée. □

Par définition de $\preccurlyeq^T$, pour deux permutations τ et τ' de $\mathfrak{S}_n$, on a $\tau \preccurlyeq^T \tau\tau'$ si et seulement si la relation $\ell^T(\tau\tau') = \ell^T(\tau) + \ell^T(\tau')$ est vérifiée. Sous la même condition sur $\ell^T(\tau\tau')$, peut-on avoir la relation $\tau' \preccurlyeq^T \tau\tau'$?

Corollaire 2.12. *Pour τ et τ' dans $\mathfrak{S}_n$, il y a équivalence entre $\tau \preccurlyeq^T \tau\tau'$ et $\tau' \preccurlyeq^T \tau\tau'$.*

Démonstration. La relation $\tau \preccurlyeq^T \tau\tau'$ implique $\ell^T(\tau\tau') = \ell^T(\tau) + \ell^T(\tau')$. Par le lemme 2.3, il existe τ'' dans $\mathfrak{S}_n$ vérifiant $\tau\tau' = \tau'\tau''$ et où $\tau'\tau''$ est une expression régulière. On a donc

$$\ell^T(\tau'\tau'') = \ell^T(\tau') + \ell^T(\tau''),$$

c'est-à-dire, $\tau' \preccurlyeq^T \tau'\tau''$. La relation $\tau\tau' = \tau'\tau''$ implique donc $\tau' \preccurlyeq^T \tau\tau'$. La réciproque se traite de manière symétrique. □

On peut se demander quelles sont les propriétés de l'ensemble ordonné $(\mathfrak{S}_n, \preccurlyeq^T)$. Est-il borné ? Deux éléments quelconques admettent-ils un minorant et un majorant commun ?

Définition 2.13. On dit qu'un ensemble ordonné $(X, \preccurlyeq)$ est un *treillis* si :
– (i) X est borné : il existe m et M dans X tels qu'on ait $m \preccurlyeq x \preccurlyeq M$ pour tout x dans X,
– (ii) pour tout x, y de X, il existe un plus grand minorant de x et y, noté $x \wedge y$,
– (iii) pour tout x, y de X, il existe un plus petit majorant de x et y, noté $x \vee y$.

Malheureusement, pour $n \geqslant 3$, l'ensemble partiellement ordonné $(\mathfrak{S}_n, \preccurlyeq^T)$ n'est pas un treillis. En effet, en reprenant le graphe de Cayley de $\mathfrak{S}_3$ relativement à T_3 donné à l'exemple 2.1, on remarque que $(\mathfrak{S}_3, \preccurlyeq^T)$ n'admet pas de plus grand élément.

2.2 Partitions non croisées

On note $\mathfrak{C}_n$ l'ensemble des éléments de $\mathfrak{S}_n$ inférieur au cycle $(1, \dots, n)$ vis à vis de ℓ^T :

$$\mathfrak{C}_n = \{\tau \in \mathfrak{S}_n,\ \tau \preccurlyeq^T (1, 2, \dots, n)\}. \tag{2.16}$$

Le but de cette sous-section est de donner une description de $\mathfrak{C}_n$ en termes de ce que l'on appellera des *partitions non croisées* et d'établir que $(\mathfrak{C}_n, \preccurlyeq^T)$ est un treillis. Pour cela on introduit un ordre $\preccurlyeq^P$ sur l'ensemble des partitions dites *non croisées* de $\{1, \dots, n\}$, noté P_n^{nc}. On montre alors que $(P_n, \preccurlyeq^P)$ est un treillis. Puis on exhibe un isomorphisme d'ensemble ordonné entre $(P_n^{nc}, \preccurlyeq^P)$ et $(\mathfrak{C}\ \preccurlyeq^T)$.

Définition 2.14. Un sous-ensemble X de $P(\{1, \dots, n\})$ est une *partition* de $\{1, \dots, n\}$ si
– les éléments de X recouvrent $\{1, \dots, n\}$, c'est-à-dire, $\bigcup_{x \in X} x = \{1, \dots, n\}$,
– les éléments de X sont disjoints, c'est-à-dire, pour tous x, y dans X avec $x \neq y$, on a $x \cap y = \emptyset$,
– l'ensemble vide n'appartient pas à X.

On note P_n l'ensemble des partitions de $\{1, \dots, n\}$.

Exemple 2.15. Les partitions de $\{1, 2, 3\}$ sont

$$\{\{1\}, \{2\}, \{3\}\},\ \{\{1\}, \{2, 3\}\},\ \{\{2\}, \{1, 3\}\}, \{\{3\}, \{1, 2\}\} \text{ et } \{\{1, 2, 3\}\}.$$

Nous allons maintenant munir P_n d'une relation d'ordre.

Définition 2.16. Soient X et Y deux éléments de P_n. On pose $X \preccurlyeq^P Y$ si pour tout élément x de X il existe un élément y de Y avec $x \subseteq y$.

La relation $X \preccurlyeq^P Y$ signifie que la partition X est *plus fine* que Y. Clairement la relation $\preccurlyeq^P$ est réflexive, antisymétrique et transitive et définit donc un ordre non strict sur P_n.

Proposition 2.17. *L'ensemble ordonné $(P_n, \preccurlyeq^P)$ est un treillis.*

Démonstration. Posons $m = \{\{1\}, \dots, \{n\}\}$ et $M = \{\{1, \dots, n\}\}$. La partition m est la plus fine de P_n, tandis que M et la moins fine. La condition (i) de la définition 2.13 est donc vérifiée.

Montrons (ii) de la définition 2.13. Soient X et Y deux éléments de P_n. Notons $x_1, \dots, x_k$ les éléments de X et $y_1, \dots, y_\ell$ ceux de Y. Pour i dans $\{1, \dots, k\}$ et j dans $\{1, \dots, \ell\}$. Posons

$$Z = \{x_i \cap y_j \mid i = 1, \dots, k;\ j = 1, \dots, \ell\} - \{\emptyset\}.$$

Par construction Z est un sous-ensemble de $P(\{1, \dots, n\})$ ne contenant pas l'ensemble vide. Soient z et z' deux éléments distincts de Z. Il existe alors i, i', j, j' avec $(i, j) \neq (i', j')$ et vérifiant $z = x_i \cap y_j$ et $z' = x_{i'} \cap y_{j'}$. L'ensemble $z \cap z'$ est donc inclus dans $(x_i \cap x_{i'}) \cap (y_j \cap y_{j'})$ qui est vide car l'un des deux ensembles $x_i \cap x_{i'}$ et $y_j \cap y_{j'}$ l'est. Par ailleurs, on a

$$\bigcup_{z \in Z} z = \bigcup_{i=1}^{k} \bigcup_{j=1}^{\ell} x_i \cap y_j = \bigcup_{i=1}^{k} \left(x_i \cap \bigcup_{j=1}^{\ell} y_j \right) = \bigcup_{i=1}^{k} \left(x_i \cap \{1, \dots, n\} \right) = \bigcup_{i=1}^{k} x_i = \{1, \dots, n\}.$$

L'ensemble Z est donc une partition de $\{1, \dots, n\}$. Montrons que c'est le plus grand minorant de X et Y. Soit W une partition de $\{1, \dots, n\}$, satisfaisant $W \preccurlyeq^P X$ et $W \preccurlyeq^P Y$. Par définition

de $\preccurlyeq^P$, pour tout w dans W, il existe x dans X et y dans Y vérifiant $w \subseteq x$ et $w \subseteq y$. L'ensemble w est donc inclus dans $x \cap y$. La partition W est alors fine que Z, c'est-à-dire, qu'on a $W \preccurlyeq^P Z$. Il y a donc égalité entre Z et $X \wedge Y$.

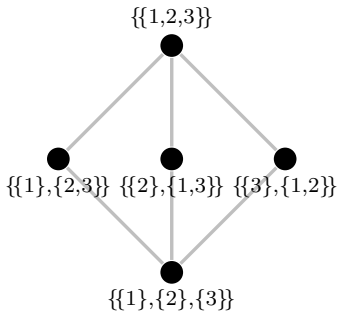
Montrons (iii) de la définition 2.13. Soient X et Y deux éléments de P_n. Posons

$$z_i = \bigcup \{x \in X \mid \exists y \in Y (y \cap x \neq \emptyset \text{ et } y \cap x_i \neq \emptyset)\},$$

et $Z = \{z_1, \dots, z_k\}$. Par construction Z est un sous-ensemble de $P(\{1, \dots, n\})$ ne contenant pas l'ensemble vide. Comme x_i est inclus dans z_i, l'ensemble Z recouvre $\{1, \dots, n\}$. Soient z_i et z_j deux éléments de Z ayant une intersection non vide. Comme Y recouvre $\{1, \dots, n\}$, il existe y dans Y tel que $z_i \cap y$ et $z_j \cap y$ soient non vides. Soit k tel que $x_k \cap y$ soit non vide. On a donc $x_k \subseteq z_i$ et $x_k \subseteq z_j$. Par conséquent l'ensemble des éléments de Y intersectant x_k et le même que celui des éléments de Y intersectant z_i. On a donc $z_i = z_k$. De même, on a la relation $z_j = z_k$. L'ensemble Z est donc une partition de $\{1, \dots, n\}$. Par construction Z est clairement un majorant de X. Soit y un élément de Y. Comme X recouvre $\{1, \dots, n\}$, il existe un élément x_k de X tel que l'intersection de x_k et y soit non vide. Il s'ensuit que y est inclus dans z_k (par construction des z_i) et donc que Z est un majorant de Y. Montrons que Z est le plus petit majorant de X et Y. Soit W une partition de $\{1, \dots, n\}$, satisfaisant $X \preccurlyeq^P W$ et $Y \preccurlyeq^P W$. Soit y un élément de Y, il existe alors w dans Wavec $y \subseteq w$. De plus, pour tout x de X tel que l'intersection de x et y soit non vide, x doit être inclus dans w car W est moins fine que X. On en déduit que z_i est inclus dans w, puis la relation $Z \preccurlyeq^P W$ □

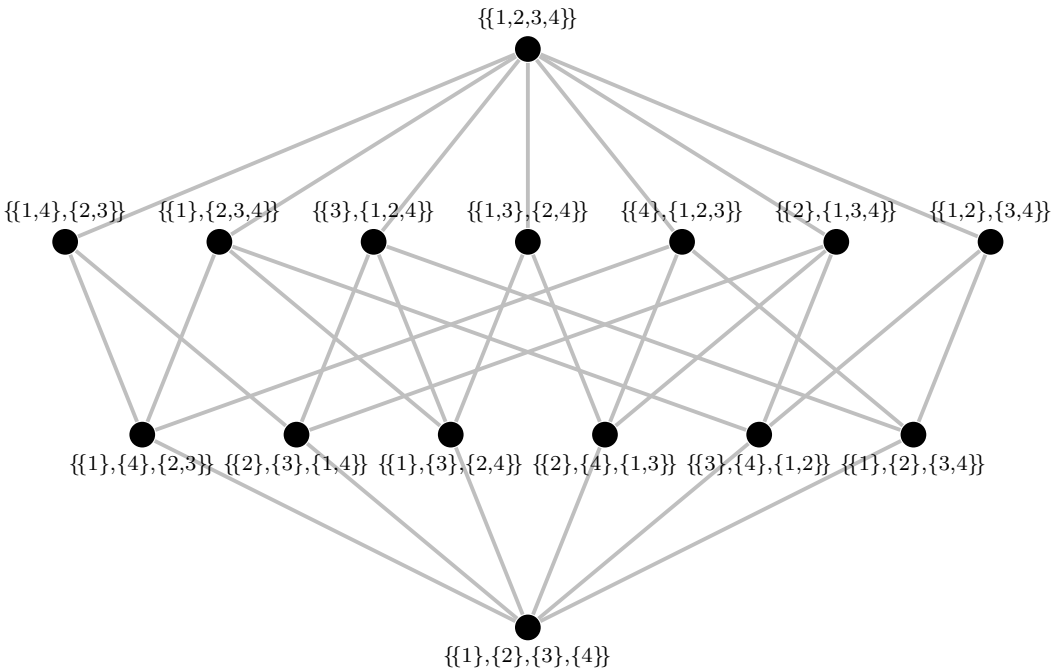
Pour représenter un ensemble ordonné, il est commode d'en utiliser une représentation visuelle. On construit un diagramme de Hasse d'un ensemble ordonné $(X, \leqslant)$ de la façon qui suit. Les éléments de X sont représentés par des points. Pour x et y deux éléments distincts de X vérifiant $x \leqslant y$, l'ordonnée du point représentant y est strictement plus grande que celle du point représentant x. De plus s'il n'existe pas z dans X vérifiant $x \leqslant z \leqslant y$, alors on lie les points correspondants à x et y par un segment.

Exemple 2.18. Le diagramme de Hasse de $(P_3, \preccurlyeq^P)$ est



On peut reconnaître qu'un ensemble ordonné $(X, \leqslant)$ est un treillis à l'aide de son diagramme de Hasse. L'existence d'un minorant m est équivalent au fait que le diagramme de Hasse de $(X, \leqslant)$ ait un point de plus petite ordonnée P et que pour tout point Q du diagramme, il existe un chemin d'arêtes reliant P à Q. L'interprétation de l'existence d'un majorant est symétrique. Les conditions (i) et (ii) de la définition 2.13 se lisent de la même manière ; nous ne les détaillons pas ici.

Exemple 2.19. Le diagramme de Hasse de $(P_4, \preccurlyeq^P)$ est



Définition 2.20. Soit X une partition de $\{1, \dots, n\}$. On dit que deux éléments distincts x et y de X se *croisent* s'il existe quatre entiers i, j, k et ℓ vérifiant $i, k \in x$, $j, \ell \in y$ et $i < j < k < \ell$. On dit que X est *non croisée* si deux éléments quelconques distincts x et y ne se croisent pas.

On note P_n^{nc} l'ensemble des partitions non croisées de $\{1, \dots, n\}$. Toutes les partitions de $\{1, 2, 3\}$ sont non croisées, on a donc $P_3 = P_3^{nc}$. Par contre pour $n \geqslant 4$, on a $P_n^{nc} \subsetneq P_n$. En effet, la partition $\{\{1, 3\}, \{2, 4, \dots, n\}\}$ est croisée.

Proposition 2.21. (G. Kreweras, [Kre72]) *L'ensemble ordonné $(P_n^{nc}, \preccurlyeq^P)$ est un treillis.*

Démonstration. Les partitions $\{\{1, \dots, n\}\}$ et $\{\{1\}, \dots, \{n\}\}$ sont non croisées et sont respectivement le ninorant et le majorant de $(P_n^{nc}, \preccurlyeq^P)$. La condition (i) de la définition 2.13 est donc vérifiée.

Montrons le (ii) de la défintion 2.13. Soient X et Y deux éléments de P_n^{nc}. Notons $x_1, \dots, x_k$ les éléments de X et $y_1, \dots, y_k$ ceux de Y. Pour i dans $\{1, \dots, k\}$ et j dans $\{1, \dots, \ell\}$. Posons

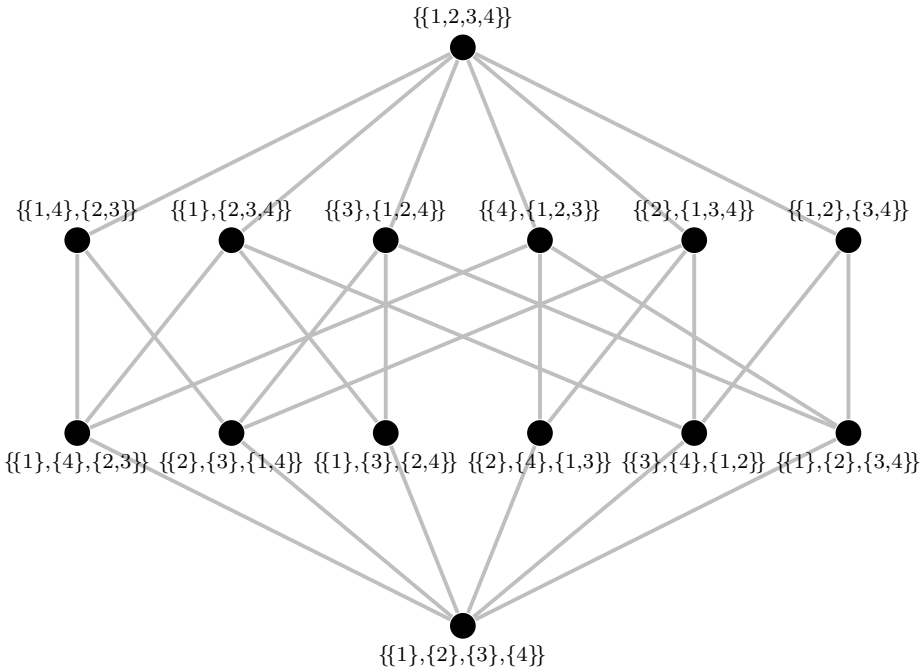
$$Z = \{x_i \cap y_j \mid i = 1, \dots, k;\ j = 1, \dots, \ell\} - \{\emptyset\}.$$

Dans la démonstration de 2.17, on a déjà montré que Z est la plus grande partition vis-à-vis de $\preccurlyeq^P$ vérifiant les relations $Z \preccurlyeq^P X$ et $Z \preccurlyeq^P Y$. Cependant, on ne sait pas encore si Z est une partition non croisée. Soient z et z' des éléments de Z. Il existe i, i', j et j' vérifiant les relations $z = x_i \cap y_j$ et $z' = x_{i'} \cap y_{j'}$. Supposons qu'il existe k, ℓ dans z et k', ℓ' dans z' vérifiant la relation $k < k' < \ell < \ell'$. Comme k et ℓ sont en particulier des éléments de x_i et k', ℓ' des éléments de $x_{i'}$, on a l'égalité $i = i'$. Sinon les éléments x_i et x_i se croiseraient, ce qui est en contradiction avec l'hypothèse que X est une partition non croisée. De même on montre l'égalité entre j et j'. Il s'ensuit que z est égale à z' et que Z est une partition non croisée.

Montrons le (iii) de la définition 2.13. Soient X et Y deux éléments de P_n^{nc}. Notons E l'ensemble des majorants de X et Y. L'ensemble E est non vide par le (i) de la définition 2.13. Notons $Z_1, ..., Z_\ell$ les éléments de E. La partition non croisée $Z_1 \wedge Z_2 \wedge ... \wedge Z_\ell$ est alors le plus petit majorant de X et de Y. □

Pour X et Y deux partitions non croisées, on note $X \wedge^{nc} Y$ (*resp.* $X \vee^{nc} Y$) le plus grand minorant (*resp.* le plus petit majorant) de X et Y. Les symboles $\wedge$ et $\vee$ étant réservés aux partitions quelconques. Donnons une description de $X \vee^{nc} Y$. En général $X \vee Y$ n'est pas une partition non croisée. Par exemple pour $X = \{\{1,3\},\{2\},\{4\}\}$ et $Y = \{\{1\},\{2,4\}\{3\}\}$, on a $X \vee Y = \{\{1,3\},\{2,4\}\}$, qui est croisée. Cependant, il est montré dans [Kre72] que la permutation non croisée $X \vee^{nc} Y$ est obtenue de $X \vee Y$ en fusionnant les éléments qui se croisent ; c'est ce qu'on pense naturellement faire.

Exemple 2.22. Le diagramme de Hasse de $(P_4^{nc}, \preccurlyeq^P)$ est



On remarque que ce diagramme est obtenu à partir de celui de l'exemple 2.19 en ôtant le point correspondant à la partition croisée $\{\{1,3\},\{2,4\}\}$ et les arêtes qui lui sont attachées.

Nous rappelons que le but de cette section est de décrire $(\mathfrak{C}_n, \preccurlyeq^T)$ à l'aide de partitions non croisées de $\{1,\dots,n\}$. Pour cela, nous construisons une application η de P_n^{nc} dans $\mathfrak{C}_n$. Soit x une partie non vide de $\{1,\dots,n\}$. Notons $i_1,\dots,i_k$ les éléments de x dans l'ordre croissant. On note alors c_x le cycle $(i_1,\dots,i_k)$ de $\mathfrak{S}_n$.

Définition 2.23. On définit une application η de P_n dans $\mathfrak{S}_n$ par :

$$\begin{array}{ccc} P_n & \to & \mathfrak{S}_n \\ \{x_1,\dots,x_k\} & \mapsto & c_{x_1}\cdot\ldots\cdot c_{x_k} \end{array} \tag{2.17}$$

La fonction η est bien définie. En effet, deux éléments distincts x et y d'une partition X de l'ensemble $\{1,\dots,n\}$ sont disjoints et donc les cycles c_x et c_y commutent.

Exemple 2.24. Pour $n = 3$, on a

$$\eta(X) = \begin{cases} 1 & \text{pour } X = \{\{1\},\{2\},\{3\}\} \\ (2,3) & \text{pour } X = \{1,\{2,3\}\} \\ (1,3) & \text{pour } X = \{2,\{1,3\}\} \\ (1,2) & \text{pour } X = \{3,\{1,2\}\} \\ (1,2,3) & \text{pour } X = \{\{1,2,3\}\} \end{cases}$$

Avant d'établir que η est un isomorphisme d'ensembles ordonnés entre $(P_n^{nc}, \preccurlyeq^P)$ et $(\mathfrak{C}_n, \preccurlyeq^T)$, nous donnons divers résultats intermédiaires qui nous seront utiles lors de la démonstration du théorème 2.29.

Lemme 2.25. (T. Brady, [Bra01]) *Pour tout sous-ensemble non vide x de $\{1, \dots, n\}$, on a la relation $c_x \preccurlyeq^T (1, \dots, n)$.*

Démonstration. Soit x une partie non vide de $\{1 \dots, n\}$. Notons $p_1, \dots, p_k$ les éléments de x dans l'ordre croissant. On vérifie

$$\begin{aligned} c_x^{-1} \cdot (1, \dots, n) &= (p_k, \dots, p_1) \cdot (1, \dots, n) \\ &= (1, \dots, p_1{-}1, p_k, p_k{+}1, \dots, n) \cdot (p_1, \dots, p_2{-}1) \cdot \dots \cdot (p_{k-1}, \dots, p_k{-}1). \end{aligned} \quad (2.18)$$

La permutation $c_x^{-1} \cdot (1, \dots, n)$ est donc produit de k cycles à supports disjoints. Par le corollaire 2.7, on obtient $\ell^T(c_x^{-1} \cdot (1, \dots, n)) = n - k$. Ainsi on a

$$n - 1 = \ell^T((1, \dots, n)) = \ell^T(c_x) + \ell^T(c_x^{-1} \cdot (1, \dots, n)) = k - 1 + n - k,$$

c'est-à-dire, $c_x \preccurlyeq^T (1, \dots, n)$. □

Lemme 2.26. *Soient τ_1' et τ_2' deux permutations à supports disjoints. Alors les relations $\tau_1 \preccurlyeq^T \tau_1'$ et $\tau_2 \preccurlyeq^T \tau_2'$ impliquent $\tau_1\tau_2 \preccurlyeq^T \tau_1'\tau_2'$.*

Démonstration. Une conséquence du lemme 2.5 est que pour toutes permutations τ et τ' à supports disjoints, on a $\ell^T(\tau\tau') = \ell^T(\tau) + \ell^T(\tau')$. Ainsi, on a

$$\ell^T(\tau_1'\tau_2') = \ell^T(\tau_1') + \ell^T(\tau_2') = \ell^T(\tau_1) + \ell^T(\tau_2) + \ell^T(\tau_1^{-1}\tau_1') + \ell^T(\tau_2^{-1}\tau_2').$$

Par la proposition 2.4, la relation $\tau \preccurlyeq^T \tau'$ implique que le support de τ est inclus dans celui de τ'. Les permutations τ_1 et τ_2 sont donc à supports disjoints. De même, les permutations $\tau_1^{-1}\tau_1'$ et $\tau_2^{-1}\tau_2'$ sont à supports disjoints. La proposition 2.4 implique alors :

$$\ell^T(\tau_1'\tau_2') = \ell^T(\tau_1\tau_2) + \ell^T(\tau_1^{-1}\tau_1'\tau_2^{-1}\tau_2') = \ell^T(\tau_1\tau_2) + \ell^T((\tau_1\tau_2)^{-1}\tau_1'\tau_2'),$$

la dernière égalité étant conséquence du fait que $\tau_1^{-1}\tau_1'$ et τ_2^{-1} sont à supports disjoints et donc commutent. □

Lemme 2.27. (T. Brady, [Bra01]) *Soient p, q, r et s des entiers vérifiant*

$$1 \leqslant p < q < r < s \leqslant n.$$

Alors on a :
– *(i) la permutation $(p, r) \cdot (q, s)$ n'est pas un élément de $\mathfrak{C}_n$.*
– *(ii) la permutation (p, r, q) n'est pas un élément de $\mathfrak{C}_n$.*

Démonstration. (i) Posons $\tau = (p, r) \cdot (q, s)$. On a alors

$$\tau \cdot (1, \dots, n) = (1, \dots, p{-}1, r, \dots, s{-}1, q, \dots, r{-}1, p, \dots, q{-}1, s, \dots, n)$$

Comme $\tau = \tau^{-1}$, par le corollaire 2.7, on a :

$$\ell^T(\tau) + \ell^T(\tau \cdot (1, \dots, n)) = 2 + n - 1 = n + 1.$$

Par la proposition 2.6, on a $\ell^T((1,\dots,n)) = n-1$. On ne peut donc pas avoir $\tau \preccurlyeq^T (1,\dots,n)$, c'est-à-dire, τ n'est pas un élément de $\mathfrak{C}_n$.

(ii) Posons $\tau = (p,r,q)$. Alors τ^{-1} vaut (p,q,r) et on a

$$(p,q,r)\cdot(1,\dots,n) = (1,\dots,p-1,q,\dots,r-1,p,\dots,q-1,r,\dots,n)$$

Par le corollaire 2.7, on a :

$$\ell^T(\tau) + \ell^T(\tau^{-1}\cdot(1,\dots,n)) = 2+n-1 = n+1.$$

Par la proposition 2.6, on a $\ell^T((1,\dots,n)) = n-1$. On ne peut donc pas avoir $\tau \preccurlyeq^T (1,\dots,n)$, c'est-à-dire, τ n'est pas un élément de $\mathfrak{C}_n$. □

Voici un premier résultat permettant de lier $\mathfrak{C}_n$ aux partitions non croisées.

Théorème 2.28. (T. Brady, [Bra01]) *L'application η est une bijection de P_n^{nc} sur $\mathfrak{C}_n$.*

Démonstration. Montrons par induction sur n que l'image de P_n^{nc} par η est incluse dans $\mathfrak{C}_n$. Soit X un élément de P_n^{nc}. Posons $X = \{x_1,\dots,x_\ell\}$. Pour $n=1$ et $n=2$, l'image de X par η est soit l'élément trivial, soit $(1,\dots,n)$ lui même, qui sont clairement dans $\mathfrak{C}_n$. Supposons $n \geqslant 3$. Notons $p_1,\dots,p_k$ les éléments de x_1 par ordre croissant. Par le lemme 2.25, on a

$$c_{x_1} \preccurlyeq^T (1,\dots,n). \tag{2.19}$$

Soient $q_1,\dots,q_{k'}$ les éléments de x_i classés dans l'ordre croissant pour $i \geqslant 2$. Comme x_1 et x_i sont non croisées, on est dans l'un des cas suivants :

– (i) $p_k < q_1$ ou $q_{k'} < p_1$,

– (ii) il existe t vérifiant $p_t < q_1$ et $q_{k'} < p_{t+1}$,

– (iii) il existe t vérifiant $q_1 < p_t$ et $p_{t+1} < q_{k'}$.

Dans les cas (i) et (iii), x_i est inclus dans

$$\{1,\dots,p_1-1,p_k,p_k+1,\dots,n\}$$

tandis que dans le cas (ii) il est inclus dans $\{p_t,\dots,p_{t+1}-1\}$. Soit $c'_1\cdot\ldots\cdot c'_{n'}$ une décomposition de $c_{x_1}^{-1}(1,\dots,n)$ en cycles à supports disjoints. En reprenant la relation (2.18) établie lors de la démonstration du lemme 2.25, on obtient que le support de c_{x_i} est inclus dans l'un des c'_i pour tout $i \geqslant 2$.

Notons I_i l'ensemble de tous les indices $j \geqslant 2$ tels que le support de c_{x_j} soit inclus dans celui de c'_i. Posons $X_i = \{x_j \mid j \in I_i\}$, pour $i = 1,\dots,n'$. Comme X est une partition non croisée, l'ensemble X_i est une partition non croisée du support de c'_i. Par hypothèse d'induction, on a la relation $\eta(X_i) \preccurlyeq^T c'_i$. Le lemme 2.26 implique

$$\eta(X_1)\cdot\ldots\cdot\eta(X_{n'}) \preccurlyeq^T c'_1\cdot\ldots\cdot c'_{n'}.$$

Ainsi on obtient $c_{x_1}^{-1}\eta(X) \preccurlyeq^T c_{x_1}^{-1}(1,\dots,n)$, et donc

$$\ell^T(c_{x_1}^{-1}(1,\dots,n)) = \ell^T(c_{x_1}^{-1}\eta(X)) + \ell^T(\eta(X)^{-1}(1,\dots,n)). \tag{2.20}$$

On obtient alors

$$\begin{aligned}
\ell^T((1,\dots,n)) &= \ell^T(c_{x_1}) + \ell^T(c_{x_1}^{-1}(1,\dots,n)) && \text{par (2.19)},\\
&= \ell^T(c_{x_1}) + \ell^T(c_{x_1}^{-1}\eta(X)) + \ell^T(\eta(X)^{-1}(1,\dots,n)) && \text{par (2.20)},\\
&= \ell^T(c_{x_1}) + \ell^T(c_{x_2}\cdot\ldots\cdot c_{x_k}) + \ell^T(\eta(X)^{-1}(1,\dots,n))\\
&= \ell^T(c_{x_1}\cdot\ldots\cdot c_{x_k}) + \ell^T(\eta(X)^{-1}(1,\dots,n)) && \text{par (2.15)},\\
&= \ell^T(\eta(X)) + \ell^T(\eta(X)^{-1}(1,\dots,n)) && \text{par (2.17)},
\end{aligned}$$

ce qui établit $\eta(X) \preccurlyeq^T (1, \dots, n)$ puis que $\eta(X)$ appartient à $\mathfrak{C}_n$.

Soit τ un élément de $\mathfrak{C}_n$ et $c_1 \cdot \ldots \cdot c_k$ une décomposition de τ en cycles à supports disjoints. Notons x_i le support de c_i. L'ensemble X égal à $\{x_1, \dots, x_k\}$, est une partition de $\{1, \dots, n\}$.

Montrons qu'on a $c_{x_i} = c_i$ pour tout i. Notons $p_1, \dots, p_{k'}$ les éléments de x_1 énumérés dans l'ordre croissant. Il existe alors une bijection de $\{1, \dots, k'\}$, que l'on note ψ, vérifiant $\psi(1) = 1$ et $c_1 = (p_{\psi(1)}, \dots, p_{\psi(k')})$. Si pour tout ℓ, on a $\psi(\ell) = \ell$, les cycles c_1 et c_{x_1} sont les mêmes. Supposons que ce n'est pas le cas et notons i la plus petite valeur de ℓ vérifiant $\psi(\ell) \neq \ell$. Comme $\psi(1)$ vaut 1 par construction de ψ, on a $i \geqslant 2$ et $\psi(i) > i$. Soit j le plus petit entier supérieur à i vérifiant $\psi(j) < \psi(i)$. Notons t_ℓ la transposition $(p_{\psi(\ell)}, p_{\psi(\ell+1)})$ pour $\ell \leqslant k'-1$ et posons $t_{k'} = (p_{\psi(k')}, p_{\psi(1)})$. Par définition de ψ, on a $c_1 = t_1 \cdot \ldots \cdot t_{i-1} \cdot \ldots \cdot t_{j-1} \cdot \ldots t_{k'-1}$. Ainsi par le lemme 2.3, il existe une expression régulière de c_1 commençant pat $t_{i-1}\, t_{j-1}$. En particulier, on a $t_{i-1}t_{j-1} \preccurlyeq^T c_1$. Par ailleurs, par le lemme 2.5, on a la relation $c_1 \preccurlyeq^T (1, \dots, n)$. Donc par transitivité de $\preccurlyeq^T$, on a $t_{i-1}t_{j-1} \preccurlyeq^T (1, \dots, n)$. Pour $j = i+1$, la permutation $t_{i-1}t_{j-1}$ est égale à $(p_{\psi(i-1)}, p_{\psi(i)}, p_{\psi(j)})$, c'est-à-dire, à $(p_{i-1}, p_{\psi(i)}, p_{\psi(j)})$ avec $p_{i-1} < p_{\psi(j)} < p_{\psi(i)}$. On obtient alors une contradiction avec le lemme 2.26 (i). Pour $j > i+1$, la permutation $t_{i-1}t_{j-1}$ est égale à $(p_{\psi(i-1)}, p_{\psi(i)})(p_{\psi(j-1)}, p_{\psi(j)})$, c'est-à-dire à

$$(p_{i-1}, p_{\psi(i)})(p_{\psi(j-1)}, p_i) \quad \text{avec} \quad p_{i-1} < p_i < p_{\psi(i)}.$$

Par définition de j, on a $\psi(j-1) > \psi(i)$ et donc la relation

$$p_{i-1} < p_i < p_{\psi(i)} < p_{\psi(j-1)}.$$

On obtient alors une contradiction avec le lemme 2.26 (ii). On a donc $c_1 = c_{x_1}$, et les autres cycles sont traités de la même manière.

Maintenant, montrons que X est une partition non croisée. Supposons qu'il existe x et y deux éléments croisés de X. Posons $x = \{p_1, \dots, p_\ell\}$ et $y = \{q_1, \dots, q'_\ell\}$. Sans perte de généralité, on peut supposer que x et y se croisent en des valeurs adjacentes, c'est-à-dire qu'il existe i et j vérifiant

$$p_i < q_j < p_{i+1} < q_{j+1}.$$

Notons t_i la transposition (p_i, p_{i+1}) et t_j la transposition (q_j, q_{j+1}). Comme il existe une expression régulière de c_x (*resp.* c_y contenant t_i, (*resp.* t_j), le lemme 2.3 assure que la permutation τ admet une expression régulière commençant par $t_i t_j$. On a donc $t_i t_j \preccurlyeq^T \tau$. Ainsi, par transitivité de $\preccurlyeq^T$, on a $t_i t_j \preccurlyeq^T (1, \dots, n)$. Ceci est impossible par le lemme 2.26.

On vient ainsi de construire une application ν de $\mathfrak{C}_n$ dans P_n^{nc} par :

$$\nu(\tau) = \{\text{support}(c_1), \dots, \text{support}(c_k)\},$$

où $c_1 \cdot \ldots \cdot c_k$ est une décomposition en cycles à supports disjoints de τ (on tient compte aussi des cycles de longueur 1). On vérifie immédiatement qu'on a $\eta \circ \nu = \mathrm{id}_{P_n^{nc}}$ ainsi que $\nu \circ \eta = \mathrm{id}_{\mathfrak{C}_n}$. L'application η est donc une bijection de P_n^{nc} sur l'ensemble $\mathfrak{C}_n$. □

Théorème 2.29. (T. Brady, [Bra01]) *L'application η est un isomorphisme d'ensemble ordonné entre $(P_n^{nc}, \preccurlyeq^P)$ et $(\mathfrak{C}_n, \preccurlyeq^T)$.*

Démonstration. Soient X et Y deux partitions non croisées.

Supposons $X \preccurlyeq^P Y$ et montrons la relation $\eta(X) \preccurlyeq^T \eta(Y)$. Posons $X = \{x_1, \dots, x_k\}$ et $Y = \{y_1, \dots, y_{k'}\}$. Notons I_j l'ensemble des indices i tels que x_i soit inclus dans y_j. La relation $X \preccurlyeq^P Y$, qui signifie que la partition X est plus fine Y, implique

$$I_1 \cup \ldots \cup I_{k'} = \{1, \dots, k\}.$$

Montrons que pour tout j appartenant à $\{1, \dots, k'\}$, on a

$$\prod_{i \in I_j} c_{x_i} \preccurlyeq^T c_{y_j}. \tag{2.21}$$

Supposons $j = 1$. Notons $p_1, \dots, p_\ell$ les éléments de y_1 dans l'ordre croissant. Notons ψ l'application de y_1 dans $\{1, \dots, \ell\}$ envoyant p_t sur t. Notons Z la partition $\{\psi(x_i), i \in I_1\}$ de $\{1, \dots, \ell\}$. Comme la partition X est non croisée et que ψ est une application croissante, la partition Z est non croisée. Le théorème 2.28 implique alors que $\eta(Z)$ appartient à $\mathfrak{C}_\ell$, c'est-à-dire, la relation $\eta(Z) \preccurlyeq^T (1, \dots, \ell)$. Ainsi de $c_{\psi(y_1)} = (1, \dots, \ell)$, on obtient la relation

$$\eta(Z) = \prod_{i \in I_j} c_{\psi(x_i)} \preccurlyeq^T c_{\psi(y_1)},$$

ce qui implique (2.21) pour $j = 1$ car ψ n'est rien d'autre qu'un réétiquetage. On établit (2.21) pour les autres valeurs de j de la même manière. Comme les c_{y_j} sont à supports disjoints, le lemme 2.5 assure la relation

$$\prod_{j=1}^{k'} \prod_{i \in I_j} c_{x_i} \preccurlyeq^T \prod_{j=1}^{k'} c_{y_j}.$$

On a donc obtenu $\eta(X) \preccurlyeq^T \eta(Y)$.

Maintenant supposons $X \not\preccurlyeq^P Y$ et montrons $\eta(X) \not\preccurlyeq^T \eta(Y)$. La relation $X \not\preccurlyeq^P Y$ implique qu'il existe x dans X qui n'est inclus dans aucun élément de Y. Notons $p_1, \dots, p_k$ les éléments de x. Il existe alors un entier i et deux éléments y et y' de Y tels que p_i soit inclus dans y et que p_{i+1} soit inclus dans y'. Il s'ensuit que la permutation $(p_i, p_{i+1})c_y c_{y'}$ est un cycle. Ainsi la permutation $(p_i, p_{i+1})\eta(Y)$ se décompose en $(\mathrm{card}(Y) - 1)$ cycles à supports disjoints. Par le corollaire 2.7, on a

$$\ell^T(\eta(Y)) = n - \mathrm{card}(Y) \quad \text{et} \quad \ell^T((p_i, p_{i+1})\eta(Y)) = n - \mathrm{card}(Y) + 1.$$

Nous avons donc obtenu la relation

$$\ell^T((p_i, p_{i+1})\eta(Y)) = \ell^T(\eta(Y)) + 1.$$

D'un autre côté, le lemme 2.3 assure que $\eta(X)$ admet une expression régulière $t_1 \cdot \ldots \cdot t_\ell$ où t_1 est égale à (p_i, p_{i+1}). Comme la relation $\ell^T(t\tau) = \ell^T(\tau) \pm 1$ est satisfaite pour toute permutation τ et toute transposition t, on obtient

$$\begin{aligned}
\ell^T(\eta(X)^{-1}\eta(Y)) &= \ell^T(t_\ell \cdot \ldots \cdot t_2 \cdot (p_i, p_{i+1}) \cdot \eta(Y)) \\
&\geqslant \ell^T((p_i, p_{i+1}) \cdot \eta(Y)) - \ell + 1 \\
&\geqslant \ell^T(\eta(Y)) - \ell + 2 \\
&\geqslant \ell^T(\eta(Y)) - \ell^T(\eta(X)) + 2.
\end{aligned}$$

Ainsi on a $\ell^T(\eta(X)) + \ell^T(\eta(X)^{-1}\eta(Y)) \geqslant \ell^T(\eta(Y)) + 2$, ce qui implique $\eta(X) \not\preccurlyeq^T \eta(Y)$. □

Comme, d'après la proposition 2.21, l'ensemble ordonné $(P_n^{nc}, \preccurlyeq^P)$ est un treillis, le théorème 2.29 implique qu'il en est de même pour $(\mathfrak{C}_n, \preccurlyeq^T)$.

2.3 Simples de B_n^{+*}

Nous allons maintenant isoler certains éléments de B_n^{+*}, appelés simples de B_n^{+*}, à partir de l'ensemble $\mathfrak{C}_n$. Ceci nous permet en particulier de comprendre la combinatoire de B_n^{+*} à partir de celle de $\mathfrak{C}_n$: nous allons montrer que les simples de B_n^{+*} forment un treillis pour la divisibilité isomorphe au treillis $(\mathfrak{C}_n, \preccurlyeq^T)$.

Commençons d'abord par définir une application r de $\mathfrak{C}_n$ dans B_n^{+*}.

Définition 2.30. On définit une application r de $\mathfrak{C}_n$ dans B_n^{+*} de la façon suivante :
– pour une transposition (p, q), on pose $r((p, q)) = a_{p,q}$,
– pour une permutation τ d'expression régulière $t_1 \dots t_k$ on pose

$$r(\tau) = r(t_1) \cdot \dots \cdot r(t_k). \tag{2.22}$$

À la proposition 2.4, nous avons montré que l'expression régulière d'une permutation ne dépend pas du groupe $\mathfrak{S}_n$ dans lequel elle est vue. Il s'ensuit que l'application r ne dépend pas de n.

Il n'est pas évident, *a priori*, que l'application r soit bien définie. En effet une permutation possède plusieurs expressions régulières. Il faut donc s'assurer que r ne dépend pas de l'expression régulière choisie.

Proposition 2.31. (T. Brady, [Bra01]) *L'application r est bien définie.*

Démonstration. Soient c et c' deux cycles à supports disjoints de $\mathfrak{S}_n$ tels que les partitions $\eta^{-1}(c)$ et $\eta^{-1}(c')$ soient non croisées. Notons i (*resp.* i') le plus petit élément du support de c (*resp.* c') et notons j (*resp.* j') le plus grand élément du support de c'. Comme c et c' sont à supports disjoints et que les partitions $\eta^{-1}(c)$ et $\eta^{-1}(c')$ sont non croisées, les intervalles $[i, j]$ et $[i', j']$ sont disjoints. La relation 2.2 garantit alors que les lettres $a_{p,q}$ constituant l'expression (2.22) de $r(c)$ commutent avec celle de $r(c')$. On a donc $r(c\,c') \equiv^{+*} r(c'\,c)$. Ainsi pour une permutation τ de l'ensemble $\mathfrak{C}_n$, l'élément $r(\tau)$ de B_n^{+*} ne dépend pas de l'ordre de l'écriture des cycles à supports disjoints de τ.

Montrons que $r(c)$, où c est un cycle de $\mathfrak{C}_n$, est bien définie. Pour simplifier les notations, supposons $c = (1, \dots, k)$ (si ce n'est pas le cas on utilise un réétiquetage). Soit $t_1 \cdot \dots \cdot t_{k-1}$ une expression régulière de c. Posons $t_\ell = (i_\ell, j_\ell)$ pour $\ell = 1, \dots, k-1$. Nous allons montrer par induction sur k l'équivalence suivante :

$$r(c) = r(t_1) \cdot \dots \cdot r(t_k) \equiv^{+*} a_{1,2} \cdot \dots \cdot a_{k-1,k}. \tag{2.23}$$

Pour $k = 2$, c'est évident. Supposons $k \geqslant 3$. Soit ℓ le plus grand indice vérifiant $t_\ell = (1, p)$ pour un certain p : un tel ℓ existe car c ne fixe pas 1. Nous allons maintenant pousser $r(t_\ell)$ vers la gauche dans l'expression de $r(c)$ sans créer de $a_{1,q}$ et décrire les changements apportés à l'expression régulière. Pour $\ell \geqslant 1$, notons (r, s) la transposition $t_{\ell-1}$ avec $r < s$. On a différents cas à traiter. Si $\{1, p\} \cap \{r, s\}$ est vide, alors, par le theorème 2.28, les ensembles $\{1, p\}$ et $\{r, s\}$ sont non croisés. Ainsi la relation (2.2) implique $a_{r,s}a_{1,p} \equiv^{+*} a_{1,p}a_{r,s}$. Notons qu'on a $(r, s)(1, p) = (1, p)(r, s)$. Si $a_{r,s}$ vaut $a_{1,p}$, alors $t_1 \cdot \dots \cdot t_{k-1}$ ne serait pas une expression régulière de c. Si r vaut 1, alors $(1, s)(1, p)$ est égale à $(1, p, s)$. Par le theorème 2.28, on doit alors avoir $p < s$. Ainsi la relation (2.3) implique $a_{1,s}a_{1,p} \equiv^{+*} a_{1,p}a_{p,s}$. Notons qu'on a la relation $(1, s)(1, p) = (1, p)(p, s)$. Si r vaut p, alors $(p, s)(1, p)$ est égale à $(1, s, p)$ avec la relation $s > p$. Ceci, par le theorème 2.28, est en contradiction avec $c \in \mathfrak{C}_n$. On ne peut

pas avoir l'égalité $s = 1$ car r doit être plus petit que s. Si s vaut p, alors la relation (2.3) implique $a_{r,p}a_{1,p} \equiv^{+*} a_{1,r}a_{r,p}$. Notons qu'on a $(r,p)(1,p) = (1,r)(r,p)$.

On réitère ce procédé jusqu'à obtenir une expression régulière de c de la forme

$$(1,p) \cdot t'_2 \cdot \ldots \cdot t'_{k-1},$$

où les transpositions t'_ℓ laissent 1 fixe. Comme c envoie 1 sur 2, on a nécessairement $p = 2$. Ainsi $t'_2 \cdot \ldots \cdot t'_{k-1}$ est une expression régulière de $(2, \ldots, k)$. En parallèle on a obtenu

$$r(c) = a_{1,2}\, r((2, \ldots, k)).$$

Par hypothèse d'induction, on obtient le résultat souhaité. □

Lemme 2.32. *Pour τ dans $\mathfrak{C}_n$, on a $|r(\tau)| = \ell^T(\tau)$.*

Démonstration. Soit $t_1 \cdot \ldots \cdot t_k$ une expression régulière de τ. Alors, par définition de r on a

$$r(\tau) = r(t_1) \cdot \ldots \cdot r(t_k),$$

et donc $|r(\tau)| = \ell^T(\tau)$. □

Proposition 2.33. *Pour τ et τ' éléments de $\mathfrak{C}_n$ tels que $\tau\tau'$ soit dans $\mathfrak{C}_n$, on a :*

$$\ell^T(\tau\,\tau') = \ell^T(\tau) + \ell^T(\tau') \Leftrightarrow r(\tau\,\tau') = r(\tau)\, r(\tau').$$

Démonstration. La condition $\ell^T(\tau\,\tau') = \ell^T(\tau) + \ell^T(\tau')$ signifie qu'il existe une expression régulière de $\tau\tau'$ dont un suffixe vaut τ et le préfixe associé τ'. La relation $r(\tau\,\tau') = r(\tau)\, r(\tau')$ est alors une conséquence directe de la définition de r.

Montrons la réciproque. La relation $r(\tau\tau') = r(\tau) \cdot r(\tau')$ implique

$$|r(\tau\tau'))| = |r(\tau)| + |r(\tau')|,$$

car $\equiv^{+*}$ préserve la longueur des mots. Par définition de r, pour toute permutation τ'', on a $|r(\tau'')| = \ell^T(\tau'')$. On a donc $\ell^T(\tau\,\tau') = \ell^T(\tau) + \ell^T(\tau')$. □

Un élément β de B_n^{+*} est dit *simple* s'il appartient à l'image de $\mathfrak{C}_n$ par r. L'ensemble des simples de B_n^{+*} est donc $r(\mathfrak{C}_n)$ et est noté $S(B_n^{+*})$.

Par le théorème 2.28, les simples de B_n^{+*} sont en bijection avec les partitions non croisées.

Exemple 2.34. Les simples de B_3^{+*} sont les images par r de $\varepsilon, (1,2), (2,3), (1,3)$ et $(1,2,3)$ et sont donc $1, a_{1,2}, a_{2,3}, a_{1,3}$ et δ_3.

On note δ_n le simple de B_n^{+*}, qui est l'image par r du cycle $(1, \ldots, n)$. Comme une expression régulière de $(1, \ldots, n)$ est $(1,2) \cdot \ldots \cdot (n-1,n)$, on a

$$\delta_n = r((1, \ldots, n)) = r((1,2)) \cdot \ldots \cdot r((n-1,n)) = a_{1,2} \cdot \ldots \cdot a_{n-1,n}.$$

Sa particularité vient du fait que la seule connaissance de δ_n permet de reconstruire les simples de B_n^{+*}. Pour être plus précis, on doit définir les relations de divisibilité à gauche et à droite dans le monoïde B_n^{+*}.

Définition 2.35. Soient β et β' deux éléments de B_n^{+*}.
– On dit que β *divise à gauche* β' ou de manière équivalente que β' est un *multiple à droite* de β, noté $\beta \preccurlyeq \beta'$, s'il existe γ dans B_n^{+*} avec $\beta' = \beta\gamma$.
– On dit que β' *divise à droite* β ou de manière équivalente que β' est un *multiple à gauche* de β, noté $\beta \succcurlyeq \beta'$, s'il existe γ dans B_n^{+*} avec $\gamma\beta' = \beta$.

Nous obtenons alors la caractérisation suivante des simples de B_n^{+*}.

Proposition 2.36. *Soit β un élément de B_n^{+*}. Il y a équivalence entre :*
– (i) *β est un simple de B_n^{+*},*
– (ii) *β divise à gauche δ_n,*
– (iii) *β divise à droite δ_n.*

Afin de démonter la proposition 2.36, nous définissons une application de B_n^{+*} dans $\mathfrak{S}_n$ dont la restriction aux simples est la réciproque de r.

Définition 2.37. Soit π le morphisme de B_n^{+*} dans $\mathfrak{S}_n$ défini par $\pi(a_{p,q}) = (p, q)$.

Tout d'abord, vérifions que l'application π est bien définie.

Proposition 2.38. *Le morphisme π est bien défini. De plus on a $\pi(r(\tau)) = \tau$ pour tout τ de $\mathfrak{C}_n$.*

Démonstration. Si les intervalles $[p, q]$ et $[r, s]$ sont nichés ou disjoints, les transpositions $\pi(a_{p,q})$ et $\pi(a_{r,s})$ commutent. Pour $p < q < r$, on a

$$(p, q)(q, r) = (q, r)(p, r) = (p, r)(p, q) = (p, q, r).$$

L'application π est donc bien définie.

Notons $t_1 \cdot \ldots \cdot t_\ell$ l'expression régulière d'une permutation τ de $\mathfrak{C}_n$. Par construction de r, on a $r(\tau) = r(t_1) \cdot \ldots \cdot r(t_\ell)$. Chacun des $r(t_i)$ est un générateur de Birman–Ko–Lee. Ainsi par définition de π, on $\pi(r(t_i)) = t_i$, puis $\pi(r(\tau)) = t_1 \cdot \ldots \cdot t_\ell = \tau$. □

Une conséquence de la proposition 2.38 est que l'application r est injective et donc définit une bijection entre $\mathfrak{C}_n$ et les simples de B_n^{+*}. Par le théorème 2.28, on en déduit que les simples de B_n^{+*} sont en bijection avec les partitions non croisées de $\{1, \ldots, n\}$.

Notons que pour τ dans $\mathfrak{C}_n$, on a $\pi(r(\tau)) = \tau$. Ce qui implique $\ell^T(\pi(r(\tau))) = \ell^T(\tau)$. De plus par le lemme 2.32 on a $|r(\tau)| = \ell^T(\tau)$. On a donc $\ell^T(\pi(r(\tau))) = |r(\tau)|$. Dans le cas général, on a le résultat suivant :

Lemme 2.39. *Soient β et β' deux éléments de B_n^{+*} :*
– (i) *on a $\ell^T(\pi(\beta)) \leqslant |\beta|$,*
– (ii) *on a $\ell^T(\pi(\beta\beta')) \leqslant |\beta| + \ell^T(\pi(\beta'))$,*
– (iii) *on a $\ell^T(\pi(\beta\beta')) \leqslant \ell^T(\pi(\beta)) + |\beta'|$.*
– (iv) *si on a $\ell^T(\pi(\beta)) = |\beta|$ avec $\pi(\beta)$ dans $\mathfrak{C}_n$, alors β est un simple de B_n^{+*}.*

Démonstration. Montrons (i). Soit $x_1 \ldots x_k$ un A_n^+-mot représentant β. La permutation $\pi(\beta)$ est donc égale au produit de transpositions $\pi(x_1) \cdot \ldots \cdot \pi(x_k)$. Une expression régulière de $\pi(\beta)$ étant constituée d'au plus k transpositions, on a $\ell^T(\pi(\beta)) \leqslant |\beta|$.

Montrons (ii) et (iii). De $\pi(\beta\beta') = \pi(\beta)\pi(\beta')$, on déduit

$$\ell^T(\pi(\beta\beta')) \leqslant \ell^T(\pi(\beta)) + \ell^T(\pi(\beta')).$$

On conclut alors par (i).

Montrons (iv) par induction sur $|\beta|$. Pour $\beta = 1$ on a $\beta = r(1)$. Pour $\beta = a_{p,q}$ on a la relation $\beta = r((p,q))$. Ainsi tout élément de B_n^{+*} de longueur 0 ou 1 est un simple. Supposons $|\beta| \geqslant 2$. Il existe alors β' de B_n^{+*} et deux entiers p et q vérifiant $\beta = \beta' \cdot a_{p,q}$. La relation $\ell^T(\pi(\beta)) = |\beta|$ implique que $\pi(\beta')(p,q)$ est une expression régulière de $\pi(\beta)$ si $\pi(\beta')$ est exprimée par une de ses expressions régulières. On a donc $\ell^T(\pi(\beta')) = |\beta| - 1$, puis l'égalité $\ell^T(\pi(\beta')) = |\beta'|$. Comme $\ell^T(\pi(\beta')(p,q))$ vaut $\ell^T(\pi(\beta')) + 1$, on a $\pi(\beta') \preccurlyeq^T \pi(\beta)$. Par hypothèse, on a $\pi(\beta) \preccurlyeq^T (1, \dots, n)$. Ainsi, par transitivité de $\preccurlyeq^T$, la permutation $\pi(\beta')$ appartient à l'ensemble $\mathfrak{C}_n$. L'hypothèse d'induction implique alors que β' est un simple, c'est-à-dire qu'on a $\beta = r(\pi(\beta))$. On a donc obtenu la relation $\beta = r(\pi(\beta'')) \cdot a_{p,q}$. Dès que $\pi(\beta')$ est exprimée par une expression régulière, l'expression $\pi(\beta') \cdot (p,q)$ est régulière. On a donc la relation $\beta = r(\pi(\beta') \cdot (p,q))$ et la tresse β est simple. □

Nous pouvons maintenant établir la proposition 2.36.

Démonstration de la proposition 2.36 . Notons c le cycle $(1, \dots, n)$.

Montrons que (i) implique (ii) et que (i) implique (iii). Comme, par hypothèse, β est un simple, il existe τ dans $\mathfrak{C}_n$ avec $r(\tau) = \beta$. Par définition de $\mathfrak{C}_n$, on a $\ell^T(c) = \ell^T(\tau) + \ell^T(\tau^{-1}c)$. Ainsi, par la proposition 2.33, on a $r(c) = r(\tau) \cdot r(\tau^{-1}c)$, c'est-à-dire, $\delta_n = \beta \cdot r(\tau^{-1}c)$. D'autre part, comme la longueur de transposition est stable par conjuguaison, on a

$$\ell^T(c) = \ell^T(\tau) + \ell^T(c\,\tau^{-1}) = \ell^T(c\,\tau^{-1}) + \ell^T(\tau).$$

Ceci, par la proposition 2.33, implique $r(c) = r(c\tau^{-1}) \cdot r(\tau)$, c'est-à-dire, $\delta_n = r(c\tau^{-1}) \cdot \beta$.

Montrons que (iii) implique (i) et que (ii) implique (i). Soit β' un élément de B_n^{+*} tel que la tresse δ_n soit égale à $\beta\,\beta'$. Comme δ_n est un élément simple de B_n^{+*}, on a $\ell^T(\pi(\delta_n)) = |\delta_n|$, ce qui implique la relation $\ell^T(\pi(\beta\,\beta')) = |\beta\,\beta'|$. Donc, par le lemme 2.39 (ii) et (iii), on a

$$|\beta| + |\beta'| \leqslant |\beta| + \ell^T(\pi(\beta')) \quad \text{et} \quad |\beta| + |\beta'| \leqslant \ell^T(\pi(\beta)) + |\beta'|.$$

Ainsi les relations $|\beta| \leqslant \ell^T(\pi(\beta))$ et $|\beta'| \leqslant \ell^T(\pi(\beta'))$ sont vérifiées. Par le lemme 2.39 (i), on a $|\beta| = \ell^T(\pi(\beta))$ et $|\beta'| = \ell^T(\pi(\beta'))$. De la relation $\ell^T(\pi(\beta)\pi(\beta')) = |\beta| + |\beta|$, on obtient

$$\ell^T(\pi(\beta)\pi(\beta')) = \ell^T(\pi(\beta)) + \ell^T(\pi(\beta')),$$

c'est-à-dire, $\pi(\beta) \preccurlyeq^T \pi(\beta)\pi(\beta')$. Le corollaire 2.12 donne $\pi(\beta') \preccurlyeq^T \pi(\beta)\pi(\beta')$. Comme le produit $\pi(\beta)\pi(\beta')$ vaut c, les permutations $\pi(\beta)$ et $\pi(\beta')$ sont dans $\mathfrak{C}_n$. Le (iv) du lemme 2.39 assure alors que β et β' sont des simples de B_n^{+*}. □

Donnons maitenant une caractérisation de l'ensemble des simples de B_n^{+*} muni de la relation de divisibilité à gauche (ou à droite).

Proposition 2.40. (D. Bessis, F. Digne, J. Michel, [BDM02]) *Les deux ensembles ordonnés* $(S(B_n^{+*}), \succcurlyeq)$ *et* $(S(B_n^{+*}), \preccurlyeq)$ *sont des treillis isomorphes à* $(P_n^{nc}, \preccurlyeq^P)$.

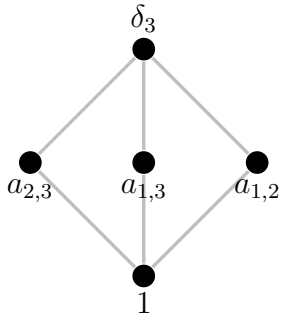
Démonstration. Soient β et β' deux simples de B_n^{+*}. Il existe alors τ et τ' de $\mathfrak{C}_n$ tels qu'on ait $\beta = r(\tau)$ et $\beta' = r(\tau')$. La relation $\beta \preccurlyeq \beta'$ est équivalente à l'existence de β'' dans B_n^{+*} vérifiant $\beta' = \beta\beta''$. En particulier β'' est un diviseur à gauche de β', donc de δ_n, par la proposition 2.36 (car β' est simple). Ainsi, encore grâce à la proposition 2.36, β'' est un simple de B_n^{+*}. La relation $\beta \preccurlyeq \beta'$ est donc équivalente à l'existence de τ'' dans $\mathfrak{C}_n$ vérifiant $r(\tau') = r(\tau)r(\tau'')$.

En utilisant la fonction π on obtient $\pi(r(\tau')) = \pi(r(\tau)r(\tau''))$, puis $\tau' = \tau\tau''$ par la proposition 2.38. La relation $\beta \preccurlyeq \beta'$ est donc équivalente à l'existence de τ'' dans $\mathfrak{C}_n$ vérifiant la relation $r(\tau\tau'') = r(\tau)r(\tau'')$, ce qui par la proposition 2.33 est équivalent à

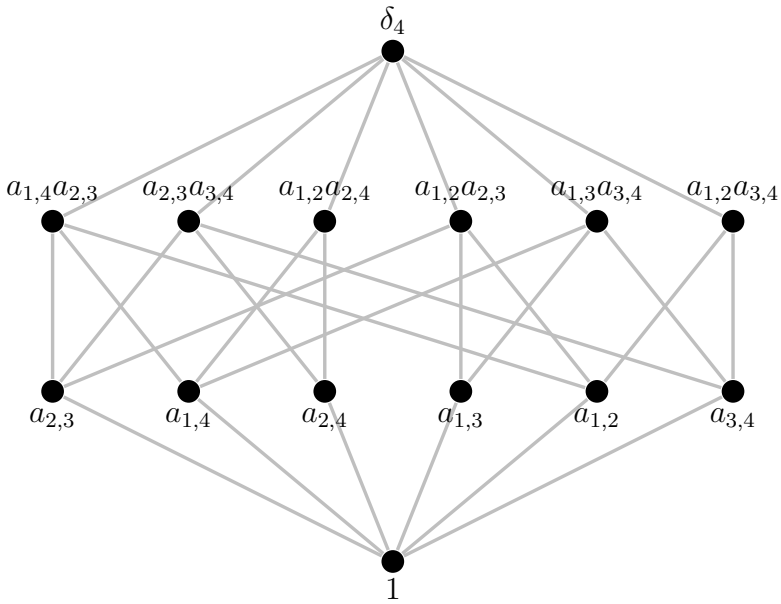
$$\ell^T(\tau\tau'') = \ell^T(\tau) + \ell^T(\tau''),$$

c'est-à-dire, à $\tau \preccurlyeq^T \tau\tau''$. Ainsi la relation $\beta \preccurlyeq \beta'$ est équivalente à $\pi(\beta) \preccurlyeq^T \pi(\beta')$. Un argument symétrique établit l'équivalence entre $\beta \succcurlyeq \beta'$ et $\pi(\beta') \preccurlyeq^T \pi(\beta)$. □

Exemple 2.41. Le diagramme de Hasse de $(S(B_3^{+*}), \succcurlyeq)$ et $(S(B_3^{+*}), \preccurlyeq)$ est



Le diagramme de Hasse de $(S(B_4^{+*}), \succcurlyeq)$ et $(S(B_4^{+*}), \preccurlyeq)$ est



Nous pouvons maintenant montrer que deux éléments quelconques de B_n^{+*} admettent un multiple commun à gauche et un multiple commun à droite.

Proposition 2.42.
– (i) *Soient u et v deux simples de B_n^{+*} alors u et v possèdent un multiple commun à droite et à gauche.*
– (ii) *Soient u et v deux éléments de B_n^{+*} alors u et v possèdent un multiple commun à droite et à gauche.*

Démonstration. (i) Par la proposition 2.36, l'élément δ_n est un multiple à droite et à gauche commun à tous les simples.

(ii) Soient β et β' deux éléments de B_n^{+*}. Posons $\beta = s_1 \cdot ... \cdot s_k$ et $\beta' = s'_1 \cdot ... \cdot s'_{k'}$ où les s_i et les s'_i sont des simples de B_n^{+*}. De telles décompositions existent car β et β' sont, par construction, des produits en les éléments $a_{i,j}$, qui sont des simples (on a $a_{i,j} = r((i,j))$). L'élément $\delta_n^{\max(k,k')}$ est alors un multiple commun à droite et à gauche de β et β' par (i). □

Pour montrer que le monoïde B_n^{+*} satisfait les conditions de Ore (théorème I.2.20), il nous reste à établir qu'il est simplifiable à gauche et à droite, c'est-à-dire que la relation $x\,\beta = x\,\beta'$ implique $\beta = \beta'$ et que la relation $\beta\,x = \beta'\,x$ implique aussi $\beta = \beta'$. C'est l'un des résultats de la prochaine section.

3 Retournement sur B_n^{+*}

Pour montrer que le monoïde B_n^{+*} est simplifiable à gauche et à droite nous utilisons la méthode, dite du *retournement*, introduite par P. Dehornoy en 1992 dans [Deh92], puis généralisée par P. Dehornoy et L. Paris en 1999 dans l'un des articles fondateurs de la théorie dite de Garside [DP99]. Le principal avantage de cette méthode est son aspect à la fois théorique et algorithmique. De plus, ces dernières années, le retournement a été le sujet de nombreuses publications [Deh00b, Deh03, DW06, AD09]. C'est pour ces différentes raisons que le retournement est la base algorithmique de cette thèse.

3.1 Complément à gauche et à droite.

Dans cette section, nous introduisons deux applications de $A_n^+ \times A_n^+$ dans $(A_n^+)^*$, notées f_g^n et f_d^n, qui nous permettrons de décrire le retournement sur le monoïde B_n^{+*}. Redonnons d'abord les définitions dans un contexte général.

Définition 3.1. Soit $\mathcal{S}$ un alphabet fini.
– Un *complément* sur $\mathcal{S}$ est une application f de $\mathcal{S} \times \mathcal{S}$ dans $\mathcal{S}^*$ telle que $f(x,x)$ soit le mot vide pour toute lettre x de $\mathcal{S}$.
– Le *monoïde à gauche associé à un complément* f est alors le monoïde $M_g(\mathcal{S}, f)$ qui admet la présentation

$$\big\langle \mathcal{S} \mid \{f(x,y)x = f(y,x)y\ ;\ x,y \in \mathcal{S}\}\big\rangle^+. \tag{2.24}$$

– Le *monoïde à droite associé à* f est alors le monoïde $M_d(\mathcal{S}, f)$ qui admet la présentation

$$\big\langle \mathcal{S} \mid \{xf(x,y) = yf(y,x)\ ;\ x,y \in \mathcal{S}\}\big\rangle^+. \tag{2.25}$$

Exemple 3.2. La fonction f définie sur $\{a,b\}$ par

$$f(a,b) = b\,a, \quad f(b,a) = a\,b, \quad f(a,a) = f(b,b) = \varepsilon,$$

est un complément sur $\{a,b\}$. Le monoïde $M_d(\{a,b\}, f)$ est alors le monoïde de présentation

$$\big\langle a,b \mid a = a\,, aba = bab\,, bab = aba\,, b = b\big\rangle^+.$$

Les relations $a = a$ et $b = b$ sont inutiles et les deux autres relations sont symétriques l'une de l'autre. On obtient alors

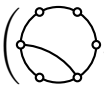
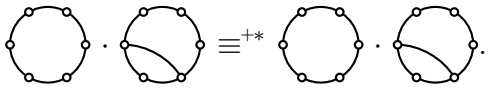
$$M_d(\{a,b\}, f) = \big\langle a,b \mid aba = bab\big\rangle^+,$$

qui est isomorphe au monoïde de tresses positives à 3 brins B_3^+ (voir la présentation (I.1.5)).

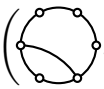
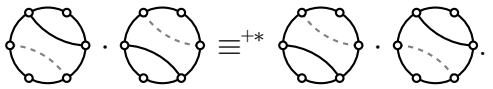
Nous allons maintenant définir un complément f_g^n sur A_n^+ tel que le monoïde B_n^{+*} soit isomorphe à $M_g(A_n^+, f_g^n)$. Pour cela nous construisons la fonction f_g^n à partir de la présentation 2.13 de B_n^{+*}. L'idée est de poser $f_g^n(a_{p,q}, a_{r,s}) = u$ s'il existe un mot v de $(A_n^+)^*$ tel que la relation $a_{p,q}\, u \equiv^{+*} a_{r,s}\, v$ soit satisfaite dans B_n^{+*}.

Afin de simplifier la compréhension, nous définissons dans un premier temps la fonction f_g^n à l'aide des diagrammes de cordes introduits à la section 1.1. Les cordes en pointillés aident à mieux visualiser les relations entre diagrammes.

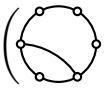
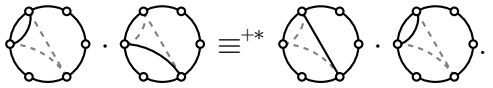
– 1. Pour $a_{p,q} = a_{q,r}$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

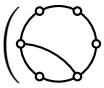
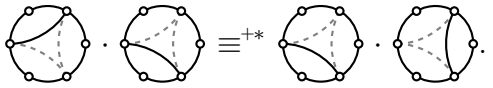
– 2. Pour $[p, q]$ et $[r, s]$ disjoints ou nichés, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

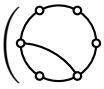
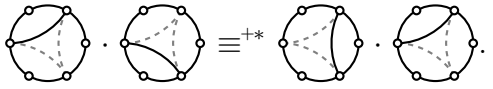
– 3. Pour $p = s$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

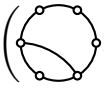
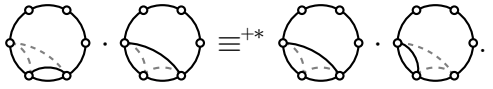
– 4. Pour $q = r$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

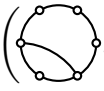
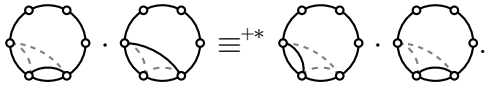
– 5. Pour $p = r$ et $q < s$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

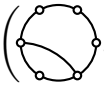
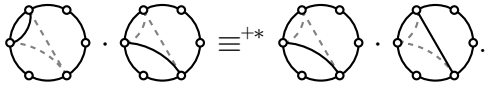
– 6. Pour $p = r$ et $q > s$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

– 7. Pour $p < r$ et $q = s$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

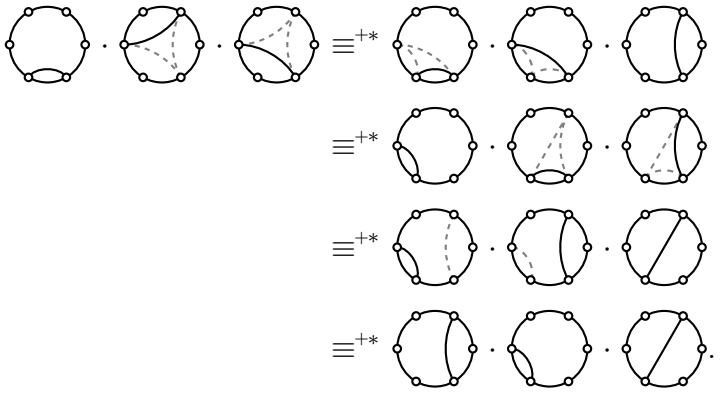
– 8. Pour $p > r$ et $q = s$, on pose

$f_g^n\Big($  $\Big) =$  , car on a  .

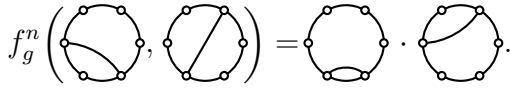
Nous n'avons pas tout à fait terminé. En effet nous n'avons pas défini encore la fonction f_g^n sur le couple $(a_{p,q}, a_{r,s})$ pour $p < r < q < s$ et $r < p < s < q$. Contrairement aux huit cas précédents, on ne peut pas lire la valeur de f_g^n directement sur les relations de la présentation de B_n^{+*}. Pour cela, on utilise la relation suivante valable pour $p < r < q < s$:

$$a_{r,q}\, a_{p,s}\, a_{p,q} \equiv^{+*} a_{r,q}\, a_{p,q}\, a_{q,s} \equiv^{+*} a_{p,r}\, a_{r,q}\, a_{q,s} \equiv^{+*} a_{p,r}\, a_{q,s}\, a_{r,s} \equiv^{+*} a_{q,s}\, a_{p,r}\, a_{r,s},$$

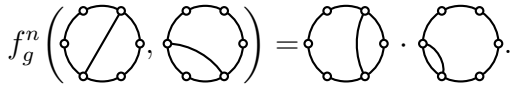
ce qui en termes de diagrammes donne



– 9. Pour $p < r < q < s$, on pose



– 10. Pour $r < p < s < q$, on pose



En résumé, on obtient la définition suivante de f_g^n :

Définition 3.3. On note f_g^n l'application de $A_n^+ \times A_n^+$ dans $(A_n^+)^*$ définie par

$$f_g^n(a_{p,q}, a_{r,s}) = \begin{cases} \varepsilon & \text{pour } a_{p,q} = a_{r,s}, \\ a_{r,s} & \text{pour } [p,q] \text{ et } [r,s] \text{ disjoints ou nichés}, \\ a_{r,s} & \text{pour } p = s, \\ a_{p,s} & \text{pour } q = r \\ a_{r,s} & \text{pour } p = r \text{ et } q < s, \\ a_{s,q} & \text{pour } p = r \text{ et } q > s, \\ a_{r,s} & \text{pour } q = s \text{ et } p < r, \\ a_{r,p} & \text{pour } q = s \text{ et } p > r, \\ a_{r,q}\, a_{p,s} & \text{pour } p < r < q < s, \\ a_{s,q}\, a_{r,p} & \text{pour } r < p < s < q. \end{cases} \tag{2.26}$$

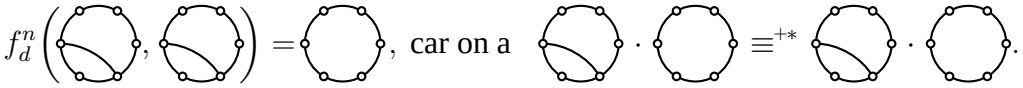
Le complément que nous venons de définir n'est pas le seul issu des relations de B_n^{+*}. En effet pour les cas 9 et 10 le complément est de longueur 2 et les deux lettres qui le composent commutent.

Proposition 3.4. *Les monoïdes B_n^{+*} et $M_g(A_n^+, f_g^n)$ sont égaux.*

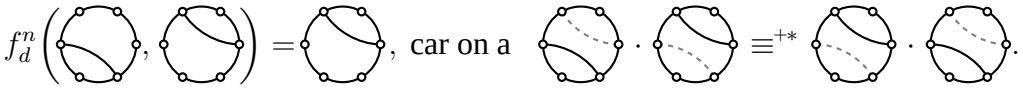
Démonstration. Par construction de f_g^n, toutes les relations de la présentation de B_n^{+*} données en (2.13) sont présentes dans la présentation de $M_g(A_n^+, f_g^n)$. Réciproquement, toujours par construction de f_g^n, toutes les relations de $M_g(A_n^+, f_d^n)$ sont satisfaites dans B_n^{+*}. □

Définissons maintenant un complément f_d^n sur A_n^+ tel que les monoïdes B_n^{+*} et $M_d(A_n^+, f_d^n)$ soient isomorphes. Comme pour f_g^n, nous utilisons d'abord les diagrammes de cordes afin d'alléger les justifications :

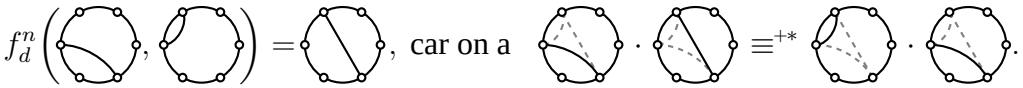
– 1. Pour $a_{p,q} = a_{q,r}$, on pose



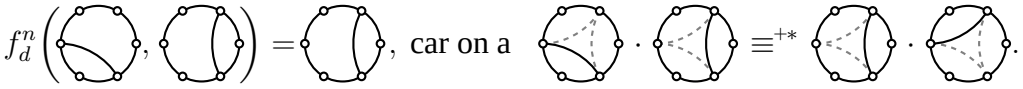
– 2. Pour $[p, q]$ et $[r, s]$ disjoints ou nichés, on pose



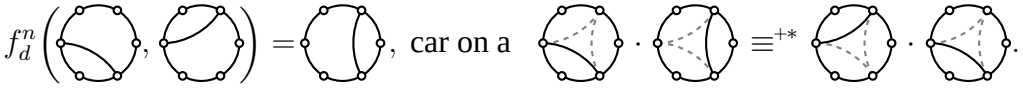
– 3. Pour $p = s$, on pose



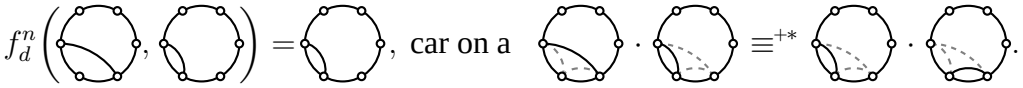
– 4. Pour $q = r$, on pose



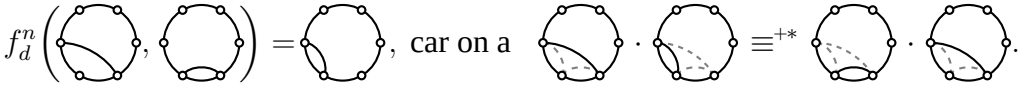
– 5. Pour $p = r$ et $q < s$, on pose



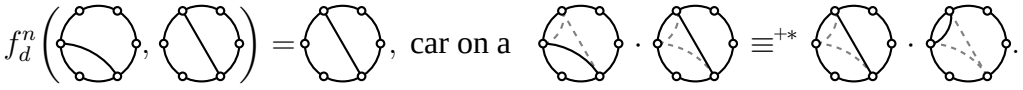
– 6. Pour $p = r$ et $q > s$, on pose



– 7. Pour $p < r$ et $q = s$, on pose



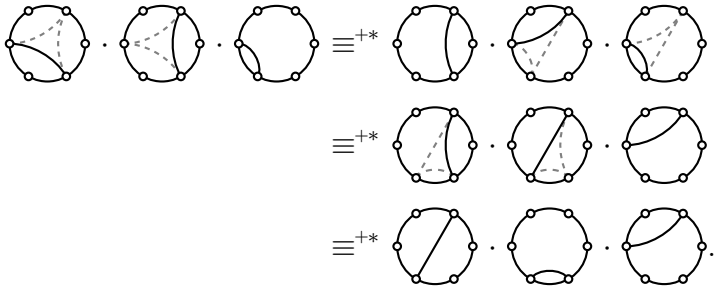
– 8. Pour $p > r$ et $q = s$, on pose



Pour $p < r < q < s$, on a

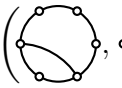
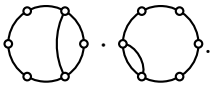
$$a_{p,q}\, a_{q,s}\, a_{p,r} \equiv^{+*} a_{q,s}\, a_{p,s}\, a_{p,r} \equiv^{+*} a_{q,s}\, a_{r,s}\, a_{p,s} \equiv^{+*} a_{r,s}\, a_{r,q}\, a_{p,s},$$

ce qui en termes de diagrammes donne

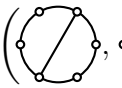
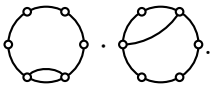


Cette relation permet de terminer la définition de f_d^n :

– 9. Pour $p < r < q < s$, on pose

$f_d^n\Big($  $\Big) =$  .

– 10. Pour $r < p < s < q$, on pose

$f_d^n\Big($  $\Big) =$  .

En résumé, on obtient la définition suivante de f_d^n :

Définition 3.5. On note f_d^n l'application de $A_n^+ \times A_n^+$ dans $(A_n^+)^*$ définie par

$$f_d^n(a_{p,q}, a_{r,s}) = \begin{cases} \varepsilon & \text{pour } a_{p,q} = a_{r,s}, \\ a_{r,s} & \text{pour } [p,q] \text{ et } [r,s] \text{ disjoints ou nichés}, \\ a_{r,q} & \text{pour } p = s, \\ a_{r,s} & \text{pour } q = r \\ a_{q,s} & \text{pour } p = r \text{ et } q < s, \\ a_{r,s} & \text{pour } p = r \text{ et } q > s, \\ a_{p,r} & \text{pour } q = s \text{ et } p < r, \\ a_{r,s} & \text{pour } q = s \text{ et } p > r, \\ a_{q,s}\, a_{p,r} & \text{pour } p < r < q < s, \\ a_{p,s}\, a_{r,q} & \text{pour } r < p < s < q. \end{cases} \tag{2.27}$$

Comme pour le complément f_d^n, on démontre le résultat suivant :

Proposition 3.6. *Les monoïdes B_n^{+*} et $M_d(A_n, f_d^n)$ sont identiques.*

Nous venons de démontrer que le monoïde B_n^{+*} est un monoïde à gauche associé à un complément et un monoïde à droite associé à un complément. Ainsi le monoïde B_n^{+*} est un monoïde *complémenté*.

Cette propriété nous permet alors d'effectuer des opérations liées à la divisibilité de manière efficace dans B_n^{+*} à l'aide de l'algorithme de retournement, que l'on n'a pas encore défini : c'est le but de la prochaine section. Cette propriété est aussi valable pour B_n^+ (voir [Deh97b]), mais nous ne la détaillons pas dans cette thèse.

3.2 Retournement à gauche et à droite

À l'aide des compléments f_g^n et f_d^n définis sur A_n^+, nous introduisons des opérations combinatoires appelées respectivement *retournement à gauche* et *retournement à droite* sur A_n^*.

Définition 3.7. Pour w, w' des A_n-mots, on dit que w est *retournable à gauche en w' en une étape*, noté $w \curvearrowright_g^{(1)} w'$, si l'on peut obtenir w' depuis w en remplaçant un facteur $x\, y^{-1}$ de w, avec x et y des A_n^+-lettres, par $f_g^n(x,y)^{-1}\, f_g^n(y,x)$.

De manière symétrique, on obtient la définition suivante pour le retournement à droite :

Définition 3.8. Pour w, w' des A_n-mots, on dit que w est *retournable à droite en w' en une étape*, noté $w \curvearrowright_d^{(1)} w'$, si l'on peut obtenir w' depuis w en remplaçant un facteur $x^{-1}\,y$ de w, avec x et y des A_n^+-lettres, par $f_d^n(x,y)\,f_d^n(y,x)^{-1}$.

Soient w et w' deux A_n-mots. On dit que w est *retournable à gauche en w' en k étapes* (*resp. retournable à droite en w' en k étapes*), noté $w \curvearrowright_g^{(k)} w'$ (*resp.* $w \curvearrowright_d^{(k)} w'$), s'il existe une suite de A_n-mots $w_1, \dots, w_{k+1}$ avec $w_1 = w$ et $w_{k+1} = w'$ vérifiant $w_i \curvearrowright_g^{(1)} w'_{i+1}$ (*resp.* $w_i \curvearrowright_d^{(1)} w'_i$) pour tout i dans $\{1, \dots, k\}$. La suite $w_1, \dots, w_{k+1}$ est alors appelée *suite de retournements à gauche* (*resp. suite de retournements à droite*). On dit que w est *retournable à gauche en w'* (*resp. retournable à droite en w'*) et on note $w \curvearrowright_g w'$ (*resp.* $w \curvearrowright_d w'$), s'il est retournable à gauche (*resp.* à droite) en w' en k étapes pour un certain entier k.

On définit le retournement à gauche par l'algorithme suivant :

Algorithme 1 (`RetGauche`)**.**
Entrée : Un couple (n, w) où n est un entier et w un A_n^+-mot
1. $w \to w'$
2. `Tant que` w' a un facteur de la forme $x\,y^{-1}$ `faire`
3. Remplacer $x\,y^{-1}$ par $f_g^n(x,y)^{-1}\,f_g^n(y,x)$
4. `Renvoyer` w'

Sortie : Un A_n-mot w' non retournable à gauche en un autre mot vérifiant $w \curvearrowright_g w'$

Symétriquement, on définit le retournement à droite par l'algorithme suivant :

Algorithme 2 (`RetDroite`)**.**
Entrée : Un couple (n, w) où n est un entier et w un A_n^+-mot
1. $w \to w'$
2. `Tant que` w' a un facteur de la forme $x^{-1}\,y$ `faire`
3. Remplacer $x^{-1}\,y$ par $f_d^n(x,y)\,f_d^n(y,x)^{-1}$
4. `Renvoyer` w'

Sortie : Un A_n-mot w' non retournable à droite en un autre mot vérifiant $w \curvearrowright_d w'$

Un A_n-mot donné w peut contenir plusieurs facteurs de la forme $x\,y^{-1}$. Ainsi le mot w' donné par l'algorithme 1 dépend, *a priori*, du choix d'un facteur de la forme $x\,y^{-1}$ dans w'. La proposition suivante montre que le choix du facteur à retourner n'a en fait pas d'importance.

Proposition 3.9. (P. Dehornoy, [Deh00a]) *Pour w, w' et w'' des A_n-mots vérifiant $w \curvearrowright_g^{(k)} w'$, $w \curvearrowright_g^{(k')} w''$, il existe w''' satisfaisant $w' \curvearrowright_g^{(k''-k)} w'''$ et $w'' \curvearrowright_g^{(k''-k')} w'''$ avec $k'' \leqslant k + k'$. Ceci reste vrai si on remplace $\curvearrowright_g$ par $\curvearrowright_d$.*

Démonstration. Si k vaut 0, alors on a $w = w'$ et donc $w' \curvearrowright_g^{(k')} w''$; dans ce cas il suffit de prendre $w''' = w''$ et $k'' = k'$. Un argument similaire traite le cas $k' = 0$. Supposons $k = 1$ et $k' = 1$. Le mot w' est alors obtenu en retournant en une étape un facteur $x\,y^{-1}$ de w. De même w'' est obtenu en retournant en une étape un facteur $x'\,y'^{-1}$ de w. Soient u, v, u' et v' des A_n-mots vérifiant $w = u\,x\,y^{-1}\,v$ et $w' = u'\,x'\,y'^{-1}\,v'$. Si les mots u et u' sont égaux, alors w' et w'' le sont aussi. On pose alors $w''' = w'$ et $k'' = 1$. Supposons $|u| > |u'|$ (le cas $|u'| > |u|$ est similaire). Comme le préfixe u de w n'est pas suivi par la lettre y'^{-1}, il existe un mot u'' vérifiant $u = u'\,x'\,y'^{-1}\,u''$. On a donc

$$w = u'\,x'\,y'^{-1}\,u''\,x\,y^{-1}\,v.$$

On note alors w''' le mot obtenu à partir de w en retournant $x\,y^{-1}$ et $x'\,y'^{-1}$. Comme les facteurs $x\,y^{-1}$ et $x'\,y'^{-1}$ sont disjoints dans w, l'ordre de retournement n'a pas d'importance. Ainsi les mots w' et w'' sont retournables en une étape en w''' ; dans ce cas k vaut 2.

Terminons la démonstration par induction sur $k+k'$. Supposons $k+k' \geqslant 2$ avec $k \geqslant 2$ ou $k' \geqslant 2$ (les autres valeurs de k ont déjà été traitées). Sans perte de généralité on peut supposer $k \geqslant 2$, un argument symétrique traitant le cas $k' \geqslant 2$. Il existe alors un mot u vérifiant la relation $w \curvearrowright_g^{(k-1)} u$ et $u \curvearrowright_g^{(1)} w'$. Par induction, comme on a $w \curvearrowright_g^{(k-1)} u$ et $w \curvearrowright_g^{(k)} w'$, il existe un mot v et un entier ℓ vérifiant $u \curvearrowright_g^{(\ell-k+1)} v$ et $w'' \curvearrowright_g^{(\ell-k')} v$ avec $\ell \leqslant k + k' - 1$. En utilisant la majoration sur ℓ et la relation $k \geqslant 2$ on obtient $(\ell - k + 1) + 1 < k + k'$. Par induction, il existe un A_n-mot w''' et un entier ℓ' vérifiant $w' \curvearrowright_g^{(\ell'-1)} w'''$ et $v \curvearrowright_g^{(\ell'-\ell+k-1)} w'''$ avec $\ell' \leqslant (\ell - k + 2)$, donc $\ell' \leqslant k' + 1$. Ainsi w' se retourne à gauche en au plus k' étapes en w''' et w'' se retourne à gauche en au plus k étapes en w''', ce qui termine la démonstration pour $\curvearrowright_g$. Le cas $\curvearrowright_d$ se traite de la même manière. □

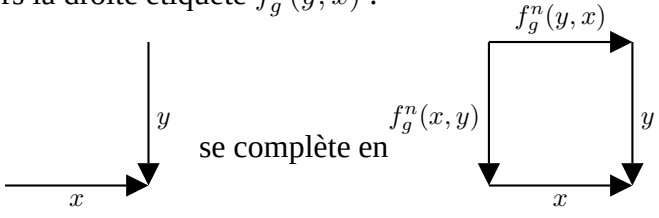
La proposition 3.9 assure que si l'algorithme 1 appliqué à un mot w se termine, alors le mot retourné ne dépend pas de la suite de retournements choisie. Par contre, à ce stade on ne sait pas encore si l'algorithme se termine. De même pour l'algorithme 2.

Corollaire 3.10. *Pour w et w' deux A_n-mots, vérifiant $w \curvearrowright_g w'$ et tels que w' ne contienne pas de facteur de la forme $x\,y^{-1}$, il existe un unique k tel qu'on ait $w \curvearrowright_g^{(k)} w'$. Le résultat reste vrai, si on remplace $\curvearrowright_d$ par $\curvearrowright_g$.*

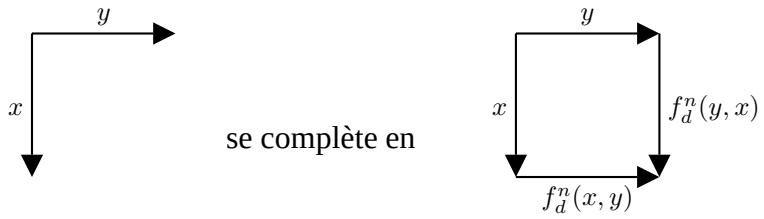
Démonstration. Soient k et k' deux entiers vérifiant $w \curvearrowright_g^{(k)} w'$ et $w \curvearrowright_g^{(k')} w'$. Par la proposition 3.9 il existe un mot w'' et un entier k'' vérifiant $w' \curvearrowright_g^{(k''-k)} w''$ et $w' \curvearrowright_g^{(k''-k')} w''$. Comme w' n'est plus retournable, on a $k'' - k = 0$, $k'' - k' = 0$ et $w'' = w'$. Ceci implique $k = k' = k''$. Un argument similaire traite le cas de $\curvearrowright_d$. □

Il est peu commode de décrire le retournement à gauche ou à droite à partir de suite de retournements. Nous introduisons une méthode plus adaptée à cette fin : le *diagramme de retournements*. Supposons que $w_1, \ldots, w_{k+1}$ soit une suite de retournements à gauche (*resp.* à droite), c'est-à-dire, une suite de A_n-mots vérifiant $w_i \curvearrowright_g^{(1)} w_{i+1}$ (*resp.* $w_i \curvearrowright_d^{(1)} w_{i+1}$) pour tout i. À cette suite nous associons un graphe orienté, construit par induction sur k. On se donne un point de départ. Au mot w_0 nous associons une suite d'arêtes étiquetées comme suit. On lit le mot w_0 de la gauche vers la droite. Si la lettre lue est x (*resp.* x^{-1}) on accroche au point de départ ou à l'extrémité libre de l'arête précédente une arête horizontale étiquetée x orientée vers la droite (*resp.* une arête verticale étiquetée x orientée vers le bas).

Dans le cas du retournement à gauche, le mot w_{i+1} est obtenu à partir de w_i en remplaçant un facteur $x\,y^{-1}$ par $f_g^n(x,y)^{-1}\, f_g^n(y,x)$. On complète alors le chemin associé au mot $x\,y^{-1}$ par un chemin d'arêtes verticales orientées vers le bas étiqueté $f_g^n(x,y)$ puis par un chemin d'arêtes horizontales orientées vers la droite étiqueté $f_g^n(y,x)$:



Dans le cas du retournement à droite, le mot w_{i+1} est obtenu à partir de w_i en remplaçant un facteur $x^{-1}\,y$ par $f_d^n(x,y)\, f_d^n(y,x)^{-1}$. On complète alors le chemin associé au mot $x^{-1}\,y$ par un chemin d'arêtes horizontales orientées vers la droite étiqueté $f_d^n(x,y)$ puis un chemin d'arêtes verticales orientées vers le bas étiqueté $f_d^n(y,x)$:



Dans les deux cas, si on obtient w_{i+1} à partir de w en remplaçant un facteur $x\,x^{-1}$ (ou bien $x^{-1}\,x$ dans le cas du retournement à gauche), on crée des arêtes verticales et horizontales étiquetées ε. Ces arêtes sont alors traitées de la même manière que les autres, voir figure 2.8.

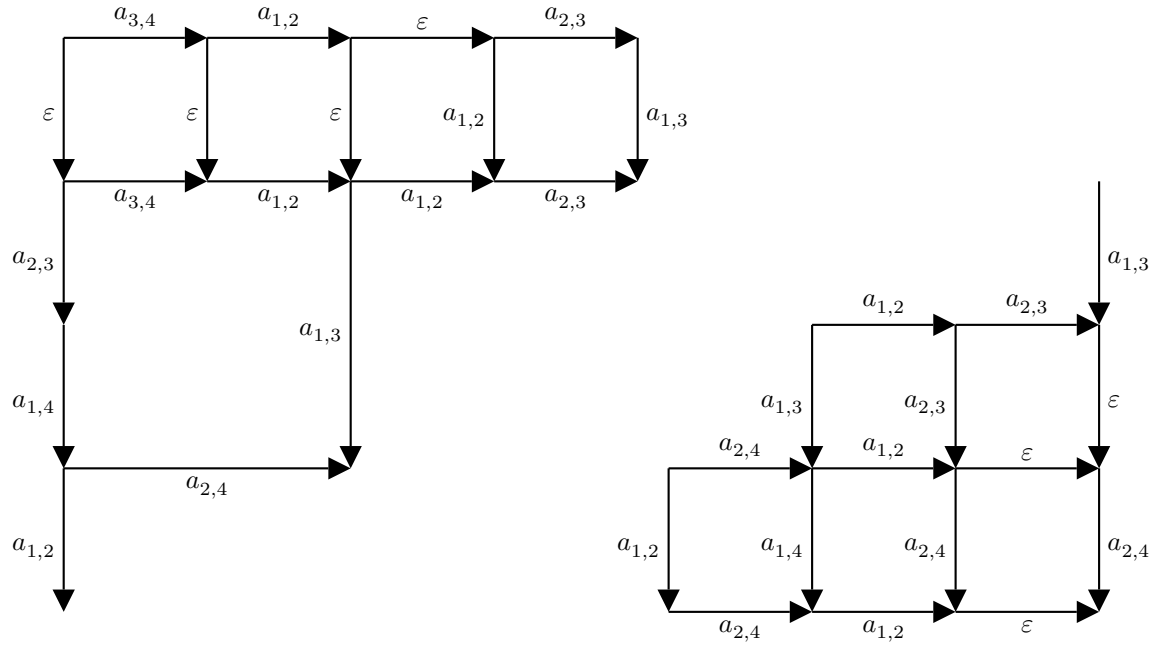


FIG. 2.8 : Retournement à gauche et à droite du A_n-mot $w = a_{1,2}^{-1}\,a_{2,4}\,a_{1,3}^{-1}\,a_{1,2}\,a_{2,3}\,a_{1,3}^{-1}$. On obtient $w{\curvearrowright_g}a_{1,2}^{-1}\,a_{1,4}^{-1}\,a_{2,3}^{-1}\,a_{3,4}\,a_{1,2}\,a_{2,3}$ et $w{\curvearrowright_d}a_{2,4}\,a_{1,2}\,a_{2,4}^{-1}\,a_{1,3}^{-1}$.

Supposons qu'un mot w se retourne à gauche en w'. Que peut-on alors dire sur le retournement à gauche de w^{-1} ? Le résultat qui suit nous assure que les retournements de w et w^{-1} sont liés :

Proposition 3.11. *Pour des A_n-mots w et w', la relation $w{\curvearrowright_g}w'$ implique $w^{-1}{\curvearrowright_g}w'^{-1}$. Le résultat reste vrai en remplaçant $\curvearrowright_g$ par $\curvearrowright_d$.*

Démonstration. Supposons $w{\curvearrowright_g}w'$. Alors, par définition de $\curvearrowright_g$, il existe une suite

$$(w_1, \dots, w_{k+1})$$

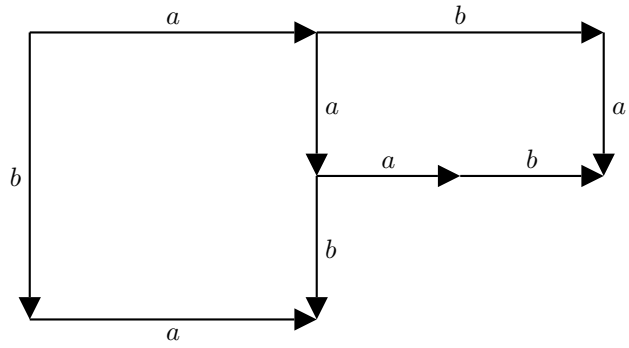
vérifiant $w_1 = w$, $w_{k+1} = w'$ et $w_i{\curvearrowright_g^{(1)}}w_{i+1}$ pour tout i. Montrons que la suite $(w_1^{-1}, \dots, w_{k+1}^{-1})$ témoigne de $w^{-1}{\curvearrowright_g}w'^{-1}$. Clairement, les égalités $w_1^{-1} = w^{-1}$ et $w_{k+1}^{-1} = w'^{-1}$ sont vérifiées. Soit i dans $\{1, \dots, k\}$. De $w_i{\curvearrowright_g^{(1)}}w_{i+1}$, on déduit l'existence de deux lettres x et y et de deux mots u et v vérifiant $w_i = u\,x\,y^{-1}\,v$ et $w_{i+1} = u\,f_d^n(x,y)^{-1}\,f_d^n(y,x)\,v$. Comme le mot w_i^{-1} est égal à $v^{-1}\,y^{-1}\,x\,u^{-1}$, il se retourne en $v^{-1}\,f_d^n(y,x)^{-1}\,f_d^n(x,y)\,u^{-1}$. Le dernier mot étant égal à w_{i+1}^{-1}, on a bien $w_i^{-1}{\curvearrowright_g^{(1)}}w_{i+1}^{-1}$. La suite $(w_1^{-1}, \dots, w_{k+1}^{-1})$ est donc une suite de retournements à gauche. Ceci termine le cas de $\curvearrowright_g$. Pour $\curvearrowright_d$, on utilise un argument similaire. □

À la section 3.3, nous allons montrer que les algorithmes 1 et 2 terminent quel que soit le mot d'entrée w. Terminons cette sous-section en insistant sur le fait que ceci n'a *a priori* rien d'évident. Introduisons d'abord des notations. Pour tout alphabet $\mathcal{S}$, on peut définir le retournement à gauche (ou à droite) sur l'alphabet $\mathcal{S}$ si on l'a au préalable muni d'un complément. L'exemple suivant montre qu'il n'est pas immédiat que le retournement défini sur un alphabet quelconque se termine :

Exemple 3.12. Posons $\mathcal{S} = \{a, b\}$ et définissons le complément f par

$$f(a,a) = f(b,b) = \varepsilon, \quad f(a,b) = a\,b \quad \text{et} \quad f(b,a) = a.$$

Alors le retournement à droite associé au complément f ne se termine pas forcément. En effet le mot $b^{-1}\,a\,b$ se retourne à droite en $a\,b^{-1}\,a\,b\,a^{-1}$ qui admet $b^{-1}\,a\,b$ comme facteur. Ainsi on peut retourner à droite successivement les mots obtenus indéfiniment :



3.3 Retournement et équivalence

Dans cette section, nous décrivons les liens existant entre les retournements (à gauche ou à droite) et la relation d'équivalence $\equiv^{+*}$ sur les A_n^+-mots. C'est une première étape vers la description de méthode permettant d'effectuer des calculs dans le monoïde B_n^{+*} : pgcd, ppcm, etc.

On définit les opérations suivantes sur les A_n^+-mots :

Définition 3.13. Soit w un A_n^+-mot, on note
– u/v l'unique mot v' vérifiant $u\,v^{-1} \curvearrowright_g u'^{-1}v'$, si un tel mot existe,
– $u\backslash v$ l'unique mot u' vérifiant $u^{-1}\,v \curvearrowright_d u'v'^{-1}$, si un tel mot existe.

Par la proposition 3.11, la relation $u\,v^{-1} \curvearrowright_g u'^{-1}v'$ implique $v\,u^{-1} \curvearrowright_g v'^{-1}u'$. Avec les notations de la définition 3.13, on a alors $v' = u/v$ et $u' = v/u$. Ainsi le mot u/v existe si et seulement si v/u existe, et dans ce cas, on a $u\,v^{-1} \curvearrowright_g (v/u)^{-1}(u/v)$. De même, le mot $u\backslash v$ existe si et seulement si $v\backslash u$ existe, et dans ce cas, on a $u^{-1}\,v \curvearrowright_d (u\backslash v)(v\backslash u)^{-1}$. Ceci est illustré, en termes de diagrammes, à la figure 2.9

FIG. 2.9 : Interprétation des mots u/v, v/u, u/v et v/u à l'aide de diagramme de retournement à gauche et à droite.

Proposition 3.14. (P. Dehornoy, [Deh00a]) *Soient u, v des A_n^+-mots*

– (i) *Supposons que u/v existe, alors on a $(u/v)\, v \equiv^{+*} (v/u)\, u$.*

– (ii) *Supposons que $u\backslash v$ existe, alors on a $u\, (u\backslash v) \equiv^{+*} v\, (v\backslash u)$.*

Démonstration. Montrons le point (i). Soient u et v deux mots tels que u/v existe. Il existe alors un entier k et un mot u' tels qu'on ait $u\, v^{-1} \curvearrowright_g^{(k)} (v/u)^{-1}(u/v)$. On utilise une induction sur k. Si k est nul alors on a soit $u = \varepsilon$, soit $v = \varepsilon$. Supposons $u = \varepsilon$. On a alors $u\, v^{-1} \curvearrowright_g v^{-1}\varepsilon$. Ceci implique $u/v = \varepsilon$ et $v/u = v$ et donc $(u/v)\, v \equiv^{+*} (v/u)\, u$. Le cas $v = \varepsilon$ se traite de la même manière.

Supposons maintenant $k \geqslant 1$. Alors u et v sont non vides. Posons $u = u'\, x$ et $v = v'\, y$, où x et y sont des A_n^+-lettres. Le mot uv^{-1} est alors égal à $u'xy^{-1}v'^{-1}$, qui est retournable à gauche en le mot $uv^{-1} \curvearrowright_g^{(1)} u' f_g^n(x,y)^{-1} f_g^n(y,x) v'^{-1}$. Par la proposition 3.4, la relation

$$f_g^n(x,y)x \equiv^{+*} f_g^n(y,x)y$$

est satisfaite. Par ailleurs, il existe un entier k' et deux mots u'' et w vérifiant

$$u' f_g^n(y,x)^{-1} \curvearrowright_g^{(k')} u''^{-1} w.$$

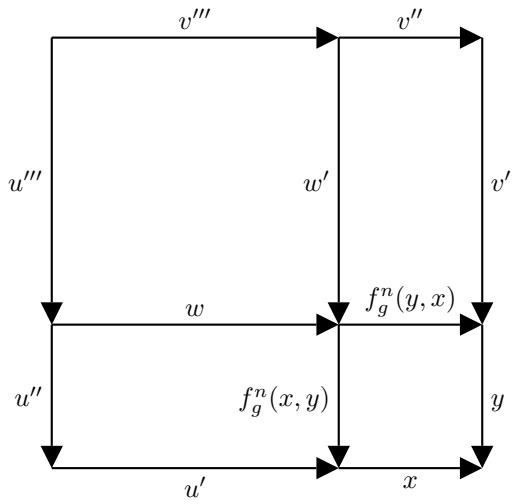
Par le corollaire 3.10, on a $1 + k' \leqslant k$, ce qui donne $k' < k$. L'hypothèse d'induction garantit alors $u''\, u' \equiv^{+*} w\, f_g^n(x,y)$. Symétriquement, il existe un entier k'' et deux mots v'' et w' vérifiant

$$f_g^n(y,x) v'^{-1} \curvearrowright_g^{(k'')} w'^{-1} v''.$$

Encore par hypothèse d'induction, on a $w'\, f_g^n(y,x) \equiv^{+*} v''\, v'$. A ce stade, on a montré :

$$uv^{-1} \curvearrowright_g^{(1)} u' f_g^n(x,y)^{-1} f_g^n(y,x) v'^{-1} \curvearrowright_g^{(k'+k'')} u''^{-1} w w'^{-1} v'',$$
$$f_g^n(x,y)x \equiv^{+*} f_g^n(y,x)y, \quad u''\, u' \equiv^{+*} w\, f_g^n(x,y), \quad w'\, f_g^n(y,x) \equiv^{+*} v''\, v'.$$

D'autre part, il existe deux mots u''', v''' et un entier ℓ vérifiant $ww'^{-1} \curvearrowright_g^{(\ell)} u'''^{-1} v'''$. Le corollaire 3.10 implique l'égalité $1 + k' + k'' + \ell = k$. En particulier, on a $\ell < k$. L'hypothèse d'induction donne alors la relation $u'''w \equiv^{+*} v'''w'$. On a résumé dans le diagramme qui suit les différentes étapes.



Comme on a $uv^{-1} \curvearrowright_g u''^{-1}u'''^{-1}v'''v''$, il nous reste à établir la relation

$$u'''u''u \equiv^{+*} v'''v''v,$$

c'est-à-dire, $u'''u''u'x \equiv^{+*} v'''v''v'y$. En utilisant les différentes équivalences établies, on a

$$u'''u''u'x \equiv^{+*} u'''wf_g^n(x,y)x \equiv^{+*} u'''wf_g^n(y,x)y \equiv^{+*} v'''w'f_g^n(y,x)y \equiv v'''v''v'y.$$

Le cas de $\curvearrowright_d$ se traite de la même manière. □

Une conséquence directe de la proposition 3.14 est que si la relation $uv^{-1} \curvearrowright_g \varepsilon$ est satisfaite alors u et v sont équivalents. De même $u^{-1}v \curvearrowright_d \varepsilon$ implique $u \equiv^{+*} v$. La réciproque est-elle vraie ? Pour pouvoir répondre à cette question nous introduisons deux conditions :

Définition 3.15. Soit (u, v, w) un triplet de A_n-mots.
– On dit que (u, v, w) satisfait la *condition du cube à gauche* si on a

$$((u/v)/(u/w))/((v/u)/(v/w)) = \varepsilon.$$

– On dit que (u, v, w) satisfait la *condition du cube à droite* si on a

$$((u\backslash v)\backslash(u\backslash w))\backslash((v\backslash u)\backslash(v\backslash w)) = \varepsilon.$$

Le résultat qui suit assure que la relation $u \equiv^{+*} v$ implique $uv^{-1} \curvearrowright_g \varepsilon$ si et seulement si la condition du cube à gauche est satisfaite pour tout triplet de A_n^+-mots. Nous n'en donnons pas de démonstration et renvoyons le lecteur a [DP99].

Proposition 3.16. (P. Dehornoy, L. Paris, [DP99]) *Il y a équivalence entre :*
– (i) $u \equiv^{+*} v$ *implique* $uv^{-1} \curvearrowright_g \varepsilon$,
– (ii) $\equiv^{+*}$ *est compatible avec* $/$, *c'est-à-dire,* $u' \equiv^{+*} u$ *et* $v' \equiv^{+*} v$ *implique* $u/v \equiv^{+*} u'/v'$.
– (iii) *tout triplet de* A_n*-mots satisfait la condition du cube à gauche.*

Bien sûr, il existe une version symétrique des équivalences de la proposition 3.16 dans le contexte du retournement à droite.

Pour pouvoir appliquer la proposition 3.16, il faut être capable d'établir la condition du cube à droite ou à gauche pour tout triplet de A_n^+-mots, ce qui nécessite *a priori* une infinité de tests. Heureusement, le résultat suivant est prouvé dans [DP99] et réduit les tests à un nombre fini.

Proposition 3.17. *Il y a équivalence entre :*
– (i) *La condition du cube à gauche (*resp. *à droite) est satisfaite pour tout triplet de A_n^+-mots.*
– (ii) *La condition du cube à gauche (*resp. *à droite) est satisfaite pour tout triplet de A_n^+-lettres.*

Nous ne donnons pas la démonstration de ce résultat qui est assez technique. On peut cependant signaler qu'il repose sur le fait que les relations du monoïde de tresses dual préservent la longueur des mots.

Proposition 3.18. *Soit (x, y, z) un triplet de A_n-lettres, alors (x, y, z) satisfait la condition du cube à gauche et à droite.*

On peut trouver une démonstration de ce résultat dans [BKL98] pour la version du monoïde de tresse dual donnée dans le même article, qui, rappelons-le, est légèrement différente de la notre.

Une conséquence de la proposition 3.16 est que le monoïde B_n^{+*} est simplifiable :

Proposition 3.19. *Le monoïde B_n^{+*} est simplifiable à droite et à gauche.*

Démonstration. Soient β, β' et γ des éléments de B_n^{+*} vérifiant $\beta\gamma = \beta'\gamma$. Soient u, u' et v des représentants respectifs de β, β' et γ. Par construction, on a $uv \equiv^{+*} u'v$. La proposition 3.16 implique alors la relation $(uv)(u'v)^{-1} \curvearrowright_g \varepsilon$. Comme $(uv)(u'v)^{-1} \curvearrowright_g \varepsilon$ implique $uu'^{-1} \curvearrowright_g \varepsilon$, la proposition 3.14 assure $u \equiv^{+*} u'$. On en déduit que B_n^{+*} est simplifiable à droite.

Un argument symétrique montre que le monoïde B_n^{+*} est simplifiable à gauche. □

Ainsi grâce au théorème I.2.20 de Ore et aux propositions 2.42 et 3.19, on obtient :

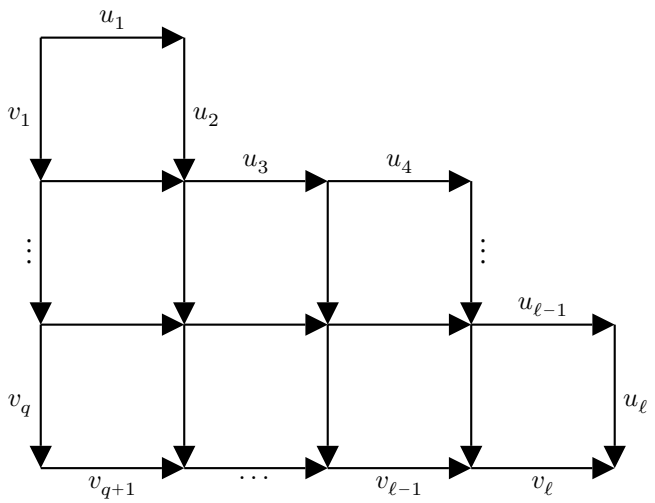
Corollaire 3.20. *Le monoïde B_n^{+*} admet B_n comme groupe de fractions.*

En particulier B_n^{+*} se plonge dans B_n et les relations $\equiv$ et $\equiv^{+*}$ coïncident sur B_n^{+*}. On peut donc utiliser le symbole $\equiv$ à la place du symbole $\equiv^{+*}$.

Nous savons maintenant que le retournement permet de détecter les équivalences de A_n^+-mots. Cependant, nous ne savons toujours pas s'il se termine en général. La proposition suivante nous donne un critère afin de montrer que les algorithmes 1 et 2 se terminent.

Proposition 3.21. (P. Dehornoy, L. Paris, [DP99])
– (i) *Supposons qu'il existe un ensemble X de A_n^+-mots contenant les A_n^+-lettres (vues comme mots de longueur 1) tel que u/v existe et appartienne à X pour tout u, v de X. Alors u/v existe pour tous A_n^+-mots u et v.*
– (ii) *Supposons de plus qu'il existe deux entiers L et N tels que tout mot de X ait une longueur inférieure ou égale à L, et que le nombre d'étapes de retournement à gauche nécessaire pour retourner uv^{-1} avec u et v dans X soit inférieur à N. Alors le retournement à gauche d'un A_n-mot w avec p lettres positives et q lettres négatives se termine en au plus $N \cdot pq$ étapes et renvoie un mot de longueur au plus $L \cdot (p + q)$.*
– (iii) *Les points (i) et (ii) restent valables si l'on remplace « / » par « \ » et « retournement à gauche » par « retournement à droite ».*

Démonstration. Soit w un A_n-mot de longueur ℓ. Comme les A_n^+-lettres appartiennent à X, on peut exprimer w comme un produit $u_1^{e_1} \dots u_\ell^{e_\ell}$ avec u_i dans X et $e_i = \pm 1$ pour tout i. Soit q le nombre de i vérifiant $e_i = -1$. Un simple argument inductif (illustré sur la figure ci-dessous) montre que w est retournable à gauche en $v_1^{-1} \dots v_q^{-1}\, v_{q+1} \dots v_\ell$ où les v_i sont des éléments de X.



Si l'on pose $p = \ell - q$, on constate que le retournement de w nécessite au plus pq retournements à gauche de mots de la forme xy^{-1} avec x, y dans X. Ceci donne le résultat sur le nombre d'étapes de retournement. Le mot retourné est composé de $|w|$ mots de X, sa longueur est donc bornée par $(p+q)\cdot L$.

Un argument symétrique établit le cas du retournement à droite. □

Nous allons maintenant montrer que l'ensemble des mots représentant les simples de B_n^{+*} est stable par $/$ et $\backslash$. Pour cela nous rappelons d'abord ce qu'est un ppcm à droite et un ppcm à gauche.

Définition 3.22. Soient β et β' deux éléments de B_n^{+*}.
– Le *ppcm à droite* de β et β' est le plus petit multiple à droite commun à β et β' pour $\preccurlyeq$.
– Le *ppcm à gauche* de β et β' est le plus petit multiple à gauche commun à β et β' pour $\succcurlyeq$.

Notation 3.23. Pour w' un A_n-mot (*resp.* un B_n^+-mot), on note $\overline{w}$ la tresse de B_n représentée par w.

Le résultat suivant permet d'obtenir le ppcm de deux éléments dès lors qu'on leur connaît un multiple commun.

Proposition 3.24. (P. Dehornoy, L. Paris, [DP99]) *Soient u et v deux A_n^+-mots tels que les tresses $\overline{u}$ et $\overline{v}$ ont un multiple à droite (*resp. *à gauche) commun. Alors le retournement à gauche (*resp. *à droite) de uv^{-1} (*resp. *$u^{-1}v$) se termine. De plus les mots $(v/u)u$ et $(u/v)v$ (*resp. *$u(u\backslash v)$ et $v(v\backslash u)$) représentent le ppcm à gauche (*resp. *à droite) de $\overline{u}$ et $\overline{v}$.*

Démonstration. La proposition 3.16 implique que les mots $(v/u)u$ et $(u/v)v$ sont équivalents et donc qu'ils représentent un multiple à gauche de u et v, que l'on note m.

Supposons que m' soit un autre multiple à gauche de u et v. Il existe alors des A_n^+-mots u' et v' vérifiant $\overline{u'\,u} = m'$ et $\overline{v'\,v} = m'$. En particulier, on a $u'u \equiv v'v$. La proposition 3.16 assure alors que le retournement à gauche de $u'u(v'v)^{-1}$ se termine par le mot vide ε. Afin de montrer que m' est un multiple à gauche de m, nous détaillons le retournement à gauche de $u'u(v'v)^{-1}$. Notons u'', v'', w, w', w'', w''' les mots satisfaisant :

$$u'u(v'v)^{-1} = u'uv^{-1}v'^{-1} \curvearrowright_g u'(v/u)^{-1}(u/v)v'^{-1} \curvearrowright_g u''^{-1}ww'^{-1}v'' \curvearrowright_g u''^{-1}w''^{-1}w'''v''.$$

Comme le retournement à gauche de $u'u(v'v)^{-1}$ se termine par le mot vide, les mots u'', v'', w'' et w''' sont vides. En particulier on a $ww'^{-1} \curvearrowright_g \varepsilon$, ce qui par la proposition 3.14 implique que w

est équivalent à w'. Les mots $u'(v/u)^{-1}$ et $v'(v/u)^{-1}$ se retournent donc à gauche en le même mot w. Par la proposition 3.14, on obtient les relations $u' \equiv w(v/u)$ et $v' \equiv w(v/u)$. On obtient alors la relation $m' = \overline{w} \cdot m$, et donc que m est le ppcm à gauche de $\overline{u}$ et $\overline{v}$ □

Proposition 3.25. *L'ensemble des mots représentant les simples de B_n^{+*} est stable par $\backslash$ et $/$.*

Démonstration. Soient u et v deux mots représentant des simples de B_n^{+*}. Par la proposition 2.36, les tresses $\overline{u}$ et $\overline{v}$ sont des diviseurs à droite de δ_n. La tresse δ_n est donc un multiple commun à gauche de $\overline{u}$ et $\overline{v}$. La proposition 3.24 implique alors que $(v/u)u$ et $(u/v)v$ représentent le ppcm à gauche de $\overline{u}$ et $\overline{v}$. Ainsi $\overline{(v/u)} \cdot \overline{u}$ et $\overline{(u/v)} \cdot \overline{v}$ sont des diviseurs à droite de δ_n. La proposition 2.36 assure donc que v/u et u/v sont des mots représentant les simples du monoïde de tresse dual B_n^{+*}.

Le cas de $\backslash$ se démontre par un argument symétrique. □

Les propositions 3.21 et 3.25 nous assurent que les algorithmes 1 et 2 se terminent. Plus précisément, on obtient :

Corollaire 3.26. *Appliqués à un mot avec p lettres négatives et q lettres positives, les algorithmes 1 et 2 se terminent en temps $O(pq)$ et renvoient un mot de longueur $O(p+q)$.*

En particulier, les algorithmes 1 et 2 appliqués à un mot de longueur ℓ se terminent en temps $O(\ell^2)$ et renvoient un mot de longueur $O(\ell)$.

Une conséquence de la proposition 3.24 et de l'arrêt des algorithmes de retournement est que ceux-ci permettent de décider ci deux tresses de B_n^{+*} se divisent ou pas :

Corollaire 3.27. *Pour u et v des A_n^+-mots , la tresse $\overline{v}$ (*resp. *$\overline{u}$) est un diviseur à droite de $\overline{u}$ (*resp. *à gauche de $\overline{v}$) si et seulement si v/u (*resp. *$v\backslash u$) est le mot vide.*

Démonstration. Que $\overline{v}$ soit un diviseur à droite de $\overline{u}$ est équivalent à ce que le ppcm à gauche de $\overline{v}$ et $\overline{u}$ soit la tresse $\overline{u}$. Par la proposition 3.24, le ppcm à gauche de $\overline{u}$ et $\overline{v}$ est représenté par le mot $(v/u)u$. Ainsi, que le ppcm à gauche de $\overline{v}$ et $\overline{u}$ soit $\overline{u}$ est équivalent à ce que le mot v/u soit vide. De même pour la division à gauche. □

III. Formes normales

Nous avons vu que toute tresse de B_n est représentée par une infinité de mots. Une forme normale est une méthode permettant d'isoler un mot particulier parmi l'infinité représentant une tresse donnée. Une telle forme permet donc en particulier de résoudre le problème du mot : pour savoir si deux mots w et w' représentent la même tresse, on calcule la forme normale de $\overline{w}$, celle de $\overline{w'}$, et on vérifie s'il y a égalité ou pas.

La première forme normale efficace d'un point de vue algorithmique sur B_n est celle introduite en 1969 par F.A. Garside dans [Gar69]. Cette forme est d'abord définie sur le monoïde de tresses positives B_n^+ puis étendue au groupe B_n tout entier en utilisant le fait que B_n est le groupe de fractions de B_n^+. On peut généraliser la forme normale de Garside à une plus vaste famille de monoïdes que le monoïde des tresses positives, qu'on appelle monoïdes de Garside. Ceci est le cas en particulier du monoïde de tresses dual B_n^{+*}.

P. Dehornoy a donné en 2008 dans [Deh08] une autre forme normale dite *alternante* sur les monoïdes dits *localement Garside*, qui sont un affaiblissement des monoïdes de Garside. Il montre en particulier, grâce aux travaux de S. Burckel, que la forme normale alternante de B_n^+ possède un lien fort avec l'ordre des tresses $<$. Comme pour la forme normale de Garside, on peut définir la forme normale alternante sur le groupe de tresses B_n tout entier en utilisant le fait que B_n est le groupe de fractions de B_n^+. Il est à noter qu'il existe des formes normales pouvant être directement définies sur le groupe de tresses B_n. C'est le cas en particulier de la forme normale introduite en 2007 par X. Bressaud dans [Bre08] et étudiée ensuite par J. Chamboredon dans [Cha07].

Le but de ce chapitre est, premièrement, de décrire les formes normales que l'on vient d'introduire, deuxièmement, de généraliser la forme normale alternante aux monoïdes de tresses duaux B_n^{+*}.

1 Structure de Garside

Nous avons déjà mentionné que le monoïde de tresses positives et le monoïde de tresses dual possédaient une structure de Garside. Nous n'avons cependant pas encore donné une vraie définition de ce qu'est un monoïde de Garside.

1.1 Monoïde de Garside

La définition de monoïde de Garside donnée ici repose sur la définition de monoïde localement Garside. On introduit ces monoïdes car ce sont ceux susceptibles de pouvoir être équipés d'une *forme normale alternante* au sens de [Deh08].

Si M est un monoïde, et x, y des éléments de M, on dira que y est un *diviseur à droite* de x, ou, de manière équivalente, que x est un *multiple à gauche* de y, et on note $x \succcurlyeq y$, si la relation $x = zy$ est vérifiée pour un certain élément z de M. L'ensemble de tous les diviseurs à droite de x est noté $\mathrm{Div}_d(x)$. De même, on définit *diviseur à gauche*, *multiple à droite*, $\preccurlyeq$ et l'ensemble $\mathrm{Div}_g(x)$.

Définition 1.1. On dit qu'un monoïde M est *localement Garside à droite* si :
– (C_1^d) Le monoïde M est simplifiable à droite, c'est-à-dire, $xz = yz$ implique $x = y$;
– (C_2^d) Deux éléments de M admettant un multiple commun à droite admettent un ppcm à droite ;
– (C_3^d) Pour tout élément x de M, il n'existe pas de suite infinie strictement croissante dans l'ensemble $(\mathrm{Div}_d(x), \succcurlyeq)$.
De même, le monoïde M est dit *localement Garside à gauche* s'il vérifie (C_1^g), (C_2^g) et (C_3^g) où (C_i^g) est une adaptation au cas gauche de la propriété (C_i^d).

Si M est un monoïde localement Garside à droite, et x, y deux éléments de M vérifiant la relation $x \succcurlyeq y$, alors l'élément z satisfaisant $x = zy$ est unique par simplification à droite. De même pour un monoïde localement Garside à gauche et $\preccurlyeq$.

Proposition 1.2. *Pour tout monoïde M localement Garside à droite, la division à droite est un ordre non strict sur M.*

Démonstration. Comme, pour tout x élément de M, on a $x = 1\,x$, la relation $\succcurlyeq$ est réflexive. Pour des éléments x, y et z vérifiant $x \succcurlyeq y$ et $y \succcurlyeq z$, il existe z' et z'' satisfaisant $x = z'y$ et $y = z''z$. En remplaçant y dans la décomposition de x par $z''z$, on obtient $x = z'z''z$. Ceci montre la relation $x \succcurlyeq z$ et donc la transitivité de $\succcurlyeq$. Pour montrer la réflexivité et la transitivité de $\succcurlyeq$, nous n'avons utilisé que l'aspect monoïdal de M. L'antisymétrie de $\succcurlyeq$ est montrée à partir des propriétés (C_1^d) et (C_3^d) du monoïde localement Garside à droite M. Soient x et y deux éléments vérifiant $x \succcurlyeq y$ et $y \succcurlyeq x$. Il existe z et z' vérifiant $x = zy$ et $y = z'x$. La relation $x = zz'x$ implique $1 = zz'$ par (C_1^d). L'élément z est donc trivial : en effet si on suppose $zz' = 1$ avec $z \neq 1$ et donc $z' \neq 1$, la suite $z, 1, z, 1, ...$ contredirait (C_3^d). Ainsi les éléments x et y sont égaux. □

Définition 1.3. Un monoïde M est dit *localement Garside* s'il est localement Garside à droite et à gauche.

Proposition 1.4. *Le monoïde de tresses dual B_n^{+*} est localement Garside.*

Démonstration. Les conditions (C_1^d) et (C_1^g) ont été prouvées à la proposition II.3.19, tandis que (C_2^d) et (C_2^g) ont été prouvées à la proposition II.3.24. Il nous reste donc à établir (C_3^d) et (C_3^g). Soit β un élément de B_n^{+*}. Par définition de $\succcurlyeq$, on a $\beta \succcurlyeq \beta'$ si et seulement si il existe γ dans B_n^{+*} vérifiant $\gamma\beta' = \beta$. En particulier, on a $|\gamma\beta'| = \beta$ et donc $|\beta'| \leqslant |\beta|$. Comme le nombre de A_n^+-mots de longueur ℓ est au plus $\left(\frac{n(n-1)}{2}\right)^\ell$, il n'existe qu'un nombre fini de diviseurs à droite de β et donc qu'il n'existe pas de suite infinie strictement croissante dans l'ensemble $(\mathrm{Div}_d(\beta), \succcurlyeq)$. On utilise un argument symétrique pour $(\mathrm{Div}_g(\beta), \preccurlyeq)$. □

Définition 1.5. On dit que Δ appartenant à M est un *élément de Garside* pour M si les diviseurs à gauche et à droite de Δ coïncident, s'ils sont en nombre fini et s'ils engendrent M.

Exemple 1.6. La tresse δ_n est un élément de Garside de B_n^{+*}. En effet, on a montré à la proposition II.2.36 que ses diviseurs à gauche et à droite sont les simples de B_n^{+*}. Ces derniers sont en bijection avec les partitions non croisées de $\{1, ..., n\}$ et sont donc en nombre fini. De plus la tresse $a_{p,q}$ est simple car elle est l'image par r de (p, q).

Définition 1.7. On dit qu'un monoïde M est un *monoïde de Garside* si M est localement Garside et contient un élément de Garside.

Une conséquence de la proposition 1.4 et de l'exemple 1.6 est que le monoïde de tresses dual B_n^{+*} est un monoïde de Garside. Comme le suggère la terminologie, il en est de même pour le monoïde de tresses positives B_n^+ étudié par F.A. Garside.

Nous allons maintenant détailler un peu ce point. Commençons d'abord par définir la tresse fondamentale Δ_n de B_n^+, en posant

$$\Delta_2 = \sigma_1 \quad \text{et} \quad \Delta_n = \delta_n \Delta_{n-1}. \tag{3.1}$$

Par exemple, on a $\Delta_3 = \sigma_1\sigma_2\,\sigma_1$, $\Delta_4 = \sigma_1\sigma_2\sigma_3\,\sigma_1\sigma_2\sigma_1$, etc. Le résultat suivant est démontré dans [Gar69] :

Proposition 1.8. *La tresse Δ_n est un élément de Garside de B_n^+.*

Comme les relations de la présentation (I.1.5) préservent la longueur, les diviseurs à droite et à gauche d'un élément de B_n^+ sont en nombre fini. Les conditions (C_3^d) et (C_3^g) sont donc vérifiées pour B_n^+. Les diviseurs de Δ_n sont appelés simples de B_n^+.

Il n'est pas plus difficile que pour le monoïde B_n^{+*} de définir un retournement à gauche et à droite sur B_n^+ détectant les équivalences et se terminant quel que soit le mot d'entrée. En particulier on montre que toutes tresses β et β' de B_n^+ possédant un multiple commun à gauche et à droite admettent un ppcm à gauche et un ppcm à droite.

1.2 Forme normale de Garside

Dans cette section nous allons décrire la forme normale dite de Garside dans le contexte des monoïdes de Garside.

Lemme 1.9. *Soit M un monoïde de Garside d'élément de Garside Δ. Alors pour tout x de M il existe un unique diviseur à droite maximal x_1 appartenant à* $\mathrm{Div}_d(\Delta)$.

Démonstration. Posons $X = \mathrm{Div}_d(x) \cap \mathrm{Div}_d(\Delta)$. L'ensemble X n'est pas vide car il contient l'élément neutre 1. Soient y et y' deux éléments de X. Alors y et y' sont des diviseurs à droite de Δ, c'est-à-dire que Δ est un multiple à gauche de y et y'. La condition (C_2^g) implique donc que y et y' ont un multiple commun à gauche, que l'on note z. Des relations $x \succcurlyeq y$ et $x \succcurlyeq y'$ on déduit que z est un diviseur à droite de x et donc un élément de X. On a ainsi montré que deux éléments de X ont un ppcm dans l'ensemble X. Les diviseurs à droite de Δ étant en nombre fini (définition 1.5), X est fini. On définit alors x_1 comme le ppcm des éléments de X. □

Exemple 1.10. Considérons le monoïde B_3^{+*} et la tresse $\beta = a_{2,3}a_{1,2}a_{2,3}a_{1,2}$. Nous rappelons que les diviseurs de δ_3 sont $\{1, a_{1,2}, a_{2,3}, a_{1,3}, a_{1,2}\,a_{2,3}\}$ et que les relations dans B_3^{+*} sont engendrées par $a_{1,2}a_{2,3} = a_{2,3}a_{1,3} = a_{1,3}a_{1,2}$. L'ensemble $\{1, a_{1,2}\}$ est évidement inclus dans l'ensemble $\mathrm{Div}_d(\beta) \cap \mathrm{Div}_d(\delta_3)$. Grâce aux relations $a_{1,2}a_{2,3} = a_{2,3}a_{1,3}$ et $a_{1,3}a_{1,2} = a_{2,3}a_{1,3}$, on obtient

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

La tresse $a_{1,3}$ est donc un élément de $\mathrm{Div}_d(\beta) \cap \mathrm{Div}_d(\delta_3)$. Ainsi le ppcm à gauche de $a_{1,2}$ et $a_{1,3}$ est un élément de $\mathrm{Div}_d(\beta) \cap \mathrm{Div}_d(\delta_3)$, c'est-à-dire, que δ_3 est un diviseur à droite de β. En effet, on vérifie la relation $\beta = a_{2,3}a_{2,3} \cdot a_{1,2}a_{2,3}$. Comme δ_3 est le plus grand élément de $\mathrm{Div}_d(\delta_3)$, on a $\beta_1 = \delta_3$.

Regardons maintenant la même tresse β mais vue dans le monoïde B_3^+.

Exemple 1.11. Considérons le monoïde B_3^+ et la tresse $\beta = \sigma_1\sigma_2\sigma_1\sigma_2$. Nous rappelons que les diviseurs de $\Delta_3 = \sigma_1\sigma_2\sigma_1$ sont $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1, \Delta_3\}$ et que les relations dans B_3^+ sont engendrées par la relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. Dans ce cas il est immédiat que Δ_3 est un diviseur à droite de β.

En itération la construction du lemme 1.9, on obtient :

Proposition 1.12. *Soit M un monoïde de Garside associé à l'élément de Garside Δ. Alors pour tout x élément de M, il existe une unique décomposition $x = x_b \cdot ... \cdot x_1$ avec $x_b \neq 1$ et où x_k est le plus grand diviseur à droite de $x_b \cdot ... \cdot x_k$ appartenant à $\mathrm{Div}_d(\Delta)$ pour tout k.*

Démonstration. Soit x un élément de M. Notons x_1 le plus grand élément de l'intersection de $\mathrm{Div}_d(x)$ et $\mathrm{Div}_d(\Delta)$. Il existe alors x'_1 dans M vérifiant $x = x'_1 \cdot x_1$. Par induction, pour $k \geqslant 2$ on définit x_k comme le plus grand élément de $\mathrm{Div}_d(x_{k-1}) \cap \mathrm{Div}_d(\Delta)$ et on note x'_k l'élément de M satisfaisant $x'_{k-1} = x'_k \cdot x_k$. Par construction la suite

$$x_1, x_2\, x_1, x_3\, x_2\, x_1, ...$$

de diviseurs à droite de x est non croissante. La condition (C_3^d) assure alors qu'il existe b tel que le terme x'_b soit trivial. On a donc $x = x_b \cdot ... \cdot x_1$.

Montrons l'unicité. Soit $y_c \cdot ... \cdot y_1$ une autre telle décomposition de x. Par construction, les éléments x_1 et y_1 sont des maximums de $\mathrm{Div}_d(x) \cap \mathrm{Div}_d(\Delta)$. Le lemme 1.9 implique donc l'égalité entre x_1 et y_1. On continue de proche en proche pour obtenir $x_k = y_k$ pour tout k. □

La décomposition $x_b \cdot ... \cdot x_1$ est appelée *forme normale de Garside de x*.

Exemple 1.13. Considérons la tresse $\beta = \sigma_2\sigma_1\sigma_2\sigma_1$ de B_3^+. On utilise les notations de la proposition 1.12. À l'exemple 1.11 on a établi $\beta_1 = \Delta_3$ avec $\beta'_1 = \sigma_2$. On a donc $\beta_2 = \sigma_2$ et $\beta'_2 = 1$. Ainsi la forme normale de Garside de β est $\sigma_1 \cdot \Delta_3$.

Exemple 1.14. Considérons la tresse $\beta = a_{2,3}a_{1,2}a_{2,3}a_{1,2}$ de B_3^{+*}. On utilise les notations de la proposition 1.12. À l'exemple 1.10 on a établi $\beta_1 = \delta_3$ avec $\beta'_1 = a_{2,3}a_{2,3}$. Comme $a_{2,3}a_{2,3}$ n'est pas un diviseur de δ_3, on a $\beta_2 = a_{2,3}$ et $\beta'_2 = a_{2,3}$. Enfin on a $\beta_3 = a_{2,3}$ et $\beta'_3 = 1$. La forme normale de Garside de la tresse β est donc $a_{2,3} \cdot a_{2,3} \cdot \delta_3$.

Les tresses considérées dans les deux exemples précédents sont identiques. Néanmoins leurs formes normales de Garside positives ou duales diffèrent.

1.3 Forme normale alternante

L'idée développée dans [Deh08] par P. Dehornoy est de décrire les tresses de B_n^+ comme suites de tresses de B_{n-1}^+. Une telle décomposition est définie dans un cadre plus général que les monoïdes de tresses positives : les monoïdes localement Garside à droite. Le calcul de la forme normale alternante sur un monoïde localement Garside à droite M dépend de deux sous-monoïdes M_0 et M_1 de M ayant certaines caractéristiques. Nous allons voir ici quelques points de [Deh08]. Les démonstrations sont omises et nous référons à l'article original.

Soit M un monoïde localement Garside à droite. On dit qu'une partie A de M est *close par ppcm à gauche*, si le ppcm à gauche de deux éléments de A appartient à A. Les sous-ensembles de M clos par ppcm à gauche permettent de décomposer les éléments de M, comme le montre le résultat suivant.

Lemme 1.15. *Supposons que M soit un monoïde localement Garside à droite et A un sous-ensemble de M clos par ppcm à gauche. Alors, pour tout élément x de M, il existe un unique diviseur à droite x_1 de x de A maximal pour la division à droite.*

La démonstration de ce lemme consiste à montrer que l'ensemble $\mathrm{Div}_d(x) \cap A$ muni de la relation $\succcurlyeq$ est un treillis, l'élément x_1 en étant alors le plus grand élément.

L'élément x_1 introduit dans le lemme 1.15 est appelé *A-fin* de x.

La forme normale de Garside repose sur ce résultat. Soit M un monoïde de Garside ayant pour élément de Garside Δ. Notons S l'ensemble des diviseurs de Δ, (on rappelle que dans un monoïde de Garside, les diviseurs à gauche et à droite de l'élément de Garside Δ coïncident). Le monoïde M est en particulier un monoïde localement Garside à droite. Comme deux éléments x et y de S admettent un multiple à gauche, à savoir Δ, ils admettent un ppcm à gauche z, par la propriété (C_2^g). L'élément z étant un diviseur de Δ, il appartient à l'ensemble S. L'ensemble S est donc clos par ppcm à gauche. La S-fin d'un élément x de M correspond au premier terme de la forme normale de Garside de x. La différence majeure entre la forme normale alternante et celle de Garside est que la version alternante fait intervenir des monoïdes et non des ensembles.

Définition 1.16. Soit M un monoïde localement Garside à droite. On dit qu'un sous-monoïde N de M est *fermé* s'il est clos par ppcm à gauche et clos par division à gauche, c'est-à-dire, que le ppcm à gauche de deux éléments de N est dans N et que tout diviseur à gauche d'un élément de N appartient à N.

Exemple 1.17. Le monoïde B_{n-1}^+ est fermé dans B_n^+. En effet, soient β et β' deux tresses de B_{n-1}^+. Il existe alors un entier k tel que Δ_{n-1}^k soit un multiple à gauche de β et β'. Le ppcm à gauche de β et β' est alors un diviseur de Δ_{n-1}^k et appartient donc à B_{n-1}^+. De même les diviseurs à gauche d'un élément de B_{n-1}^+ sont dans B_{n-1}^+.

On peut améliorer le lemme 1.15 si A est un sous-monoïde fermé de M.

Lemme 1.18. (P. Dehornoy, [Deh08]) *Soit M un monoïde localement Garside à droite et M_1 un sous-monoïde fermé de M. Alors pour tout x de M, il existe une unique décomposition $x' \cdot x_1$ de x vérifiant*

$$x_1 \in M_1 \quad \text{et} \quad \mathrm{Div}_d(x') \cap M_1 = \{1\}. \tag{3.2}$$

L'élément x_1 est la M_1-fin de x tandis que x' est déterminé par $x' = xx_1^{-1}$.

Exemple 1.19. Calculons la B_3^+-fin de Δ_4. Par construction Δ_4 est égale à $\delta_4 \cdot \Delta_3$. La tresse δ_4 est représentée par le mot $\sigma_1\sigma_2\sigma_3$. On ne peut appliquer aucune relation de la présentation sur ce dernier mot, donc δ_4 est représentée par un unique mot. Il s'ensuit que le seul diviseur à droite de la tresse δ_4 existant dans B_3^+ est trivial. Ainsi la B_3^+-fin de Δ_4 est Δ_3.

Revenons au cas d'un monoïde de Garside M associé à un élément de Garside Δ et de l'ensemble S des simples associé à Δ, c'est-à-dire, des diviseurs de Δ. Le cas de B_3^+ avec la tresse de Garside Δ_3 montre que S n'est pas un monoïde en général ($\sigma_1\sigma_1$ n'est pas un diviseur de Δ_3). On peut naturellement se demander s'il existe des monoïdes de Garside (M, Δ) pour lesquels l'ensemble des simples S est un monoïde. De tels monoïdes sont assez inintéressants, en effet pour que M soit de Garside, il faut que S engendre M, ce qui signifie ici que S doit être M tout entier. Ce qui implique que M soit fini. De plus le premier terme de la forme normale de Garside d'un élément x de M , c'est-à-dire, la S-fin de x, serait x lui-même, ce qui n'a pas beaucoup d'intérêt.

Définition 1.20. Pour M, monoïde localement Garside à droite, on dit que le couple (M_2, M_1) *recouvre* M si M_2 et M_1 sont des sous-monoïdes fermés de M et si l'union $M_2 \cup M_1$ engendre M.

Pour chaque entier i, on définit le symbole $[i]$ par

$$[i] = \begin{cases} 1 & \text{pour } i \text{ impair,} \\ 2 & \text{sinon.} \end{cases}$$

Le résultat suivant montre que l'on peut décomposer de manière unique un élément d'un monoïde M en construisant alternativement la M_1-fin et la M_2-fin, où M_1 et M_2 sont des sous-monoïdes de M ayant certaines propriétés :

Proposition 1.21. (P. Dehornoy, [Deh08]) *Supposons que M soit un monoïde localement Garside à droite et (M_2, M_1) un recouvrement de M. Alors, pour tout élément non trivial x de M, il existe une unique suite d'éléments $(x_p, \dots, x_1)$ vérifiant $x_p \neq 1$ et, pour tout $i \geq 1$,*

$$x_i \in M_{[i]} \quad \text{et} \quad \mathrm{Div}_d(x_p \cdot \dots \cdot x_{i+1}) \cap M_{[i]} = \{1\}. \tag{3.3}$$

Regardons le cas particulier des monoïdes de Garside B_n^+ associés à l'élément de Garside Δ_n. Par définition le ppcm à gauche Δ_n des générateurs d'Artin $\sigma_1, \dots, \sigma_{n-1}$ est aussi leur ppcm à droite. Ceci implique que l'automorphisme intérieur Φ_n du groupe B_n associé à Δ_n préserve le monoïde B_n^+, et, donc, que Φ_n induit un automorphisme du monoïde B_n^+. De plus, l'automorphisme Φ_n préserve la divisibilité à gauche (et à droite), donc il préserve les opérations de pgcd et de ppcm. On vérifie facilement que Φ_n échange σ_i et σ_{n-i} pour tout i, donc, géométriquement, Φ_n agit comme une symétrie sur les diagrammes de tresses.

Notons que les sous-monoïdes B_{n-1}^+ et $\Phi_n(B_{n-1}^+)$ sont clos pour $n \geq 3$. Comme l'image de la tresse σ_1 par Φ_n est σ_{n-1}, le couple $(\Phi_n(B_{n-1}^+), B_{n-1}^+)$ recouvre le monoïde B_n^+. Il est donc possible d'appliquer la proposition 1.21 pour les monoïdes $M = B_n^+$, $M_1 = B_{n-1}^+$ et $M_2 = \Phi_n(B_{n-1}^+)$. La proposition 1.21 dans ce cas particulier devient :

Proposition 1.22. (P. Dehornoy, [Deh08]) *Toute tresse β de B_n^+ admet une décomposition unique*

$$\beta = \Phi_n^{[b]-1}(\beta_b) \cdot \Phi_n^{[b-1]-1}(\beta_{b-1}) \cdot \dots \cdot \beta_3 \cdot \Phi_n(\beta_2) \cdot \beta_1 \tag{3.4}$$

avec $\beta_b, \dots, \beta_1$ éléments de B_{n-1}^+ tels que, pour tout $k \geqslant 1$,

$$\mathrm{Div}_d(\Phi_n^{[b]-1}(\beta_b) \cdot \Phi_n^{[b-1]-1}(\beta_{b-1}) \cdot \dots \cdot \Phi_n^{[k+1]-1}(\beta_{k+1})) \cap M_{[k]} = \{1\}.$$

Définition 1.23. La suite $(\beta_b, \dots, \beta_1)$ introduite à la proposition 1.22 est appelée Φ_n-*éclatement* de β.

Le Φ_n-éclatement d'une tresse de B_n^+, consiste à prendre alternativement le plus grand diviseur à droite qui laisse invariant le n-ème et le premier brin.

Exemple 1.24. Calculons le Φ_4-éclatement de Δ_4. A l'exemple 1.19 nous avons déjà vu que la B_3^+-fin de Δ_4 est Δ_3 et que la tresse quotient $\Delta_4\Delta_3^{-1}$ est représentée par un seul mot positif, à savoir $\sigma_1\sigma_2\sigma_3$. La $\Phi_4(B_3^+)$-fin de $\sigma_1\sigma_2\sigma_3$ est le plus gros diviseur à droite sans σ_1, c'est à dire, la tresse $\sigma_2\sigma_3$. Comme on a $\sigma_2\sigma_3 = \Phi_4(\sigma_2\sigma_1)$, le Φ_4-éclatement de Δ_4 est $(\sigma_1, \sigma_2\sigma_1, \Delta_3)$.

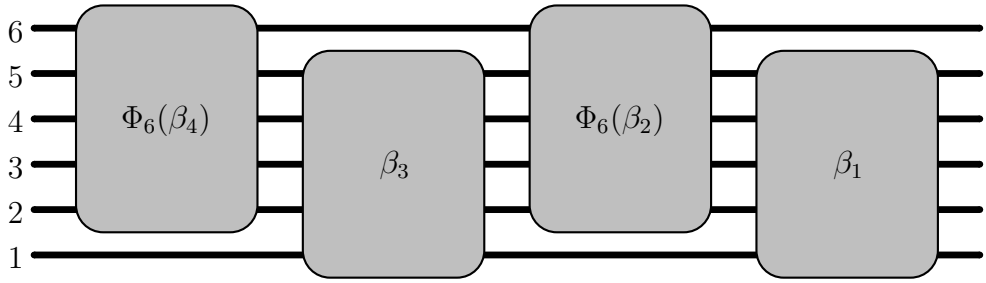


FIG. 3.1 : Partant d'une tresse β de B_6^+, on prend le plus grand diviseur à droite de β laissant le 6 ème brin invariant, puis on prend le plus grand diviseur à droite du reste laissant le 1 er brin invariant, etc.

Le Φ_n-éclatement permet d'étendre certaines propriétés de B_{n-1}^+ à B_n^+. En particulier on peut définir une forme normale sur B_n^+ par induction sur n. Avant de poursuivre il nous faut définir l'application Φ_n sur les Σ_n^+-mots, c'est-à-dire, les mots en les lettres σ_i avec $1 \leqslant i \leqslant n-1$.

L'application Φ_n envoie σ_i sur σ_{n-i}. A partir de cette observation, on peut introduire l'homomorphisme sur les B_n^+-mots, aussi noté Φ_n, envoyant la lettre σ_i sur la lettre σ_{n-i}. Notons que si une tresse β est représentée par un Σ_n^+-mot w alors la tresse $\Phi_n(\beta)$ est représentée par le mot $\Phi_n(w)$.

Définition 1.25.
– Pour β dans B_2^+, la Φ_2-*forme normale* de β est l'unique mot de la forme σ_1^k représentant β.
– Pour β dans Σ_n^+ avec $n \geqslant 3$, la Φ_n-*forme normale* de β est le B_n^+-mot

$$\Phi_n^{[b]-1}(w_b)\, \Phi_n^{[b-1]-1}(w_{b-1}) \dots w_3\, \Phi_n(w_2)\, w_1,$$

où $(\beta_b, \dots, \beta_1)$ est le Φ_n-éclatement de β et w_k la Φ_{n-1}-forme normale de β_k pour tout k.

Comme le Φ_n-éclatement d'une tresse β de B_{n-1}^+ est la suite (β), la Φ_n-forme normale et la Φ_{n-1}-forme normale coïncident sur B_{n-1}^+. On peut donc retirer l'indice n et parler de la Φ-forme normale ou bien de la *forme normale alternante*.

En utilisant les résultats de S. Burckel dans [Bur94, Bur97], P. Dehornoy montre que la forme normale alternante de B_n^+ peut servir à décrire la restriction de l'ordre des tresses $<$ à B_n^+ :

Théorème 1.26. (P. Dehornoy, [Deh08]) *Pour β, β' dans B_n^+, la relation $\beta < \beta'$ est vraie si et seulement si le Φ_n-éclatement de β est plus petit que le Φ_n-éclatement de β' vis à vis de l'extension `ShortLex` de la restriction de l'ordre $<$ à B_{n-1}^+.*

On rappelle que si $(X, \prec)$ est un ensemble ordonné, une suite finie s d'éléments de X est dite `ShortLex` plus petite qu'une autre suite finie s', si la longueur de s est strictement plus petite que celle de s', ou alors si les longueurs de s et s' sont égales et s est $\prec$-lexicographiquement plus petite que s', c'est-à-dire que lorsque les deux suites sont lues en partant de la gauche, le premier terme dans s qui ne coïncide pas avec son homologue dans s' est plus petit pour l'ordre $\prec$.

2 La forme normale tournante

Le monoïde de tresses dual B_n^{+*} est un monoïde de Garside. Ainsi dès qu'on a deux sous-monoïdes M_0 et M_1 de B_n^{+*} recouvrant B_n^{+*}, on peut introduire une forme normale alternante.

Construire une forme normale n'est pas difficile. Ce qui est difficile est de décrire les propriétés de cette forme normale et d'essayer de s'en servir en interaction avec d'autres structures définies sur le monoïde considéré.

Nous n'allons donc pas nous contenter d'adapter la forme normale alternante à B_n^{+*} mais nous allons la généraliser à l'aide de quelques modifications afin de définir une nouvelle forme normale dite *tournante* ayant de bonnes propriétés vis-à-vis de la restriction de l'ordre $<$ à B_{n-1}^{+*}.

2.1 La B_{n-1}^{+*}-fin

Dans la sous-section 1.3, nous avons rappelé que la forme normale alternante était construite à partir de l'opération dite de Φ_n-éclatement basée sur l'automorphisme intérieur du groupe B_n associé à Δ_n.

En général, la conjugaison par une tresse positive n'a aucune raison de stabiliser le monoïde de tresses positives B_n^+. C'est parce que l'on conjugue par l'élément de Garside Δ_n que l'application $\beta \mapsto \Delta_n^{-1}\beta\Delta_n$ est un automorphisme de B_n^+. [Deh02].

Nous avons vu que le monoïde B_n^{+*} est aussi un monoïde de Garside relativement à l'élément de Garside δ_n défini par

$$\delta_n = a_{1,2}\, a_{2,3} \ldots a_{n-1,n}.$$

Pour toute tresse β de B_n^{+*}, on définit $\phi_n(\beta)$ comme étant l'unique tresse de B_n^{+*} vérifiant

$$\delta_n\, \beta = \phi_n(\beta)\, \delta_n. \tag{3.5}$$

Existe-t-il une bonne description de l'action de ϕ_n sur les tresses $a_{p,q}$ comme dans le cas de Φ_n sur les tresses σ_i ? Le résultat suivant répond à la question :

Lemme 2.1. *Pour p, q avec $1 \leqslant p < q \leqslant n$, on a*

$$\phi_n(a_{p,q}) = \begin{cases} a_{p+1,q+1} & \text{pour } q \leqslant n-1, \\ a_{1,p+1} & \text{pour } q = n. \end{cases} \tag{3.6}$$

Démonstration. Supposons $q \leqslant n-1$. Par définition de δ_n et $d_{p,q}$ (voir (II.2.4)), on a $\delta_n = d_{1,n}$. La relation (II.2.5) implique $a_{p,q} = d_{p,q} d_{p,q-1}^{-1}$. Ainsi en appliquant deux fois (II.2.8) puis (II.2.5), on obtient :

$$\delta_n \cdot a_{p,q} = d_{1,n} \cdot d_{p,q}\, d_{p,q-1}^{-1} = d_{p+1,q+1} \cdot d_{1,n} \cdot d_{p,q-1}^{-1} = d_{p+1,q+1}\, d_{p+1,q}^{-1} \cdot d_{1,n} = a_{p+1,q+1} \cdot \delta_n.$$

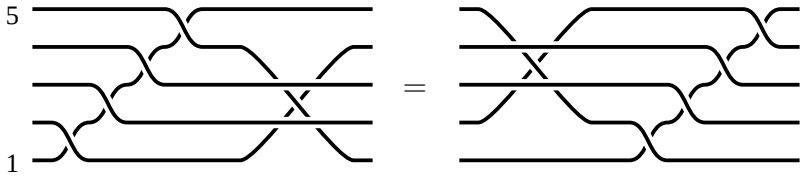


FIG. 3.2 : Illustration de la formule (3.6) pour $n = 5$ et $a_{p,q} = a_{1,4}$.

Supposons maintenant $q = n$. En reprenant la définition de δ_n et en utilisant successivement

la relation (II.2.3), on obtient

$$\begin{aligned}
\delta_n \cdot a_{p,n} &= a_{1,2}\, a_{2,3} \dots a_{p-1,p}\, a_{p,p+1} \dots a_{n-2,n-1}\, a_{n-1,n} \cdot a_{p,n} \\
&= a_{1,2}\, a_{2,3} \dots a_{p-1,p}\, a_{p,p+1} \dots a_{n-2,n-1} \cdot a_{p,n-1} \cdot a_{n-1,n} \\
&= \dots \\
&= a_{1,2}\, a_{2,3} \dots a_{p-1,p}\, a_{p,p+1} \cdot a_{p,p+1} \cdot \dots a_{n-2,n-1}\, a_{n-1,n} \\
&= a_{1,2}\, a_{2,3} \dots a_{p-1,p} \cdot a_{p,p+1} \cdot a_{p,p+1} \dots a_{n-2,n-1}\, a_{n-1,n} \\
&= a_{1,2}\, a_{2,3} \dots \cdot\ a_{p-1,p+1} \cdot a_{p-1,p}\, a_{p,p+1} \dots a_{n-2,n-1}\, a_{n-1,n} \\
&= \dots \\
&= a_{1,2} \cdot a_{2,p+1} \cdot a_{2,3} \dots a_{p-1,p}\, a_{p,p+1} \dots a_{n-2,n-1}\, a_{n-1,n} \\
&= a_{1,p+1} \cdot a_{1,2}\, a_{2,3} \dots a_{p-1,p}\, a_{p,p+1} \dots a_{n-2,n-1}\, a_{n-1,n} = a_{1,p+1} \cdot \delta_n
\end{aligned}$$

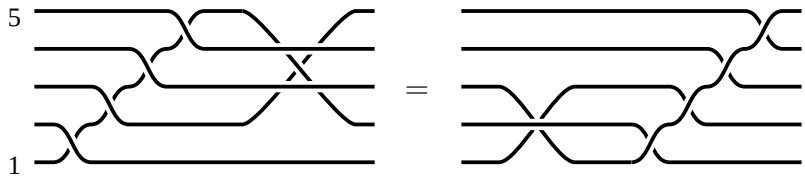


FIG. 3.3 : Illustration de la formule (3.6) pour $n = 5$ et $a_{p,q} = a_{2,5}$.

Ceci établit les formules de (3.6) □

Notons que la relation $\phi_n(a_{p,q}) = a_{p+1,q+1}$ est toujours vérifiée à condition que les indices soient pris modulo n et qu'on les échange en cas de besoin afin que le plus petit indice soit à gauche, par exemple le symbole $a_{p+1,n+1}$ donne $a_{p+1,1}$ puis $a_{1,p+1}$.

Il est plus facile de visualiser l'action de l'automorphisme ϕ_n sur un diagramme de cordes. Avec cette manière de voir, il agit comme une rotation d'angle $\frac{2\pi}{n}$ dans le sens trigonométrique.

L'expression « forme normale alternante » provient du fait que l'automorphisme Φ_n de B_n^+ est d'ordre 2. Par analogie, comme ϕ_n est d'ordre n, la forme normale définie à partir de ϕ_n sera dite « tournante ».

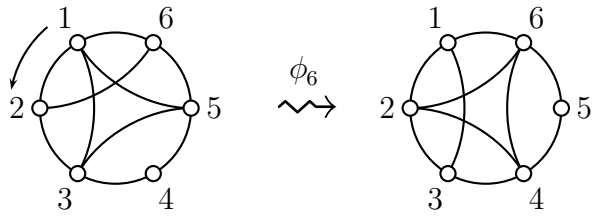


FIG. 3.4 : Représentation de l'automorphisme ϕ_n comme une rotation d'angle $\frac{2\pi}{n}$ dans le sens trigonométrique.

Maintenant que nous venons de décrire l'automorphisme de Garside ϕ_n de B_n^{+*}, nous pouvons construire l'opération de ϕ_n-éclatement, une adaptation du Φ_n-éclatement au cas dual. Tout d'abord assurons-nous que toute tresse de B_n^{+*} admet un unique diviseur à droite maximal appartenant à B_{n-1}^{+*}.

Lemme 2.2. *Pour $n \geqslant 3$, toute tresse β de B_n^{+*} admet un unique diviseur à droite maximal appartenant au monoïde B_{n-1}^{+*}.*

Démonstration. Pour γ dans $\mathrm{Div}_d(\beta)$, on doit avoir $|\gamma| \leqslant |\beta|$. Donc l'ensemble $\mathrm{Div}_d(\beta) \cap B_{n-1}^{+*}$, qui est non vide car il contient la tresse triviale 1, contient un élément β_1 de longueur maximale. Soit γ un élément quelconque de $\mathrm{Div}_d(\beta) \cap B_{n-1}^{+*}$. Comme B_{n-1}^{+*} est clos par ppcm à gauche, car c'est un monoïde de Garside, le ppcm à gauche de β_1 et γ, noté $\beta_1 \vee_G \gamma$, est un élément de B_{n-1}^{+*}. D'autre part la relation $\beta_1 \vee_G \gamma \succcurlyeq \beta_1$ implique $|\beta_1| \leqslant |\beta_1 \vee_G \gamma|$. Ainsi par construction de β_1, on doit avoir $|\beta_1| = |\beta_1 \vee_G \gamma|$, ce qui implique $\beta_1 = \beta_1 \vee_G \gamma$, puis que γ est un diviseur à droite de β. La tresse β_1 est donc un diviseur à droite maximal de β appartenant à B_{n-1}^{+*}.

Montrons maintenant l'unicité. Soit β_1' un autre diviseur à droite maximal de β appartenant à B_{n-1}^{+*}. Par construction de β_1 et β_1', on doit avoir $\beta_1 \leqslant \beta_1'$ et $\beta_1' \leqslant \beta_1$, ce qui, par l'antisymétrie de $\succcurlyeq$ établie à la proposition 1.2, donne $\beta_1 = \beta_1'$. □

Définition 2.3. La tresse β_1 du lemme 2.2 est appelée la B_{n-1}^{+*}-*fin* de β et est notée $\mathrm{fin}_{n-1}(\beta)$.

Le résultat suivant donne une caractérisation de la B_{n-1}^{+*}-fin d'une tresse de B_n^{+*} donnée.

Lemme 2.4. *Pour toute tresse β de B_n^{+*} et toute tresse β_1 de B_{n-1}^{+*}, il y a équivalence entre :*
– (i) *La tresse β_1 est la B_{n-1}^{+*}-fin de β ;*
– (ii) *Il existe une tresse β' de B_n^{+*} dont la B_{n-1}^{+*}-fin est triviale et vérifiant la relation $\beta = \beta'\,\beta_1$.*

Démonstration. Montrons que (i) implique (ii). Comme β_1 est un diviseur à droite de β, il existe β' dans B_n^{+*} vérifiant $\beta = \beta'\,\beta_1$. Notons β_1' la B_{n-1}^{+*}-fin de β'. La tresse $\beta_1'\beta_1$ est donc un diviseur à droite de β appartenant à B_{n-1}^{+*}. Ainsi par l'hypothèse faite sur β_1, on doit avoir l'égalité $\beta_1 = \beta_1'\,\beta_1$ et donc $\beta_1' = 1$.

Montrons que (ii) implique (i). Par hypothèse, la tresse β_1 est un diviseur à droite de β. Il nous reste donc à montrer que c'est le plus grand. Notons β_1' la B_{n-1}^{+*}-fin de β. Il existe alors γ dans B_{n-1}^{+*} vérifiant $\beta_1' = \gamma\,\beta_1$. La tresse γ est donc un diviseur à droite de β', ce qui par hypothèse faite sur β', montre que γ est triviale, c'est-à-dire, que β_1 est égale à β_1'. □

La B_{n-1}^{+*}-fin peut être caractérisée comme l'unique diviseur à droite β_1 de β tel que la tresse $\beta\,\beta_1^{-1}$ n'ait pas de diviseur à droite non trivial dans B_{n-1}^{+*}.

Exemple 2.5. Calculons la B_2^{+*}-fin de la tresse δ_3^2 où δ_3 est l'élément de Garside de B_3^{+*}. Comme B_2^{+*} est engendré par la seule tresse $a_{1,2}$, la B_2^{+*}-fin de δ_3^2 est la plus grande puissance de $a_{1,2}$ qui divise à droite δ_3^2. Par définition, on a $\delta_3^2 = a_{1,2}\,a_{2,3}\,a_{1,2}\,a_{2,3}$. En appliquant deux fois la relation (II.2.3), on obtient

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

La présentation (II.2.13) implique que toutes les relations de B_3^{+*} sont conséquences de

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

Le mot $a_{1,2}\,a_{2,3}$ n'apparaissant pas dans ces relations, il est seul dans sa classe d'équivalence. Ainsi la tresse qu'il représente ne peut pas être divisible à droite par $a_{1,2}$. On a donc montré que la B_2^{+*}-fin de δ_3^2 est $a_{1,2}^2$.

2.2 Le ϕ_n-éclatement

Pour le Φ_n-éclatement (définissant la forme normale alternante), on obtient une décomposition distinguée en considérant alternativement la B^+_{n-1}-fin et la $\Phi_n(B^+_{n-1})$-fin. Dans le cas du monoïde de tresses dual, pour obtenir une décomposition similaire, nous utiliserons cycliquement la B^{+*}_{n-1}-fin, la $\phi_n(B^{+*}_{n-1})$-fin, ..., et la $\phi_n^{n-1}(B^{+*}_{n-1})$-fin.

Afin de montrer que toute tresse de B^{+*}_n admet une telle décomposition, nous devons d'abord nous assurer que les images de B^{+*}_{n-1} par les différentes itérations de ϕ_n recouvrent B^{+*}_n. En fait seulement deux itérations seront suffisantes.

Lemme 2.6. *Pour $n \geqslant 3$, le monoïde B^{+*}_n est inclus dans $B^{+*}_{n-1} \cup \phi_n(B^{+*}_{n-1}) \cup \phi_n^2(B^{+*}_{n-1})$.*

Démonstration. Pour $q \leqslant n-1$, la tresse $a_{p,q}$ appartient à B^{+*}_{n-1}. Ensuite, pour $p = n$ et $p \geqslant 2$, on a $a_{p,n} = \phi_n(a_{p-1,n-1})$, qui appartient à $\phi_n(B^{+*}_{n-1})$. Finalement pour $p = 1$ et $q = n$, on trouve

$$a_{p,q} = \phi_n(a_{n-1,n}) = \phi_n^2(a_{n-2,n-1}),$$

qui appartient à $\phi_n^2(B^{+*}_{n-1})$. □

En itérant la construction de la $\phi_n^k(B^{+*}_{n-1})$-fin, on associe à chaque tresse de B^{+*}_n une suite finie de tresses de B^{+*}_{n-1} qui la spécifie complètement.

Proposition 2.7. *Supposons $n \geqslant 3$. Alors, pour chaque tresse non triviale β de B^{+*}_n, il existe une unique suite $(\beta_b, \dots, \beta_1)$ de tresses de B^{+*}_{n-1} satisfaisant $\beta_b \neq 1$ et*

– $\beta = \phi_n^{b-1}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_2) \cdot \beta_1$, (2.7.i)

– *pour $k \geqslant 1$, la tresse β_k est la B^{+*}_{n-1}-fin de $\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \beta_k$.* (2.7.ii)

Démonstration. Partant de $\beta^{(0)} = \beta$, on définit deux suites notées $\beta^{(k)}$ et β_k en posant :

$$\beta^{(k)} = \phi_n^{-1}\big(\beta^{(k-1)}\,\beta_k^{-1}\big) \quad \text{et} \quad \beta_k = \mathrm{fin}_{n-1}(\beta^{(k-1)}). \tag{3.8}$$

Prouvons les relations suivantes par induction sur $k \geqslant 1$:

$$\beta = \phi_n^k(\beta^{(k)}) \cdot \phi_n^{k-1}(\beta_k) \cdot \ldots \cdot \beta_1, \tag{3.9}$$

$$\mathrm{fin}_{n-1}\big(\phi_n\big(\beta^{(k)}\big)\big) = 1. \tag{3.10}$$

Supposons $k = 1$. Alors le lemme 2.2 implique que la B^{+*}_{n-1}-fin de la tresse $\beta\,\beta_1^{-1}$ est triviale. Ainsi, comme $\phi_n(\beta^{(1)})$ est égale à $\beta\,\beta_1^{-1}$, la B^{+*}_{n-1}-fin de $\phi_n(\beta^{(1)})$ est triviale et la relation $\beta = \phi_n(\beta^{(1)})$ est satisfaite. Supposons maintenant $k \geqslant 2$. Par construction de $\beta^{(k)}$, on a la relation $\phi_n(\beta^{(k)}) = \beta^{(k-1)}\,\beta_k^{-1}$ et donc $\beta^{(k-1)} = \phi_n(\beta^{(k)}) \cdot \beta_k$. On obtient alors

$$\phi_n^{k-1}\big(\beta^{(k-1)}\big) = \phi_n^k(\beta^{(k)}) \cdot \phi_n^{k-1}\big(\beta_k\big). \tag{3.11}$$

D'un autre côté, l'hypothèse d'induction donne :

$$\beta = \phi_n^{k-1}(\beta^{(k-1)}) \cdot \phi_n^{k-2}(\beta_{k-1}) \cdot \ldots \cdot \beta_1. \tag{3.12}$$

En substituant (3.11) dans (3.12), on obtient la relation (3.9). Comme la tresse β_k est la B^{+*}_{n-1}-fin de la tresse $\beta^{(k-1)}$, le lemme 2.2 implique la relation (3.10).

Par construction, la suite

$$\beta_1,\ \phi_n(\beta_2)\,\beta_1,\ \phi_n^2(\beta_3)\,\phi_n(\beta_2)\,\beta_1,\ \ldots$$

de diviseurs à droite de β est non décroissante. Comme on sait depuis la proposition 1.4 que B_n^{+*} est un monoïde localement Garside, donc en particulier localement Garside à droite, la condition (C_3^d) nous assure que la suite doit être constante à partir d'un certain rang. Il existe donc un entier b minimal tel que pour $k \geqslant b$, on ait

$$\phi_n^{k-1}(\beta_k) \cdot ... \cdot \beta_1 = \phi_n^{b-1}(\beta_b) \cdot ... \cdot \beta_1.$$

La relation (3.9) implique alors

$$\beta = \phi_n^b(\beta^{(b)}) \cdot \phi_n^{b-1}(\beta_b) \cdot ... \cdot \beta_1,$$

avec $\beta_b \neq 1$ par minimalité de b.

Par construction de b, pour $k \geqslant b+1$ on a $\beta_k = 1$, ce qui, par la relation (3.8), entraîne $\phi_n(\beta^{(k)}) = \beta^{(k-1)}$. Ainsi les relations

$$\beta^{(b)} = \phi_n(\beta^{(b+1)}), \quad \phi_n^{-1}(\beta^{(b)}) = \phi_n(\beta^{(b+2)}) \text{ et } \phi_n^{-2}(\beta^{(b)}) = \phi_n(\beta^{(b+3)})$$

sont satisfaites. La relation (3.10) impliquant alors que les B_{n-1}^{+*}-fins de

$$\beta^{(b)},\ \phi_n^{-1}(\beta^{(b)}) \text{ et } \phi_n^{-2}(\beta^{(b)}),$$

sont triviales, la tresse $\beta^{(b)}$ n'est divisible à droite ni par x, ni par $\phi_n(x)$, ni par $\phi_n^2(x)$, où x est une A_{n-1}^+-lettre. Le lemme 2.6 implique alors que $\beta^{(b)}$ n'est divisible à droite par aucun $a_{p,q}$ avec $1 \leqslant p < q \leqslant n$, c'est-à-dire que la tresse $\beta^{(b)}$ est triviale. On a donc montré que la tresse β est égale à $\phi_n^{b-1}(\beta_b) \cdot ... \cdot \beta_1$.

Prouvons maintenant l'unicité de $(\beta_b, ..., \beta_1)$. Soit $(\gamma_c, ..., \gamma_1)$ une autre suite de tresses de B_{n-1}^{+*} vérifiant

$$\beta = \phi_n^{c-1}(\gamma_c) \cdot ... \cdot \phi_n(\gamma_2) \cdot \phi_n(\gamma_1),$$

avec $\gamma_c \neq 1$ et satisfaisant $\gamma_k = \text{fin}_{n-1}(\phi_n^{c-k}(\gamma_c) \cdot ... \cdot \gamma_k)$ pour tout $k \geqslant 1$. À l'aide d'une induction sur $k \geqslant 1$, montrons les relations

$$\gamma_k = \beta_k \quad \text{et} \quad \phi_n^{c-k-1}(\gamma_c) \cdot ... \cdot \phi_n(\gamma_{k+2}) \cdot \gamma_{k+1} = \beta^{(k)}. \tag{3.13}$$

Par hypothèse, pour $k = 1$, on a $\beta = \big(\phi_n^{c-1}(\gamma_c) \cdot ... \cdot \phi_n(\gamma_2)\big) \cdot \gamma_1$ où γ_1 est la B_{n-1}^{+*}-fin de β. Le lemme 2.2 assurant que la B_{n-1}^{+*}-fin d'une tresse est unique, on a $\beta_1 = \gamma_1$. Il s'ensuit que (3.13) est satisfaite pour $k = 1$. Montrons (3.13) pour $k \geqslant 2$. Par induction, on a

$$\big(\phi_n^{c-k-1}(\gamma_c) \cdot ... \cdot \phi_n(\gamma_{k+2})\big) \cdot \gamma_{k+1} = \beta^{(k)},$$

et par hypothèses sur γ_{k+1}, la tresse γ_{k+1} est la B_{n-1}^{+*}-fin de $\beta^{(k)}$. Toujours grâce au lemme 2.2, on établit (3.13) pour k. On a ainsi démontré que les tresses γ_k et β_k sont les mêmes pour tout k. En particulier on obtient la relation

$$\phi_n^{c-b-1}(\gamma_c) \cdot ... \cdot \phi_n(\gamma_{b+2}) \cdot \gamma_{b+1} = \beta^{(b)}. \tag{3.14}$$

Or par définition de b, la tresse $\beta^{(b)}$ est triviale, tandis que, par hypothèse, la tresse γ_c est non triviale. La relation (3.14) peut alors seulement être satisfaite pour $c = b$. □

Définition 2.8. La suite $(\beta_b, ..., \beta_1)$ de la proposition 2.7 est appelée le ϕ_n-*éclatement* de β. Sa longueur est appelée la n-*largeur* de β.

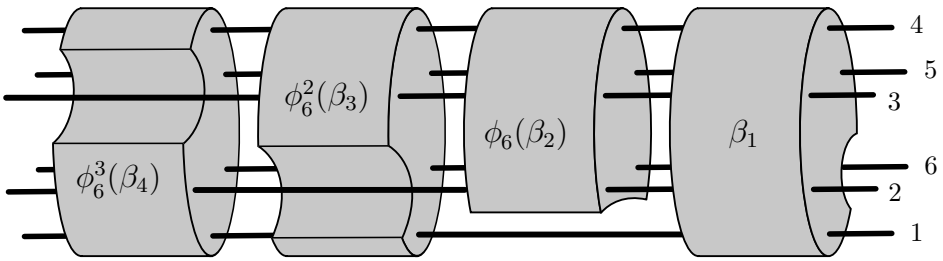


FIG. 3.5 : Le ϕ_6-éclatement d'une tresse de B_6^{+*}. Partant de la droite on extrait le plus grand diviseur à droite qui laisse le sixième brin invariant, puis on extrait le plus grand diviseur à droite de la tresse restante laissant le premier brin invariant, etc.

Pour reconnaître un ϕ_n-éclatement nous n'allons pas utiliser directement la condition (2.7.ii) mais une autre plus commode qui lui est équivalente.

Lemme 2.9. *La condition (2.7.ii) est équivalente à*

$$\textit{pour tout } k \geqslant 1, \textit{ la } B_{n-1}^{+*}\textit{-fin de } \phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1}) \textit{ est triviale.} \tag{3.15}$$

Démonstration. Pour tout $k \geqslant 1$, le lemme 2.2 implique que la B_{n-1}^{+*}-fin de la tresse

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

est β_k si et seulement si la B_{n-1}^{+*}-fin de la tresse

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

est triviale. Les conditions (2.7.ii) et (3.15) sont donc équivalentes. □

La notion de ϕ_n-éclatement étant fondamentale pour la suite, nous en donnons quelques exemples.

Exemple 2.10. Calculons le ϕ_n-éclatement des générateurs $a_{p,q}$ de B_n^{+*}. Pour $q \leqslant n-1$, la tresse $a_{p,q}$ appartient à B_{n-1}^{+*}, donc son ϕ_n-éclatement est $(a_{p,q})$. Comme $a_{p,n}$ n'est pas un élément de B_{n-1}^{+*}, le terme le plus à droite dans son éclatement est trivial. De plus, pour $p \geqslant 2$, on a $\phi_n^{-1}(a_{p,n}) = a_{p-1,n-1}$. Donc pour $p \geqslant 2$, le ϕ_n-éclatement de $a_{p,n}$ est la suite$(a_{p-1,n-1}, 1)$. Finalement, les tresses $a_{1,n}$ et $\phi_n^{-1}(a_{1,n})$, qui est égale à $a_{n-1,n}$, n'appartiennent pas à B_{n-1}^{+*}, mais la tresse $\phi_n^{-2}(a_{1,n})$, soit $a_{n-2,n-1}$, si. Donc le ϕ_n-éclatement de $a_{1,n}$ est la suite $(a_{n-2,n-1}, 1, 1)$. Pour résumer, le ϕ_n-éclatement de $a_{p,q}$ est

$$\begin{cases} (a_{p,q}) & \text{pour } p < q \leqslant n-1, \\ (a_{p-1,n-1}, 1) & \text{pour } 2 \leqslant p \text{ et } q = n, \\ (a_{n-2,n-1}, 1, 1) & \text{pour } p = 1 \text{ et } q = n. \end{cases}$$

Exemple 2.11. Calculons le ϕ_3-éclatement de la tresse δ_3^2. Avec les notations de la preuve de la proposition 2.7, on obtient

$$\begin{aligned} &\beta^{(0)} = \beta = (a_{1,2}\, a_{2,3})^2, && \beta_1 = \mathrm{fin}_2(\beta^{(0)}) = a_{1,2}^2, \\ &\beta^{(1)} = \phi_3^{-1}\big(\beta^{(0)}\beta_1^{-1}\big) = \phi_3^{-1}(a_{1,2}a_{1,3}) = a_{1,3}a_{2,3}, && \beta_2 = \mathrm{fin}_2(\beta^{(1)}) = 1, \\ &\beta^{(2)} = \phi_3^{-1}\big(\beta^{(1)}\beta_2^{-1}\big) = \phi_3^{-1}(a_{1,3}a_{2,3}) = a_{2,3}a_{1,2}, && \beta_3 = \mathrm{fin}_2(\beta^{(2)}) = a_{1,2}, \\ &\beta^{(3)} = \phi_3^{-1}\big(\beta^{(2)}\beta_3^{-1}\big) = \phi_3^{-1}(a_{2,3}) = a_{1,2}, && \beta_4 = \mathrm{fin}_2(\beta^{(3)}) = a_{1,2}, \\ &\beta^{(4)} = \phi_3^{-1}\big(\beta^{(3)}\beta_4^{-1}\big) = 1. \end{aligned}$$

et on arrête car le reste $\beta^{(4)}$ est trivial. Ainsi le ϕ_3-éclatement de δ_3^2 est la suite $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$.

À l'aide du ϕ_n-éclatement, nous allons maintenant construire une forme normale pour les éléments de B_n^{+*}. Le principe est le suivant. Tout d'abord, chaque tresse de B_2^{+*} est représentée par un unique mot de la forme $a_{1,2}^k$. Comme le ϕ_n-éclatement permet de faire correspondre de manière unique à toute tresse de B_n^{+*} une suite de tresses de B_{n-1}^{+*}, nous allons construire la forme normale tournante sur B_n^{+*} par induction sur $n \geqslant 2$.

Au lemme 2.1 on a montré que l'image d'une A_n^+-lettre par ϕ_n est une A_n^+-lettre. Nous définissons un homomorphisme d'A_n^+-mots, que l'on note aussi ϕ_n, qui envoie la lettre $a_{p,q}$ sur $a_{p+1,q+1}$ pour $q \leqslant n-1$ et $a_{p,n}$ sur $a_{1,p+1}$. Notons que si une tresse β de B_n^{+*} est représentée par un A_n^+-mot w alors la tresse $\phi_n(\beta)$ est représentée par le A_n^+-mot $\phi_n(w)$.

Définition 2.12.
- Pour β de B_2^{+*}, la *ϕ_2-forme normale tournante* de β est définie comme étant l'unique A_2^+-mot $a_{1,2}^k$ représentant β.
- Pour β de B_n^{+*} avec $n \geqslant 3$, la *ϕ_n-forme normale tournante* de β est définie comme étant le A_n^+-mot $\phi_n^{b-1}(w_b) \dots w_1$, où $(\beta_b, \dots, \beta_1)$ est le ϕ_n-éclatement de β et w_k est la ϕ_{n-1}-forme normale tournante de β_k pour tout k.

Comme le ϕ_n-éclatement d'une tresse β de B_{n-1}^{+*} est la suite (β) de longueur 1, la ϕ_n-forme normale tournante et la ϕ_{n-1}-forme normale tournante coïncident sur B_{n-1}^{+*}. Nous pouvons donc enlever l'indice n et parler de *forme normale tournante*, pour une tresse de B_n^{+*}. Naturellement, on dira qu'un mot est *tournant* s'il est la forme normale tournante de la tresse qu'il représente.

Exemple 2.13. Calculons la forme normale tournante de δ_4^2. D'abord, nous vérifions que nous avons la relation $\delta_4^2 = a_{1,2}\, a_{1,4}\, \delta_3^2$. Le ϕ_4-éclatement de β est donc $(a_{2,3}, a_{2,3}, 1, \delta_3^2)$. Le ϕ_3-éclatement de $a_{2,3}$ est la suite $(a_{1,2}, 1)$, et, donc, sa forme normale tournante est $\phi_3(a_{1,2})$, soit $a_{2,3}$. Ensuite, nous avons vu à l'exemple 2.11 que le ϕ_3-éclatement de δ_3^2 est la suite $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$. Donc, sa forme normale tournante est $\phi_3^3(a_{1,2}) \cdot \phi_3^2(a_{1,2}) \cdot \phi_3(1) \cdot a_{1,2}^2$, soit

$$a_{1,2} \cdot a_{1,3} \cdot \varepsilon \cdot a_{1,2} a_{1,2},$$

ou bien encore $a_{1,2}a_{1,3}a_{1,2}a_{1,2}$. Finalement, la forme normale tournante de δ_4^2 est

$$\phi_4^3(a_{2,3}) \cdot \phi_4^2(a_{2,3}) \cdot \phi_4(1) \cdot a_{1,2}\, a_{1,3}\, a_{1,2}\, a_{1,2},$$

soit $a_{1,2} \cdot a_{1,4} \cdot \varepsilon \cdot a_{1,2}a_{1,3}a_{1,2}a_{1,2}$, à savoir $a_{1,2}a_{1,4}a_{1,2}a_{1,3}a_{1,2}a_{1,2}$.

2.3 Algorithmes

Dans cette section nous décrivons des algorithmes nous permettant de calculer la forme normale tournante.

Nous commençons par un algorithme pour la divisibilité à droite.

Algorithme 3 (`DivDRet`)**.**

Entrée : Un triplet (n, w, u) où n est un entier et w et u des A_n^+-mots

1. `RetGauche(`n`,`wu^{-1}`)` $\rightarrow w'$`;`
2. `Si` w' est positif `faire`
3. `  Renvoyer` w'`;`
4. `Sinon faire`
5. `  Renvoyer` $\otimes$`;`

Sortie : Un A_n^+-mot ou $\otimes$

Proposition 2.14. *L'algorithme* `DivDRet` *appliqué à* (n, w, u) *retourne en temps* $O(C_n|w||u|)$*, où* C_n *ne dépend que de* n*, un mot* w' *vérifiant* $w \equiv w'u$ *si un tel mot existe ou le symbole erreur* $\otimes$ *sinon.*

Démonstration. Après la ligne 1, le mot w' est égal à $(u/w)^{-1} \cdot w/u$. Par le corollaire II.3.27 la tresse $\overline{u}$ est un diviseur à droite de $\overline{w}$ si et seulement si (u/w) est vide, c'est-à-dire si w' est un mot positif. La complexité en temps est une conséquence du corollaire II.3.26. □

L'algorithme `DivDRet` est l'algorithme qu'on utilise dans nos expérimentations sur ordinateur. Cependant nous ne connaissons pas une estimation fine de sa complexité en temps en fonction du nombre de brins n. Les récents travaux de M. Autord donnent une borne inférieure quartique dans le cas du monoïde de tresses positives B_n^+, voir [AD09]

À l'aide de la forme normale de Garside sur B_n^{+*} nous pouvons décrire un autre algorithme pour la divisibilité à droite :

Proposition 2.15. (D.B.A. Epstein et al, [ECH+92]) *Pour* w *et* u *des* A_n^+*-mots, on peut décider si la relation* $\overline{w} \succcurlyeq \overline{u}$ *est satisfaite en temps* $O(K\,|w||u|)$*, où* K *est la complexité en temps d'un algorithme calculant le pgcd de deux simples de* B_n^{+*}.

Une valeur possible de K introduite dans la proposition 2.15 est donnée par :

Proposition 2.16. (J.S. Birman, K.H. Ko, S.J. Lee, [BKL98]) *Il existe un algorithme calculant le pgcd de deux simples de* B_n^{+*} *en temps* $O(n)$.

L'algorithme construit à partir des propositions 2.15 et 2.16 est noté `DivD`, son entrée et sa sortie sont de même types que celles de l'algorithme `DivDRet`. De la même manière, il existe un algorithme `DivG` pour la division à gauche.

Comme conséquence des propositions 2.15 et 2.16, on obtient la complexité suivante pour les algorithmes `DivD` et `DivG`.

Corollaire 2.17. *L'algorithme* `DivD` *(*resp. `DivG`*) appliqué à* (n, w, u) *(*resp. *à* (n, u, w)*) renvoie en temps* $O(n \cdot |w|)$ *un mot* w' *vérifiant* $w \equiv w'u$ *(*resp. $w \equiv uw'$*) si un tel mot existe ou le symbole erreur* $\otimes$ *sinon.*

L'algorithme suivant calcule l'image d'un A_n^+-mot par l'homomorphisme de mot ϕ_n (envoyant $a_{p,q}$ pour $p \leqslant n-1$ et $a_{p,n}$ sur $a_{1,p+1}$). On rappelle que pour un mot w, $w(h)$ désigne la $h$ème lettre du mot w en partant de la gauche, la numérotation commençant à 1.

Algorithme 4 (`Phi`)**.**

Entrée : Un triplet (n, k, w) où n, k sont des entiers avec $0 \leqslant k \leqslant n$ et w un A_n^+-mot

1. $w \to w'$;
2. `Pour` $k = 1$ jusqu'à $|w|$ `faire`
3. $\quad w'[k] \to a_{p,q}$;
4. $\quad p + k \to p$; $q + k \to q$;
5. $\quad$ `Si` $p > n$ `faire` $p - n \to p$;
6. $\quad$ `Si` $q > n$ `faire` $q - n \to q$;
7. $\quad a_{p,q} \to w'[k]$;
8. `Renvoyer` w';

Sortie : Un A_n^+-mot

Proposition 2.18. *L'algorithme* `Phi` *appliqué à* (n, k, w) *renvoie en temps* $O(\log(n)|w|)$ *le* A_n^+*-mot* $\phi_n^k(w)$.

Démonstration. L'addition, la soustraction et la comparaison d'entiers compris entre 0 et n est en $O(\log(n))$. L'intérieur de la boucle `pour` est donc en $O(\log(n))$ et $|w|$ tours de boucle sont nécessaires. On obtient donc la complexité annoncée. □

De la définition du ϕ_n-éclatement, nous construisons l'algorithme suivant qui appliqué à un mot w renvoie une suite de A_{n-1}^+-mots $(w_b, \dots, w_1)$ telle que la suite de $(\overline{w}_b, \dots, \overline{w}_1)$ soit le ϕ_n-éclatement de la tresse $\overline{w}$.

Algorithme 5 (`Eclatement`)**.**
Entrée : Un couple (n, w) où n est un entier $\geqslant 3$ et w est un A_n^+-mot
1. $() \to s$; $w \to w'$; $0 \to k$;
2. `Tant que` w' `!=`ε `faire`
3. $\quad \varepsilon \to u$;
4. $\quad$ `Tant qu'il existe une` A_{n-1}-lettre x `avec DivD(`w'`,Phi(`n`,`k`,`x`)) !=`$\otimes$ `faire`
5. $\quad\quad$ `DivD(`w'`,Phi(`n`,`k`,`x`))` $\to w'$;
6. $\quad\quad$ $x \cdot u \to u$;
7. $\quad$ Insérer u à gauche dans s;
8. $\quad$ $k+1 \to k$;
9. $\quad$ `Si` $k = n$ `faire` $0 \to k$;
10. `Renvoyer` s;

Sortie : Une suite de A_{n-1}^+-mots

Proposition 2.19. *L'algorithme* `Eclatement` *appliqué à* (n, w) *retourne une suite* $(w_b, \dots, w_1)$ *en temps* $O(n^3 \cdot |w|^2)$ *telle que* $(\overline{w}_b, \dots, \overline{w}_1)$ *soit le* ϕ_n*-éclatement de* $\overline{w}$*.*

Démonstration. Les propriétés de la suite retournée sont une conséquence directe de la proposition 2.7. Chaque appel à `DivD` est en $O(n \cdot |w'|)$ avec $|w'| \leqslant |w|$. L'algorithme `Eclatement` nécessitant $O(\mathrm{card}(A_n^+) \cdot |w|)$ appels à `DivD`, on obtient le résultat. □

À partir de maintenant, si w est un mot tournant à n brins, l'unique suite de mots normaux tournant à $(n-1)$ brins $(w_b, \dots, w_1)$ telle que $(\overline{w_b}, \dots, \overline{w_1})$ soit le ϕ_n-éclatement de $\overline{w}$ est appelé ϕ_n*-éclatement* de w.

À l'aide de l'algorithme `eclatement` permettant de calculer le ϕ_n-éclatement d'une tresse de B_n^{+*}, nous construisons un algorithme renvoyant la forme normale tournante d'une tresse de B_n^{+*}. Le principe est celui donné à la définition 2.12.

Algorithme 6 (`FormeTournante`)**.**
Entrée : Un couple (n, w) où n est un entier ≥ 2 et w est un A_n^+-mot
1. `Si` $n = 2$ `faire Renvoyer` w;
2. `Eclatement(`n`,`w`)` $\to (w_b, \dots, w_1)$;
3. $\varepsilon \to w'$; $0 \to k'$;
4. `Pour` $k = 0$ `jusqu'à` b `faire`
5. $\quad$ `Phi(`n`,`k'`,FormeTournante(`$n-1$`,`w_k`))` $\cdot\, w' \to w'$;
6. $\quad$ $k' + 1 \to k'$;
7. $\quad$ `Si` $k' = n$ `faire` $0 \to k'$;
8. `Renvoyer` w';

Sortie : Un A_n^+-mot

Proposition 2.20. *L'algorithme* `FormeTournante` *appliqué à* (n, w) *retourne la forme normale tournante de* $\overline{w}$ *en temps* $O(n^4 \cdot |w|^2)$.

Démonstration. À la ligne 4, l'entier k' est égal à k modulo n. Le reste de l'algorithme est juste une adaptation de la définition 2.12.

Notons $C(n,\ell)$ la complexité en temps de l'algorithme `FormeTournante` appliqué à un A_n^+-mot w de longueur ℓ. Pour $n = 2$, la complexité $C(n,\ell)$ est constante. Pour $n \geqslant 3$, la complexité $C(n,\ell)$ est linéaire en

$$n^3\ell^2 + C(n-1,|w_1|) + ... + C(n-1,|w_b|),$$

avec $\ell = |w_1| + ... + |w_b|$. Comme $C(n,\ell)$ est au moins linéaire en ℓ, on obtient

$$C(n,\ell) \leqslant n^3\ell^2 + C(n-1,\ell).$$

Ainsi $C(n,\ell)$ appartient à $O(n^4|w|^2)$. □

Pour le moment, nous nous sommes seulement intéressés à calculer la forme normale tournante d'une tresse à partir d'un mot la représentant. Pour cela nous avons utilisé l'opération de ϕ_n-éclatement. Peut-on facilement retrouver le ϕ_n-éclatement d'une tresse à partir de sa forme normale tournante ? La réponse est donnée par le résultat suivant :

Lemme 2.21. *Supposons $n \geqslant 3$. Pour tout A_n-mot tournant w, le ϕ_n-éclatement de w peut être calculé en temps au plus $O(\log(n)\ell)$.*

Démonstration. Par définition de ϕ_n, un générateur $a_{p,q}$ appartient à $\phi_n^k(B_{n-1}^{+*})$ si et seulement si on a $p \neq k \mod n$ et $q \neq k \mod n$. Ainsi, étant donné un A_n-mot tournant w, on peut directement lire le ϕ_n-éclatement $(w_b, ..., w_1)$ de w. En effet, lisant w à partir de la droite, w_1 est le suffixe maximal de w qui est un A_{n-1}-mot, puis $\phi_n(w_2)$ est le suffixe maximal du mot restant qui est l'image d'un A_{n-1}-mot par ϕ_n, etc, jusqu'à obtenir le mot vide. □

Exemple 2.22. Considérons le mot tournant $w = a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}$ et calculons le ϕ_4-éclatement de w. En lisant w à partir de la droite, on trouve que le suffixe maximal de w ne contenant pas de lettre $a_{p,q}$ avec $p = 0 \mod n$ ou $q = 0 \mod n$ est $a_{2,3}\, a_{1,2}$. On a donc $w_1 = a_{2,3}\, a_{1,2}$. En répétant ce procédé, on trouve facilement que le ϕ_4-éclatement de w est

$$(\phi_4^{-3}(a_{1,2}),\ \phi_4^{-2}(a_{1,4}),\ \phi_4^{-1}(1),\ a_{2,3}\, a_{1,2}),$$

donc la suite $(a_{2,3}, a_{2,3}, 1, a_{2,3}\, a_{1,2})$.

3 Contraintes sur le ϕ_n-éclatement

L'opération de ϕ_n-éclatement associe à chaque tresse non triviale de B_n^{+*} une suite finie de tresses de B_{n-1}^{+*}. Maintenant, dans l'autre direction, toute suite finie de tresses de B_{n-1}^{+*} n'est pas le ϕ_n-éclatement d'une tresse de B_n^{+*}. Le but de cette section est d'établir certaines contraintes qui sont satisfaites par les termes d'un ϕ_n-éclatement. La contrainte principale étant qu'un ϕ_n-éclatement contient nécessairement ce que l'on appelle *une échelle*, qui correspond à une succession de lettres $a_{p,q}$ (pas forcément adjacentes) dont les indices q forment une suite croissante (les barreaux de l'échelle).

3.1 Dernières lettres

La première étape est de montrer que la dernière lettre de la forme normale tournante d'un terme d'un ϕ_n-éclatement doit respecter des contraintes en fonction de sa position.

Définition 3.1. Pour tout mot non vide w, la dernière lettre de w est notée par $w^{\#}$. De même, pour toute tresse non triviale β de B_n^{+*}, on définit la *dernière lettre* de β, notée $\beta^{\#}$, comme étant la dernière lettre de la forme normale tournante de β.

Lemme 3.2. *Supposons $n \geqslant 3$, et que $(\beta_b, \dots, \beta_1)$ soit un ϕ_n-éclatement.*
- *(i) Pour $k \geqslant 2$, la lettre $\beta_k^{\#}$ est $a_{p,n-1}$ pour un certain indice p, sauf si β_k est triviale.*
- *(ii) Pour $k \geqslant 3$, la tresse β_k est non triviale.*
- *(iii) Pour $k \geqslant 2$, si la forme normale tournante de β_k est $w\, a_{n-2,n-1}$ avec w un mot non vide, alors la lettre $w^{\#}$ est $a_{p,n-1}$ pour un certain indice p.*

Démonstration. (i) Supposons $k \geqslant 2$. Posons $a_{p,q} = \beta_k^{\#}$. Comme β_k est une tresse de B_{n-1}^{+*}, on a forcément $q \leqslant n-1$. Par (3.15), la B_{n-1}^{+*}-fin de

$$\phi_n^{b-k+1}(\beta_b) \cdot \dots \cdot \phi_n(\beta_k)$$

est triviale. En particulier, $\phi_n(\beta_k^{\#})$ ne peut pas appartenir à B_{n-1}^{+*}. Ainsi q doit être égal à $n-1$.

(ii) Supposons que β_c soit triviale avec $c \geqslant 3$ et que β_k soit non triviale pour tout k dans $\{b, \dots, c\}$. La définition d'un ϕ_n-éclatement implique que la tresse β_b est non triviale, c'est-à-dire, qu'on a $c \leqslant b-1$. Par définition de c, on a $\beta_{c+1} \neq 1$. Le point (i) montre alors que la dernière lettre de β_{c+1} est $a_{r,n-1}$ pour un certain indice r. La condition (3.15) implique que la B_{n-1}^{+*}-fin de la tresse

$$\phi_n^{b-c-1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{c+1})\, \phi_n(\beta_c)$$

est triviale. Ainsi, comme β_c est une tresse triviale, nous en déduisons que la B_{n-1}^{+*}-fin de

$$\phi_n^{b-c-1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{c+1})$$

est triviale. Ceci implique que la dernière lettre de $\phi_n^2(\beta_{c+1})$, qui est $\phi_n^2(a_{r,n-1})$, n'appartient pas à B_{n-1}^{+*}. Par la relation (3.6), la seule possibilité est $r = n-2$. On a donc $\phi_n^3(a_{r,n-1}) = a_{1,2}$. Par ailleurs, comme la forme normale tournante w_{c-1} de β_{c-1} est un A_{n-1}^+-mot, son image par ϕ_n ne contient pas de lettre $a_{1,q}$. Maintenant, les relations

$$a_{1,2}\, a_{p,q} \equiv \begin{cases} a_{p,q}\, a_{1,2} & \text{pour } 2 < p, \\ a_{1,q}\, a_{1,2} & \text{pour } 2 = p, \end{cases}$$

impliquent qu'il existe un A_n^+-mot w' satisfaisant $a_{1,2}\, \phi_n(w_{c-1}) \equiv w'\, a_{1,2}$. La tresse $a_{1,2}$ est alors un diviseur à droite de $\phi_n^3(\beta_{c+1}^{\#}) \cdot \phi_n(\beta_{c-1})$, puis de

$$\phi_n^3(\beta_{c+1}) \cdot \phi_n^2(\beta_c) \cdot \phi_n(\beta_{c-1}).$$

Comme par hypothèse on a $c-1 \geqslant 2$, ceci contredit (3.15).

(iii) Supposons que la forme normale tournante de β_k soit $w\, a_{n-2,n-1}$ avec $w \neq \varepsilon$. Soit $a_{p,q}$ la dernière lettre de w. Comme w est un A_n^+-mot on a $q \leqslant n-2$. Par ailleurs les relations

$$a_{p,q}\, a_{n-2,n-1} \equiv \begin{cases} a_{n-2,n-1}\, a_{p,q} & \text{for } q < n-2, \\ a_{p,n-1}\, a_{p,q} & \text{for } q = n-2, \end{cases} \tag{3.16}$$

impliquent l'égalité $q = n-1$. En effet, dans le cas contraire, $a_{p,q}$ serait un diviseur à droite de la tresse β_k, c'est-à-dire que la B_{n-1}^{+*}-fin de $\phi_n(\beta_k)$ serait non triviale, ce qui est en contradiction avec (3.15). □

3.2 Barrières

Si $(\beta_b, \dots, \beta_1)$ est le ϕ_n-éclatement d'une tresse de B_n^{+*}, alors le lemme 3.2 nous dit que, pour $k \geqslant 3$, la lettre $\beta_k^{\#}$ doit être une certaine lettre $a_{p-1,n-1}$. Nous allons maintenant montrer que la tresse β_{k-1} ne peut pas être n'importe quelle tresse de B_{n-1}^{+*} : sa forme normale tournante doit satisfaire certaines contraintes faisant intervenir l'entier p, à savoir contenir une lettre appelée $a_{p,n}$*-barrière*.

Définition 3.3. La lettre $a_{r,s}$ est appelée $a_{p,q}$*-barrière* si on a

$$1 \leqslant r < p < s < q \leqslant n \quad \text{ou} \quad 1 \leqslant p < r < q < s \leqslant n. \tag{3.17}$$

Par définition, si la lettre x est une $a_{p,q}$-barrière, alors dans la présentation de B_n^{+*} il n'existe pas de relation de la forme $a_{p,q} \cdot x = y \cdot a_{p,q}$ permettant de pousser la lettre $a_{p,q}$ à droite au travers de la lettre x : donc, en un sens, x agit comme une barrière.

En termes de diagrammes de cordes, $a_{r,p}$ est une $a_{p,q}$-barrière si et seulement si la corde associée à $a_{r,s}$ et la corde associée à $a_{p,q}$ ont un point d'intersection qui n'est pas une extrémité (voir figure 3.6).

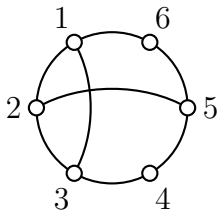


FIG. 3.6 : La lettre $a_{2,5}$ est une $a_{1,3}$ barrière car les cordes associées à $a_{2,5}$ et à $a_{1,3}$ ont un point d'intersection à l'intérieur du disque.

Nous allons maintenant prouver que presque tous les termes β_k d'un éclatement ont une forme normale tournante contenant nécessairement une barrière. La raison est simple : s'il n'y avait pas de barrière dans la forme normale tournante de β_k, alors les relations du monoïde de tresse dual nous permettraient de faire passer la dernière lettre de $\phi_n^2(\beta_{k+1})$ à travers $\phi_n(\beta_k)$ et l'insérer dans β_{k-1}, contredisant la définition d'un éclatement.

Lemme 3.4. *Supposons $n \geqslant 3$, que β soit une tresse de B_{n-1}^{+*} et que la B_{n-1}^{+*}-fin de $\phi_n(a_{p,n}\beta)$ soit triviale pour un certain $p \leqslant n-2$. Alors la forme normale tournante de β n'est pas le mot vide et contient une $a_{p,n}$-barrière.*

Démonstration. Supposons que la forme normale tournante w de β ne contienne pas de $a_{p,n}$-barrière et montrons alors qu'on a une contradiction. Soient w' le mot $a_{p,n}w$ et X l'ensemble de toutes les lettres $a_{q,r}$ avec $p < r \leqslant n-1$. Posons $w' = u\,v$ où v est le suffixe maximal de w écrit seulement avec des lettres de X. Par hypothèse, la B_{n-1}^{+*}-fin de $\overline{w'}$ est triviale. Ainsi le mot w' se termine par $a_{q,n-1}$ pour un certain indice q, c'est-à-dire que le mot v est non vide. Comme la première lettre de w' est $a_{p,n}$, qui n'appartient pas à l'ensemble X, le mot u est aussi non vide. Soit $a_{s,t}$ la dernière lettre de u. Par construction de u, la lettre $a_{s,t}$ est soit $a_{p,n}$ soit elle satisfait $t \leqslant p$. Dans les deux cas, notons que la tresse $\phi_n(a_{s,t})$ appartient à B_{n-1}^{+*}. Montrons maintenant que la tresse $a_{s,t}$ quasi-commute avec v, c'est-à-dire qu'il existe un mot v' satisfaisant $a_{s,t}v \equiv v'a_{s,t}$. Chaque lettre $a_{q,r}$ apparaissant dans v n'est pas une $a_{p,n}$-barrière, c'est–à-dire qu'elle vérifie la relation

$$p \leqslant q < r \leqslant n-1.$$

Donc, les relations

$$a_{s,t}a_{q,r} \equiv \begin{cases} a_{q,r}a_{s,t}, & \text{pour } p<q \text{ ou } t<p \qquad \text{par (II.2.2)},\\ a_{s,r}a_{s,t}, & \text{pour } q=t=p \qquad \text{par (II.2.3)},\\ a_{r,t}a_{s,t}, & \text{pour } a_{s,t}=a_{p,n} \text{ et } q=p \qquad \text{par (II.2.3)}, \end{cases}$$

impliquent que la lettre $a_{s,t}$ quasi-commute avec v. Ainsi, $\phi_n(a_{s,t})$ est un diviseur à droite de $\phi_n(a_{p,n}\,\beta)$. Ceci contredit l'hypothèse demandant que la B^{+*}_{n-1}-fin de $\phi_n(a_{p,n}\beta)$ soit triviale puisque que la tresse $\phi_n(a_{s,t})$ appartient à B^{+*}_{n-1}. □

Nous appliquons maintenant le lemme 3.4 dans le contexte d'un ϕ_n-éclatement.

Proposition 3.5. *Soit $(\beta_b, \dots, \beta_1)$ le ϕ_n-éclatement d'une tresse de B^{+*}_n avec $n \geqslant 3$. Alors, pour tout k dans $\{b-1, \dots, 2\}$ tel que $\beta^{\#}_{k+1}$ ne soit pas $a_{n-2,n-1}$, la forme normale tournante de β_k contient une $\phi_n(\beta^{\#}_{k+1})$-barrière.*

Démonstration. La condition (3.15) implique que la B^{+*}_{n-1}-fin de la tresse

$$\phi_n^{b-k+1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{k+1})\,\phi_n(\beta_k)$$

est triviale. En particulier, la B^{+*}_{n-1}-fin de $\phi_n^2(\beta^{\#}_{k+1})\,\phi_n(\beta_k)$ est triviale. Le lemme 3.4 implique alors que la forme normale tournante de β_k contient une $a_{p,n}$-barrière dès que $\beta^{\#}_k$ est différente de $a_{n-2,n-1}$. □

Exemple 3.6. Considérons la tresse β dont la forme normale tournante est

$$a_{2,4}\,a_{1,3}\,a_{4,5}\,a_{2,4}\,a_{2,4}\,a_{3,5}\,a_{4,5}.$$

Le ϕ_5-éclatement de β est $(\beta_4, \beta_3, \beta_2, \beta_1)$ avec

$$\beta_4 = a_{1,4}, \quad \beta_3 = a_{1,4}, \quad \beta_2 = a_{3,4}a_{1,3}a_{1,3}a_{2,4}a_{3,4} \quad \text{et} \quad \beta_1 = 1.$$

La lettre $\beta^{\#}_4$ est $a_{1,4}$, donc, par la proposition 3.5, la forme normale tournante de β_3 doit contenir une $a_{2,5}$-barrière : ceci est vrai puisque $a_{1,4}$ est une $a_{2,5}$-barrière. La lettre $\beta^{\#}_3$ est $a_{1,4}$, qui est différente de $a_{3,4}$. Alors, encore par la proposition 3.5, la forme normale tournante de β_2 doit contenir une $a_{2,5}$-barrière : ceci est vrai puisque la forme normale tournante de β_2 est $a_{3,4}a_{1,3}a_{1,3}a_{2,4}a_{3,4}$, qui contient la $a_{2,5}$-barrière $a_{1,3}$.

La proposition 3.5 implique que, dans un ϕ_n-éclatement, le terme à droite d'un terme se terminant par $a_{p,n-1}$ avec $p < n-2$ doit contenir une barrière. Ainsi, si un terme d'un ϕ_n-éclatement ne contient pas de barrière alors son terme de gauche se termine nécessairement par la lettre $a_{n-2,n-1}$.

Corollaire 3.7. *Supposons $n \geqslant 3$ et que $(\beta_b, \dots, \beta_1)$ est une suite d'éléments de B^{+*}_{n-1} qui est le ϕ_n-éclatement d'une certaine tresse de B^{+*}_n. Alors, pour tout c dans $\{b-1, \dots, 2\}$ tel que β_c est soit triviale soit $a_{n-1,n}$, on a $\beta^{\#}_{c+1} = a_{n-2,n-1}$.*

Démonstration. Supposons $\beta_c \in \{1, a_{n-2,n-1}\}$. Soit $a_{p-1,n-1}$ la dernière lettre de la forme normale tournante de β_{c+1}. La condition (3.15) implique que la B^{+*}_{n-1}-fin de $\phi_n^2(\beta_{c+1})\phi_n(\beta_c)$ est triviale. En particulier la B^{+*}_{n-1}-fin de $\phi_n(a_{p,n}\,\beta_c)$ est triviale. Ensuite, comme la forme normale tournante de β_c ne contient pas de barrière, la proposition 3.10 implique $p = n-1$. Nous avons donc $\beta^{\#}_{c+1} = a_{n-2,n-1}$. □

3.3 Échelles

Nous avons vu à la proposition 3.5 que tout mot tournant w de B^{+*}_{n-1} tel que la B^{+*}_{n-1}-fin de $\phi_n(a_{p,n}\,\overline{w})$ est triviale pour $p \leqslant n-2$ contient au moins une $a_{p,n}$-barrière. Nous allons maintenant montrer que, sous les mêmes hypothèses, w contient non seulement une barrière, mais une suite de barrières se recouvrant deux à deux. Les mots contenant une telle suite de lettres seront appelés échelles.

Définition 3.8. Pour $n \geqslant 3$, on dit qu'un A^+_{n-1}-mot w est une *$a_{p,n}$-échelle de hauteur h adossée à $a_{q-1,n-1}$*, s'il existe une décomposition

$$w = w_0\, x_1\, w_1 \,...\, w_{h-1}\, x_h\, w_h, \tag{3.18}$$

et une suite $p = f(0) < f(1) < ... < f(h) = n-1$ telle que
(i) pour tout $k \leqslant h$, la lettre x_k est une $a_{f(k-1),n}$-barrière de la forme $a_{..,f(k)}$,
(ii) pour tout $k < h$, le mot w_k ne contient pas de $a_{f(k),n}$-barrière,
(iii) la dernière lettre de w est $a_{q-1,n-1}$.

Par convention, tout A^+_{n-1}-mot dont la dernière lettre est $a_{q-1,n-1}$ est une $a_{n-1,n}$-échelle adossée à $a_{q-1,n-1}$ et sa hauteur est 0. Il n'existe pas de $a_{p,n}$-barrière avec $n \leqslant 3$, donc parmi les A^+_3-mots il n'existe que des $a_{1,2}$-échelles.

La notion d'échelle est facilement illustrée en représentant les générateurs $a_{p,q}$ comme des lignes verticales reliant la p-ème ligne à la q-ème ligne sur une partition à n lignes. De cette manière, pour tout $k \geqslant 0$, la lettre x_k ressemble au barreau d'une échelle—voir Figure 3.7.

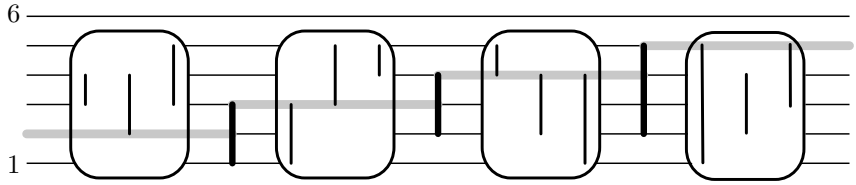


FIG. 3.7 : Une $a_{2,5}$-échelle adossée à $a_{3,5}$ (la dernière lettre). La ligne grise part de la position 2 pour grimper jusqu'à la position 5 en utilisant les barreaux de l'échelle. Les barreaux de l'échelle sont représentés par des lignes noires verticales plus épaisses. Les espaces entre les barreaux de l'échelle sont représentés par une boîte. Dans une telle boîte, les lignes verticales représentant une lettre $a_{i,j}$ ne coupent pas la ligne grise.

Notre but est de démontrer que la forme normale tournante d'un terme non terminal d'un ϕ_n-éclatement est une échelle. Pour ceci, nous commençons par un lemme préparatoire montrant que des barrières apparaissent forcément après certaines lettres dans une forme normale tournante. En appliquant ce résultat autant de fois qu'il le faut, on obtiendra la description d'une échelle.

Lemme 3.9. *Supposons $n \geqslant 4$, que w est le suffixe d'un A^+_{n-1}-mot tournant, que $a_{p,q}$ appartienne à B^{+*}_{n-2}, et que la B^{+*}_{n-1}-fin de $\phi_n(a_{p,q}\overline{w})$ soit triviale. Alors le mot w contient une $a_{q,n}$-barrière.*

Démonstration. Notons X l'ensemble des lettres $a_{r,s}$ avec $s > q$. Posons $w = u\,v$ où v est le suffixe maximal de w écrit avec seulement des lettres de X. Comme, par hypothèse, la B^{+*}_{n-1}-fin de $\phi_n(a_{p,q}\overline{w})$ est triviale, la dernière lettre de w existe et est de la forme $a_{..,n-1}$; en particulier le mot v est non vide.

Comme la lettre $a_{p,q}$ n'appartient pas à X, le mot u est aussi non vide. Notons $a_{t,t'}$ la dernière lettre de u. Par définition de u, on a $t' \leqslant q$. Supposons que v ne contienne pas de $a_{q,n}$-barrière, c'est-à-dire que toute lettre $a_{r,s}$ de v satisfasse $r \geqslant q$, et montrons alors qu'on a une contradiction. Par (II.2.2) et (II.2.3), nous avons

$$a_{t,t'}\, a_{r,s} \equiv \begin{cases} a_{r,s} a_{t,t'} & \text{pour } r > q \text{ ou } t' < q, \\ a_{t,s} a_{t,t'} & \text{pour } q = r = t', \end{cases}$$

ce qui implique que les mots $a_{t,t'}$ et v quasi-commutent, c'est-à-dire qu'il existe un A_n^+-mot v' satisfaisant la relation $a_{t,t'}\, v \equiv v'\, a_{t,t'}$. Ainsi $\phi_n(a_{t,t'})$ est un diviseur à droite de la tresse représentée par le mot $\phi_n(a_{p,q}w)$. L'hypothèse portant sur $a_{p,q}$ et la relation $t' \leqslant q$ impliquent que $\phi_n(a_{t,t'})$ est un élément de B_{n-1}^{+*}, ce qui contredit l'hypothèse faite sur la trivialité de la B_{n-1}^{+*}-fin de la tresse $\phi_n(a_{p,q}\, \overline{w})$. □

Nous pouvons maintenant montrer que tout mot normal satisfaisant quelques conditions additionnelles est une échelle.

Proposition 3.10. *Supposons $n \geqslant 3$, que β appartienne à B_{n-1}^{+*}, que la B_{n-1}^{+*}-fin de β soit triviale et que la forme normale tournante de β contienne une $a_{p,n}$-barrière. Alors la forme normale tournante de β est une $a_{p,n}$-échelle adossée à $\beta^{\#}$.*

Démonstration. Posons $f(1) = p$ et notons par w la forme normale tournante de β. Par hypothèse w admet la décomposition $w_0\, x_1\, w^{(0)}$, où w_0 est le préfixe maximal de w qui ne contient pas de $a_{p,n}$-barrière et où $x_1 = a_{..,f(1)}$ est une $a_{p,n}$-barrière. Comme par hypothèse, la B_{n-1}^{+*}-fin de $\overline{w}$ est triviale, il en est de même pour la B_{n-1}^{+*}-fin de $\phi_n(x_1\, \overline{w}^{(0)})$. Supposons que $f(1)$ soit différent de $n-1$. Le lemme 3.9 implique alors que le mot $w^{(0)}$ admet la décomposition $w_1\, x_2\, w^{(1)}$, où w_1 est le préfixe maximal de $w^{(0)}$ qui ne contient pas de $a_{f(1),n}$-barrière et où x_2 est une $a_{f(1),n}$-barrière. Nous répétons le même argument jusqu'à obtenir la décomposition

$$w_0\, x_1\, w_1 \ldots\, x_h w^{(h)}$$

de w avec $f(h) = n-1$. Ainsi, en posant $w_h = w^{(h)}$, nous avons montré que la forme normale tournante de β satisfait les conditions de la définition 3.8, en d'autres mots, c'est une échelle. □

En appliquant la proposition 3.10 aux entrées successives d'un ϕ_n-éclatement, on déduit que tous ses termes, exceptés les extrêmes, sont des échelles.

Corollaire 3.11. *Supposons $n \geqslant 3$ et que $(\beta_b, \ldots, \beta_1)$ soit une suite d'éléments de B_{n-1}^{+*} qui est le ϕ_n-éclatement d'une certaine tresse de B_n^{+*}. Alors, pour tout k dans $\{b-1, \ldots, 2\}$, la forme normale tournante de β_k est une $\phi_n(\beta_{k+1}^{\#})$-échelle adossée à $\beta_k^{\#}$.*

Démonstration. La condition (3.15) implique que la B_{n-1}^{+*}-fin de la tresse $\phi_n^2(\beta_{k+1})\phi_n(\beta_k)$ est triviale. En particulier, les B_{n-1}^{+*}-fins de $\phi_n^2(\beta_{k+1}^{\#})\phi_n(\beta_k)$ et $\phi_n(\beta_k)$ sont triviales. Par le lemme 3.2, la lettre $\beta_{k+1}^{\#}$ est de la forme $a_{..,n-1}$. La proposition 3.5 garantit que la forme normale tournante de β_k contient une $\phi_n(\beta_{k+1}^{\#})$-barrière. Ainsi la proposition 3.10 implique que la forme normale tournante de β_k est une $\phi_n(\beta_{k+1}^{\#})$-échelle adossée à $\beta_k^{\#}$. □

Par définition d'une échelle, comme la lettre $a_{n-2,n-1}$ n'est pas une barrière, si $w\, a_{n-2,n-1}$ est une $a_{p,n}$-échelle et si w n'est pas le mot vide, alors w est une $a_{p,n}$-échelle adossée à $a_{r-1,n-1}$ pour un certain entier r—voir lemme 3.2 (iii).

Exemple 3.12. Reprenons la tresse de l'exemple 3.6. Son ϕ_4-éclatement est $(\beta_4, ..., \beta_1)$ avec

$$\beta_4 = a_{1,4}, \quad \beta_3 = a_{1,4}, \quad \beta_2 = a_{3,4}a_{1,3}a_{1,3}a_{2,4}a_{3,4} \quad \text{et} \quad \beta_1 = 1.$$

La forme normale tournante de β_4 se termine par $a_{1,4}$; la forme normale tournante de β_3 doit alors être une $a_{2,5}$-échelle adossée à $a_{1,4}$. Ceci est vrai : dans ce cas précis l'échelle est $\varepsilon \cdot a_{1,4} \cdot \varepsilon$, et sa hauteur est 1, ce qui, avec les notations de la définition 3.8, correspond à $w_0 = \varepsilon$, $x_1 = a_{1,4}$ et $w_1 = \varepsilon$. De même, la forme normale tournante de β_3 se termine par $a_{1,4}$, donc par le corollaire 3.11, la forme normale tournante de β_2 doit être une $a_{2,5}$-échelle adossée à $a_{3,4}$. Ceci est encore vrai. Dans ce cas, l'échelle a pour hauteur 2, et sa décomposition est $a_{3,4} \cdot a_{1,3} \cdot a_{1,3} \cdot a_{2,4} \cdot a_{3,4}$, qui, avec les notations de la définition 3.8, correspond à $w_0 = a_{3,4}$, $x_1 = a_{1,3}$, $w_1 = a_{1,3}$, $x_2 = a_{2,4}$ et $w_2 = a_{3,4}$. Nous observons que $a_{1,3}$ est une $a_{2,5}$-barrière et que $a_{2,4}$ est une $a_{3,5}$-barrière.

4 Forme normale tournante et automates

Dans cette section, nous allons donner une construction inductive d'automates permettant de reconnaître la famille des mots tournants.

Dans [Deh08], P. Dehornoy montre que l'ensemble des mots qui sont des formes normales alternantes peut être reconnu par un automate. Cependant, la méthode utilisée ne permet pas d'expliciter des automates compréhensibles sauf pour $n = 3$.

4.1 Reconnaître un mot tournant

Nous avons établi plusieurs contraintes que devaient satisfaire les ϕ_n-éclatements et les mots tournants : dernière lettre, contenir une barrière, etc. Dans cette section, nous montrons que ces contraintes sont suffisantes.

Pour cela nous avons besoin d'énoncés techniques préliminaires.

Lemme 4.1. *Soit β une tresse non triviale de B_n^{+*} dont la B_{n-1}^{+*}-fin est triviale. Alors tout A_n^+-mot représentant β se termine par $\beta^\#$, qui vaut $a_{p,n}$ pour un certain p.*

Démonstration. Soit w un A_n^+-mot représentant β. Comme la B_{n-1}^{+*}-fin de β est triviale, le mot w se termine par $a_{p,n}$ pour un certain p. Soit w' un autre A_n^+-mot représentant β. Pour la même raison que w, le mot w' se termine par $a_{q,n}$ pour un certain q. La tresse est donc un multiple à gauche de $a_{p,n}$ et $a_{q,n}$. Supposons sans perte de généralité $p \leqslant q$. Pour $p \neq q$, le ppcm à gauche de $a_{p,n}$ et $a_{q,n}$ est $a_{p,q}a_{q,n}$. Par la relation II.2.3, le mot $a_{p,q}a_{q,n}$ est équivalent à $a_{p,n}a_{p,q}$. Ainsi, la relation $p \neq q$ implique que β est divisible à droite par $a_{p,q}$, qui est un élément de B_{n-1}^{+*}. On a obtenu une contradiction et on a $p = q$. Comme la forme normale tournante de β est un représentant particulier de β, on a $a_{p,n} = \beta^\#$, où, on le rappelle, $\beta^\#$ est la dernière lettre de la forme normale tournante de β. □

Le résultat précédent rend la définition de la dernière lettre d'une tresse (définition 3.1) plus naturelle.

Lemme 4.2. *Pour β une tresse de B_{n-1}^{+*}, il y a équivalence entre*
- *(i) un A_{n-1}^+-mot représentant β contient une $a_{p,n}$-barrière ;*
- *(ii) tout A_{n-1}^+-mot représentant β contient une $a_{p,n}$-barrière.*

Démonstration. La relation $(ii) \Leftarrow (i)$ est évidente. Montrons que (i) implique (ii). Cela revient à montrer que si $u = v$ est une relation de II.2.13 avec u contenant une $a_{p,n}$-barrière alors le mot v en contient aussi une. Pour la relation II.2.2 c'est évident car elle préserve les lettres. Pour la relation II.2.3, la propriété est immédiate si on considère des diagrammes de cordes.

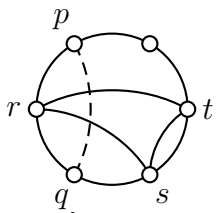


FIG. 3.8 : La relation (2.3) préserve les $a_{p,q}$-barrières : si un des membres de $a_{r,s}a_{s,t} = a_{s,t}a_{r,t} = a_{r,t}a_{r,s}$ contient une $a_{p,q}$-barrière alors les deux autres aussi.

□

Ainsi contenir une barrière n'est pas une propriété de mot mais est une propriété de tresse. On dit qu'une tresse de B_n^{+*} *contient une* $a_{p,q}$*-barrière* si elle est représentée par un mot contenant une $a_{p,q}$-barrière.

Lemme 4.3. *Soient β une tresse de B_{n-1}^{+*} et p un entier vérifiant $2 \leqslant p \leqslant n-1$. Alors 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.*
– (iii) *tout A_n^+-mot représentant $a_{p,n}\beta$ se termine par $\beta^{\#}$.*

Démonstration. L'implication $(i) \Rightarrow (ii)$ est le lemme 3.4. Montrons que (ii) implique (iii). Pour cela déterminons quels sont les générateurs $a_{r,s}$ divisant à droite $a_{p,n}\beta$. Soit w un A_{n-1}^+-mot représentant β. D'après le corollaire II.3.27, pour deux A_n^+-mots u et v, la tresse $\overline{v}$ est un diviseur à droite de $\overline{u}$ si et seulement si v/u est le mot vide. Déterminons alors pour quelle valeur de r et s, le mot $a_{r,s}/(a_{p,n}w)$ est vide. Supposons $s \leqslant n-1$ avec $a_{r,s} \neq \beta^{\#}$. La tresse β n'étant pas divisible à droite par $a_{r,s}$ d'après le lemme 4.1, le mot $a_{r,s}/w$ est non vide. Comme le retournement d'un A_{n-1}-mot est un A_{n-1}-mot il existe alors w' et $a_{t,t'}$ avec $t' \leqslant n-1$ vérifiant

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

La tresse $a_{t,t'}$ n'étant évidemment pas un diviseur à droite de $a_{p,n}$, le mot $a_{r,s}$ ne divise pas la tresse $a_{p,n}\overline{w}$ pour $s \leqslant n-1$.

Supposons $s = n$. Par hypothèse un représentant de β contient une $a_{p,n}$-barrière. Ainsi par le lemme 4.2, la forme normale tournante de β contient une $a_{p,n}$-barrière. La proposition 3.10 assure donc que la forme normale tournante est une $a_{p,n}$-échelle. Une première étape consiste à maîtriser le retournement à gauche de $a_{i,j}a_{t,n}^{-1}$ pour $j \leqslant n-1$:

$$f_g^n(a_{i,j}, a_{t,n}) = \begin{cases} a_{t,n} & \text{pour } [i,j] \text{ et } [t,n] \text{ nichés ou disjoints,} \\ a_{i,n} & \text{pour } j = t, \\ a_{t,n} & \text{pour } i = t, \\ a_{t,j}a_{i,n} & \text{pour } i < t < j. \end{cases} \tag{3.19}$$

Notons $u_1, ..., u_\ell$ une suite de retournements à gauche de $a_{p,n}wa_{s,n}^{-1}$. Notons x_k^{-1} la lettre négative la plus à droite dans u_k. Comme le retournement à gauche consiste à remplacer un sous-mot de

la forme xy^{-1} par $f_g^n(x,y)^{-1}f_g^n(y,x)$, la relation (3.19) implique que x_k est de la forme $a_{r_k,n}$. Par la relation (3.19) on a $r_{k+1} \leqslant r_k$ pour tout k. De plus si u_k commence par le mot $v\, a_{i,j} a_{r_k,n}^{-1}$ avec $i < r_k \leqslant j$ alors l'entier r_{k+1} vaut i. Donc d'une certaine manière la valeur r_k descend les barres de l'échelle w. Il s'ensuit que le mot $a_{p,n}\, w\, a_{s,n}^{-1}$ se retourne à gauche en $a_{p,n}a_{r_\ell,n}^{-1}w'$ pour un certain w' avec $r_\ell < p$. On déduit alors que le mot $a_{r,s}/(a_{p,n}w)$ est non vide. Nous venons donc d'établir que la seule A_n^+-lettre qui divise à droite $a_{p,n}\beta$ est $\beta^\#$.

Montrons que (iii) implique (i). Posons $a_{q-1,n-1} = \beta_k^\#$. Comme la seule A_n^+-lettre qui divise à droite $\phi_n(a_{p,n}\beta)$ est $a_{q,n}$, la B_{n-1}^{+*}-fin de $\phi_n(a_{p,n})$ est triviale. □

Théorème 4.4. *Une suite finie $(\beta_b, \dots, \beta_1)$ de tresses de B_{n-1}^{+*} est le ϕ_n-éclatement d'une tresse de B_n^{+*} si et seulement si*

– *(i) pour $k \geqslant 3$ et $k = b$, 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 $k \geqslant 3$, on a $\beta_k^\# \neq a_{n-2,n-1}$ alors β_{k-1} contient une $\phi_n(\beta_k^\#)$-barrière.*

Démonstration. Soit $(\beta_b, \dots, \beta_1)$ un ϕ_n-éclatement d'une tresse de B_n^{+*}. Le (i) est une conséquence du lemme 3.2 (i) et de la proposition 2.7. La condition 3.15 implique que la B_{n-1}^{+*}-fin de la tresse

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

est triviale pour tout $k \geqslant 1$. En particulier la B_{n-1}^{+*}-fin de $\phi_n(\beta_k)$ est triviale pour $k \geqslant 2$, c'est-à-dire que la condition (ii) est vérifiée. Le (iii) est une conséquence de la proposition 3.5.

Montrons maintenant qu'une suite $(\beta_b, \dots, \beta_1)$ satisfaisant les conditions (i), (ii) et (iii) est un ϕ_n-éclatement de B_n^{+*}. La condition (i) implique que β_b est non triviale. Pour $k \geqslant 3$, montrons

$$\text{la seule } A_n^+\text{-lettre divisant à droite } \phi_n^{b-k+1}(\beta_b) \cdot \dots \cdot \phi_n(\beta_k) \text{ est } \phi_n(\beta_k^\#). \tag{3.20}$$

Notons que la condition (i) assure l'existence de $\beta_k^\#$ pour $k \geqslant 3$. Pour $k = b$, la condition (ii) implique que la B_{n-1}^{+*}-fin de $\phi_n(\beta_k)$ est triviale. Par le lemme 4.1, la seule A_n^+-lettre qui divise à droite $\phi_n(\beta_k)$ est $\phi_n(\beta_k^\#)$. La relation (3.20) est donc vérifiée pour $k = b$. Supposons que (3.20) soit satisfaite pour $k+1$ et montrons la pour k. Soit $a_{p,q}$ une A_n^+-lettre différente de $\phi_n(\beta_k^\#)$. Notons w un représentant de $\phi_n^{b-k+1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{k+1})$. Par hypothèse, le mot w se termine par la lettre $\phi_n^2(\beta_{k+1}^\#)$. Notons u le préfixe de w de longueur $|w| - 1$. De même notons v un représentant de la tresse β_k. Montrons que le retournement à gauche de $u\phi_n^2(\beta_{k+1}^\#)\phi_n(v)\phi_n(a_{p,q}^{-1})$ commence par une lettre négative. Par le lemme 4.3 et la condition (iii), la seule A_n^+-lettre qui divise à droite $\phi_n(\beta_{k+1}^\#\beta_k)$ est $\phi_n(\beta_k^\#)$. Ainsi, par le corollaire II.3.27, il existe une A_n^+-lettre $a_{r,s}$ et un A_n-mot v' tels que le mot $va_{p,q}^{-1}$ se retourne à gauche en $a_{r,s}^{-1}v'$. On a donc

$$u\, \phi_n^2(\beta_{k+1}^\#)\, v\, a_{p,q}^{-1} \curvearrowright_g u\, \phi_n^2(\beta_{k+1}^\#)\, a_{r,t}^{-1}\, v'.$$

Comme la lettre $\beta_k^\#$ est de la forme $a_{..,n-1}$, la lettre $\phi_n^2(\beta_k^\#)$ est de la forme $a_{1,..}$. On en déduit que les lettres $\phi_n^2(\beta_k^\#)$ et $\phi_n(a_{r,s})$ sont différentes. La seule A_n-lettre divisant à droite la tresse

$$\phi_n^{b-k+1}(\beta_b) \cdot \dots \cdot \phi_n^2(\beta_{k+1})$$

étant $\phi_n^2(\beta_{k+1}^\#)$, par le corollaire II.3.27, il existe une A_n^+-lettre $a_{t,t'}$ et un A_n-mot u vérifiant

$$u\, \phi_n^2(\beta_{k+1}^\#)\, \phi_n(a_{r,s}^{-1}) \curvearrowright_g a_{t,t'}^{-1}\, u'.$$

On a donc montré que le retournement à gauche de $u\phi_n^2(\beta_{k+1}^{\#})va_{p,q}^{-1}$ donne $a_{t,t'}^{-1}u'v'$. Ainsi, par le corollaire II.3.27, la tresse $a_{p,q}$ n'est pas un diviseur à droite de $\phi_n^{b-k+1}(\beta_b)\cdot\ldots\cdot\phi_n(\beta_k)$, ce qui établit (3.20) pour k.

Une conséquence de (3.20) et de la condition (ii) est que la B_{n-1}^{+*}-fin de

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

est triviale pour $k\geqslant 3$. De même pour $k=2$ sauf si β_2 est triviale.

Afin d'établir la condition 3.15, il nous reste à montrer que la B_{n-1}^{+*}-fin de $\phi_n^{b-2}(\beta_b)\cdot\ldots\cdot\phi_n(\beta_2)$ est triviale pour $\beta_2=1$, c'est à dire que la B_{n-1}^{+*}-fin de $\phi_n^{b-2}(\beta_b)\cdot\ldots\cdot\phi_n^2(\beta_3)$ est triviale. Pour β_2 triviale, la condition (iii) implique que la dernière lettre de β_3 est $a_{n-2,n-1}$. Par (3.20) pour $k=3$, la seule A_n^+-lettre divisant à droite $\phi_n^{b-2}(\beta_b)\cdot\ldots\cdot\phi_n^2(\beta_3)$ est $\phi_n^2(a_{n-2,n-1})$, à savoir la tresse $a_{1,n}$. Ainsi tout diviseur à droite non trivial de $\phi_n^{b-2}(\beta_b)\cdot\ldots\cdot\phi_n^2(\beta_3)$ est un multiple à gauche de $a_{1,n}$, ceci impliquant que la B_{n-1}^{+*}-fin de $\phi_n^{b-2}(\beta_b)\cdot\ldots\cdot\phi_n^2(\beta_3)$ est triviale. □

Les conditions du théorème 4.4 sont faciles à vérifier si les tresses $\beta_b,\ldots,\beta_1$ sont données par leurs formes normales tournantes :

Corollaire 4.5. *Soit $(w_b,\ldots,w_1)$ une suite de A_{n-1}^+-mots. Alors le A_n^+-mot*

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

est tournant si et seulement si les conditions suivantes sont vérifiées.

- *(i) pour $k\geqslant 1$, le mot w_k est tournant,*
- *(ii) pour $k\geqslant 3$, le mot w_k se termine par $a_{p-1,n-1}$ pour un certain p,*
- *(iii) le mot w_2 est soit vide (sauf pour b=2), soit se termine par $a_{p-1,n-1}$ pour un certain p,*
- *(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. La condition (i) du théorème 4.4 est une conséquence immédiate des conditions (ii) et (iii). Les conditions (i) et (ii) impliquent que la B_{n-2}^{+*}-fin de la tresse w_k est triviale. Notons $a_{p-1,n-1}$ la dernière lettre de w_k, c'est-à-dire, $a_{p-1,n-1}=\overline{w}_k^{\#}$. Le lemme 4.1 implique que la seule A_{n-1}^+-lettre divisant à droite $\overline{w}_k$ est $a_{p-1,n-1}$. Comme $\overline{w}_k$ est un élément de B_{n-1}^{+*}, la seule A_n^+-lettre qui divise à droite $\overline{w}_k$ est $a_{p-1,n-1}$. Ainsi la seule lettre divisant à droite $\phi_n(\overline{w}_k)$ est $a_{p,n}$. Il s'ensuit que la B_{n-1}^{+*}-fin de $\overline{w}_k$ est triviale, c'est-à-dire, que la condition (ii) du théorème 4.4 est vérifiée. La condition (iii) du théorème 4.4 est une conséquence immédiate des points (ii) et (iv). On conclut à l'aide de la définition 2.12 et de (i). □

Nous avons ainsi obtenu une caractérisation inductive des mots tournants.

4.2 Automates et langage régulier

Dans cette section nous faisons de brefs rappels sur les automates et les langages réguliers. Toutes les définitions et tous les résultats de cette sous-section sont issus de [ECH+92].

Définition 4.6. Un *langage* sur un alphabet $\mathcal{S}$ est un sous-ensemble de $\mathcal{S}^*$, c'est-à-dire, des $\mathcal{S}$-mots.

Il est usuel de classifier des langages en fonction des types de machines capable de les reconnaître. Un *automate fini* est une machine simple permettant de reconnaître certains langages.

Définition 4.7. Un *automate fini* est un quintuplet $(E, \mathcal{S}, t, Q, i)$, où E est un ensemble fini *d'états*, $\mathcal{S}$ est un *alphabet* fini, $t : E \times \mathcal{S} \to E$ est une fonction de *transition*, Q est le sous-ensemble de E des *états terminaux* et i est l'état initial.

L'idée est que l'automate commence à l'état initial i, et lit un ruban sur lequel un $\mathcal{S}$-mot est imprimé. Après avoir lu une lettre, l'état de l'automate change, en fonction de l'état dans lequel il se trouve, de la lettre lue et de la fonction de transition t. Alors le ruban est décalé d'une lettre vers la droite, c'est-à-dire, la tête de lecture est décalée d'une lettre vers la gauche. Si après avoir lu tout le ruban l'automate se trouve dans un état terminal, on dit que la mot écrit sur le ruban est *reconnu* par l'automate.

Définition 4.8. L'ensemble des $\mathcal{S}$-mots reconnus par un automate fini est un langage dit *régulier* sur $\mathcal{S}$.

On représente souvent un automate à l'aide d'un graphe orienté, avec un noeud pour chaque état et une flèche étiquetée par une lettre de $\mathcal{S}$ pour chaque transition. Par convention, un état terminal est représenté par ◯ et l'état initial est représenté par ⟶◯ . Voir la figure 3.9 pour un exemple.

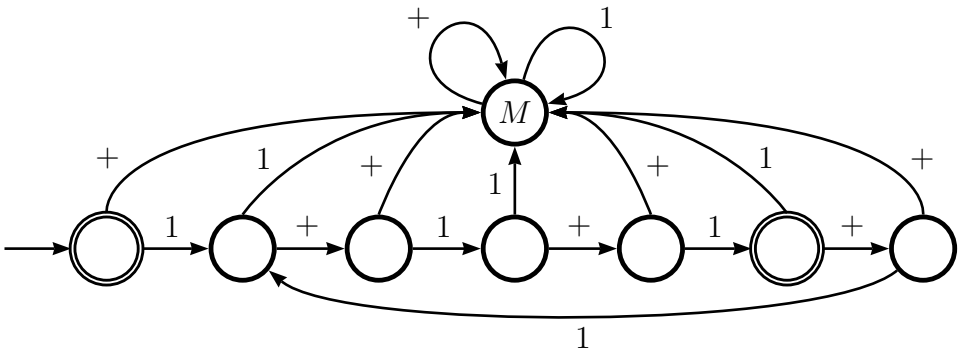


FIG. 3.9 : Un automate fini sur l'alphabet $\mathcal{S} = \{+, 1\}$. Le mot vide est interprété comme représentant 0 et est reconnu. Les autres mots reconnus sont ceux de la forme $1 + 1 + 1 + ... + 1$ à condition qu'il représente 0 modulo 3.

Étant donné un automate fini, on peut quelque fois le simplifier sans modifier le langage qu'il reconnaît. On peut supprimer tous les états *inaccessibles*, c'est-à-dire, ceux qui ne peuvent pas être atteint à partir de l'état initial. Ensuite, on peut regrouper tous les états *morts* en un seul ; un état est dit *mort* s'il est accessible, non terminale et si on ne peut pas en sortir, c'est-à-dire, les seules flèches partant d'un état mort pointent vers lui-même. Par exemple l'état étiqueté M dans l'automate de la figure 3.9 est un état mort.

Dans la suite, afin d'alléger les automates, on ne dessinera pas les états morts. Si à partir de l'état courant il n'existe pas de flèche étiquetée x sortant de l'état courant, alors si x est lu on se retrouve dans l'état mort et le mot sur le ruban de l'automate n'est pas reconnu.

Par exemple l'automate de la figure 3.9 devient :

Avec notre convention de lecture, un automate lit un mot de la droite vers la gauche. Dans la littérature, et en particulier dans [ECH$^+$92], les automates lisent les mots de la gauche vers la droite. Nous avons choisi cette convention car c'est la plus commode pour décrire les langages

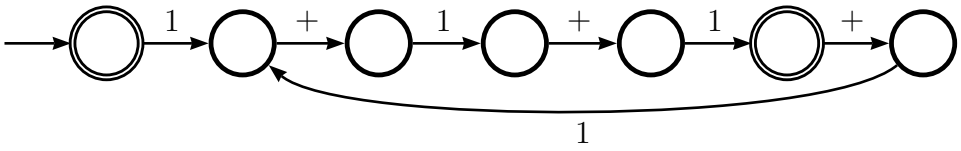


FIG. 3.10 : Automate de la figure 3.9 auquel on a retiré l'état mort M.

de la section suivantes Cependant, notons que ces conventions n'ont aucune importance du point de vue langage régulier. En effet, on a le résultat suivant liant un langage régulier L et le langage des mots de L écrits à l'envers :

Théorème 4.9. *Si L est un langage régulier sur un alphabet $\mathcal{S}$, alors le langage contenant les mots de L écrit à l'envers est aussi un langage régulier.*

4.3 Cas des mots tournants

Dans cette section nous décrivons la construction, par induction sur n, d'un automate reconnaissant le langage des mots tournants à n brins.

Notation 4.10. Notons T_n le langage sur A_n^+ des mots tournants à n brins.

Commençons d'abord par $n = 2$. Toute puissance de $a_{1,2}$ étant un mot tournant à 2 brins, l'automate suivant reconnaît le langage T_2.

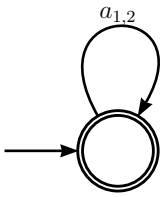


FIG. 3.11 : Automate reconnaissant le langage T_2 des mots tournants à 2 brins.

Intéressons nous maintenant au cas $n = 3$. Une conséquence du corollaire 4.5 est la caractérisation suivante des mots tournants à 3 brins.

Proposition 4.11. *Un A_3^+-mot $a_{[b]}^{e_b} \cdot \ldots \cdot a_{1,3}^{e_3} a_{2,3}^{e_2} a_{1,2}^{e_1}$ est tournant si et seulement si e_k est non nul pour $k \geqslant 3$, où on pose*

$$a_{[k]} = \begin{cases} a_{1,2} & \textit{pour } k = 1 \mod 3, \\ a_{2,3} & \textit{pour } k = 2 \mod 3, \\ a_{1,3} & \textit{pour } k = 3 \mod 3. \end{cases}$$

Démonstration. Les mots tournants à deux brins sont les puissances de $a_{1,2}$. Posons $w_k = a_{1,2}^{e_k}$. Le mot $w = a_{[b]}^{e_b} \cdot \ldots \cdot a_{1,3}^{e_3} a_{2,3}^{e_2} a_{1,2}^{e_1}$ est alors égal à

$$\phi_3^{b-1}(w_k) \cdot \ldots \cdot \phi_3^2(w_3) \cdot \phi_3(w_2) \cdot w_1.$$

Comme il n'existe pas de barrière dans B_3^{+*}, le mot w est tournant si et seulement siil vérifie les conditions (ii) et (iii) du corollaire 4.5, ce qui revient à $e_k \neq 0$ pour $k \geqslant 3$. □

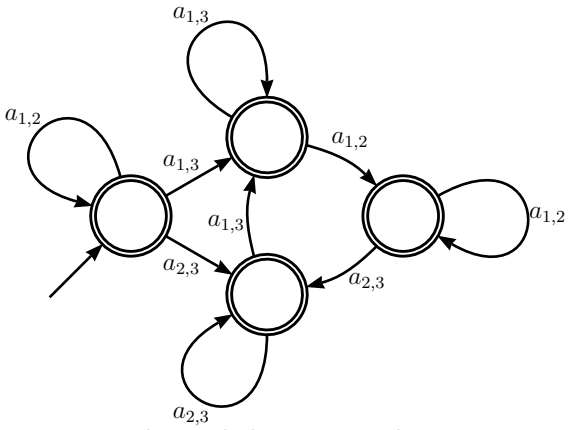


FIG. 3.12 : Automate reconnaissant le langage T_3 des mots tournants à 3 brins.

À l'aide de la proposition 4.11, on vérifie aisément que l'automate donné à la figure 3.12 reconnaît les mots tournants à 3 brins.

Malheureusement, pour $n \geqslant 4$, il n'existe pas de caractérisation des mots tournants à n brins aussi élémentaire que celle donnée à la proposition 4.11 dans le cas $n = 3$. Afin de construire un automate reconnaissant le langage T_n, nous allons utiliser la caractérisation des mots tournants à n brins donnée au corollaire 4.5 ainsi qu'une induction sur n.

La première étape consiste à construire un automate $\mathcal{A}_n$ reconnaissant les A_n^+-mots tournants se terminant par une lettre $a_{p,n}$ pour un certain p.

Notation 4.12. Notons $T_n^{\geqslant 2}$ l'ensemble des mots w de T_n se terminant par une lettre $a_{p,n}$ pour un certain p.

Remarquons que les mots de $T_n^{\geqslant 2}$ sont des A_{n-1}^+-mots tournants dont le ϕ_n-éclatement est de la forme $(w_b, \dots, w_2, 1)$, d'où la notation.

Afin de décrire facilement le processus d'induction il est utile de bien nommer les états de l'automate $\mathcal{A}_n^{\geqslant 2}$ reconnaissant le langage $T_n^{\geqslant 2}$.

Définition 4.13. On note F_n l'ensemble des couples (p, m) où p est un $(n-2)$-uplet $(p_n, \dots, p_3)$ avec p_i dans $\{0, \dots, i-1\}$ et m est un sous-ensemble de $\{a_{1,n}, a_{2,n}, \dots, a_{n-2,n}\}$. Pour $e = (p, m)$ un élément de F_n, on note $e(0)$ le $(n-2)$-uplet p et $e(1)$ l'ensemble m. De même on note $e(0, i)$ l'entier p_i.

Cette manière de noter les états semble étrange dans un premier temps. Précisons le fonctionnement du premier paramètre.

Définition 4.14. Pour e un élément de F_n, on note $\alpha_n(e)$ la A_n^+-lettre

$$\phi_n^{e(0,n)}(\phi_{n-1}^{e(0,n-1)}(\dots(\phi_4^{e(0,4)}(\phi_3^{e(0,3)}(a_{1,2})))\dots)).$$

L'idée est que pour arriver à un état e de F_n la dernière lettre lue par l'automate doit être $\alpha(e)$.

Afin de maintenir un procédé d'induction, nous n'allons pas seulement construire un automate

$$\mathcal{A}_k^{\geqslant 2} = (E_k^{\geqslant 2}, \mathcal{S}_k^{\geqslant 2}, t_k^{\geqslant 2}, Q_k^{\geqslant 2}, i_k^{\geqslant 2}),$$

reconnaissant le langage mais un automate ayant les propriétés suivantes :

Propriétés 4.15.
– $\mathcal{A}_k^{\geqslant 2}$ reconnaît $T_k^{\geqslant 2}$, (4.15.i)
– on a $\mathcal{S}_k^{\geqslant 2} = A_k^+$ et $\{*, M\} \subseteq E_k^{\geqslant 2} \subseteq F_k \cup \{*, M\}$, (4.15.ii)
– M est l'état mort de $\mathcal{A}_k^{\geqslant 2}$ et $*$ son état initial, c'est-à-dire, $i_k^{\geqslant 2} = *$, (4.15.iii)
– toutes les transitions sont de la forme $t_k^{\geqslant 2}(e, x) = M$ ou $t_k(e, \alpha_k(e')) = e'$, (4.15.iv)
– tout état différent de M de $\mathcal{A}_k^{\geqslant 2}$ est terminal, c'est-à-dire, $Q_k^{\geqslant 2} = E_k^{\geqslant 2} - \{M\}$. (4.15.v)

L'étape initiale de la construction inductive peut être obtenue pour $n = 2$, mais il nous paraît plus judicieux de commencer directement à partir de l'automate $\mathcal{A}_3^{\geqslant 2}$ donné à la figure 3.13

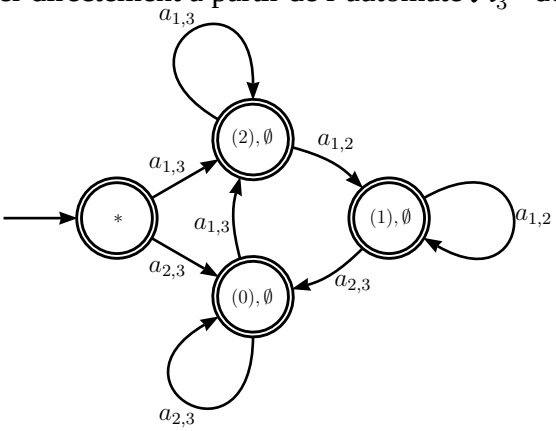


FIG. 3.13 : Automate $\mathcal{A}_3^{\geqslant 2}$ satisfaisant les propriétés 4.15.

Proposition 4.16. *L'automate $\mathcal{A}_3^{\geqslant 2}$ de la figure 3.13 satisfait les propriétés 4.15.*

Démonstration. L'automate de la figure 3.12 reconnaît le langage T_3. Remarquons que l'automate $\mathcal{A}_3^{\geqslant 2}$ est obtenu de ce dernier en retirant la boucle étiquetée $a_{1,2}$ basée sur l'état initial. Ainsi tout mot reconnu par $\mathcal{A}_3^{\geqslant 2}$ est tournant et ne se termine pas par la lettre $a_{1,2}$. La condition 4.15.i est donc vérifiée. Les autres propriétés de 4.15 se vérifient directement à l'aide de la figure 3.13. □

Pour la suite, on suppose que l'automate $\mathcal{A}_{n-1}^{\geqslant 2}$ est construit et satisfait les propriétés 4.15. Notre but est de décrire la construction de l'automate $\mathcal{A}_n^{\geqslant 2}$ à partir de $\mathcal{A}_{n-1}^{\geqslant 2}$. Comme cette construction est assez technique, nous allons illustrer les différentes étapes pour $n = 4$.

Pour satisfaire la condition (iv) du corollaire 4.5, nous devons modifier l'automate $\mathcal{A}_{n-1}^{\geqslant 2}$ afin qu'il « mémorise » la lecture d'une $a_{p,n}$-barrière pour différentes valeurs de p, c'est le rôle de l'ensemble m décrivant les états de F_n.

Notation 4.17. Pour e un état de F_n et p un entier de $\{1, \dots, n-2\}$, on note $e \cup \{a_{p,n}\}$ l'état de F_n égal à $(e(0), e(1) \cup \{a_{p,n}\})$.

Définition 4.18. Soit $\mathcal{A} = (E, A_{n-1}^+, t, Q, \{*\})$ un automate satisfaisant $E \subseteq F_n \cup \{*, M\}$ et tel que la lettre $a_{p,n}$ n'appartienne pas à $e(1)$ pour tout e de E. On définit $\mathcal{A}(a_{p,n})$ comme étant l'automate $(E', \mathcal{S}', t', Q', \{*\})$ avec $\mathcal{S}' = \mathcal{S}$,

$$E' = E \cup \{e \cup \{a_{p,n}\}, e \in E - \{*, M\}\},\ Q \cup \{e \cup \{a_{p,n}\}, e \in Q - \{*\}\},$$

et où la fonction de transition $t'(e, x)$ est définie par

$$t'(e,x) = \begin{cases} t(e,x) & \text{pour } e \in E \text{ et } x \text{ pas une } a_{p,n}\text{-barrière}, \\ t(e,x) \cup \{a_{p,n}\} & \text{pour } e \in E \text{ et } x \text{ une } a_{p,n}\text{-barrière}, \\ (t(e',x) \cup \{a_{p,n}\} & \text{pour } e = e' \cup \{a_{p,n}\} \text{ avec } e \in E. \end{cases}$$

Proposition 4.19. *Soient $\mathcal{A}$ un automate et p un entier comme dans la définition 4.18. Alors l'automate $\mathcal{A}(a_{p,n})$ reconnaît le même langage que $\mathcal{A}$. De plus si après avoir lu un A_{n-1}^+-mot l'automate $\mathcal{A}(a_{p,n})$ est dans l'état e alors le mot w contient une $a_{p,n}$-barrière si et seulement si la lettre $a_{p,n}$ appartient à $e(1)$.*

Démonstration. Soit w un A_n^+-mot de longueur ℓ. Notons e_k (*resp.* (e'_k)) l'état dans lequel se trouve $\mathcal{A}$ (*resp.* $\mathcal{A}(a_{p,n})$) après avoir lu la k ème lettre de w. Supposons que w ne contienne pas de $a_{p,n}$-barrière. La définition de t' implique qu'on a $e_k = e'_k$ pour tout k de $\{1, \dots, \ell\}$. Il s'ensuit que w est reconnu par $\mathcal{A}$ si et seulement s'il l'est par $\mathcal{A}(a_{p,n})$.

Supposons maintenant que w contienne une $a_{p,n}$-barrière. Soit ℓ' la longueur du préfixe maximale de w ne contenant pas de $a_{p,n}$-barrière. Par définition de t', on a $e'_k = e_k$ pour $1 \leqslant k \leqslant \ell'$ et $e'_k = e_k \cup \{a_{p,n}\}$ pour $k > \ell'$. Comme, par construction de Q', l'état e_ℓ appartient à Q si et seulement si $e'_\ell \cup \{a_{p,n}\}$ appartient à Q', le mot w est reconnu par l'automate $\mathcal{A}$ si et seulement s'il l'est par l'automate $\mathcal{A}(a_{p,n})$.

Comme, par hypothèse, tout élément e de E vérifie $a_{p,n} \notin e(1)$, l'automate $\mathcal{A}(a_{p,n})$ se trouve dans l'état e avec $a_{p,n}$ appartenant à e si et seulement si une $a_{p,n}$-barrière a déjà été lue (voir définition de t'). □

Exemple 4.20.

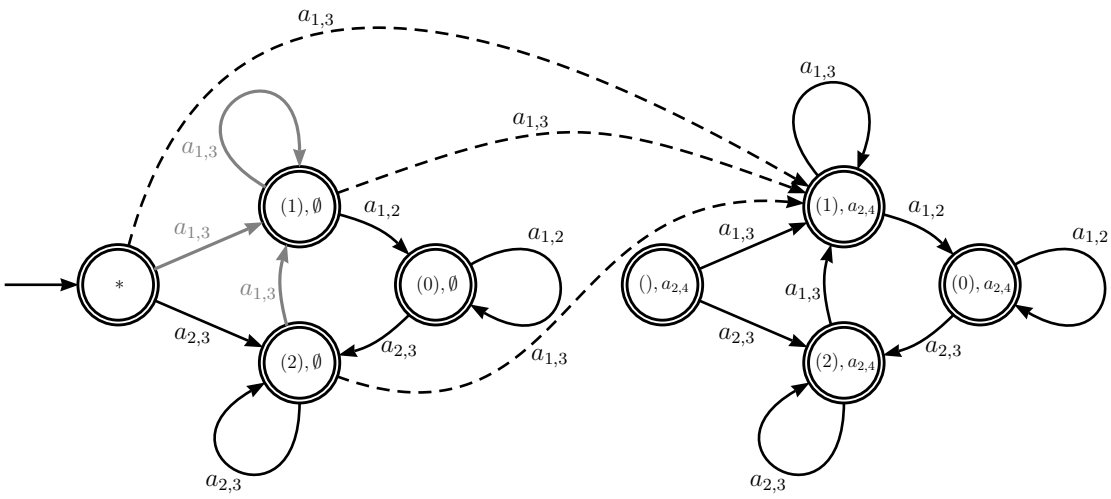


FIG. 3.14 : L'automate $\mathcal{A}_3^{\geqslant 2}(a_{2,4})$. Les transitions supprimées après la duplication de $\mathcal{A}_3^{\geqslant 2}$ sont grisées, celles rajoutées ensuite sont en tireté.

À la figure 3.14, on remarque que beaucoup d'états sont inaccessibles dans $\mathcal{A}_3^{\geqslant 2}(a_{2,4})$. En supprimant ces états, l'automate de la figure 3.14 devient celui de la figure 3.15

Définition 4.21. Pour $n \geqslant 4$, on note $\mathcal{A}_n^*$ l'automate $\mathcal{A}_{n-1}^{\geqslant 2}(a_{2,n})...(a_{n-2,n})$ duquel on a supprimer tous les états inaccessibles.

Une conséquence directe de la proposition 4.19 est :

Proposition 4.22. *L'automate $\mathcal{A}_n^*$ reconnaît le langage $T_{n-1}^{\geqslant 2}$ pour $k = n-1$. De plus si après avoir lu un mot w de $T_{n-1}^{\geqslant 2}$ l'automate est dans l'état e alors, pour $p \in \{1, \dots, n-2\}$, le mot w contient une $a_{p,n}$-barrière si et seulement si $a_{p,n}$ appartient à $e(1)$.*

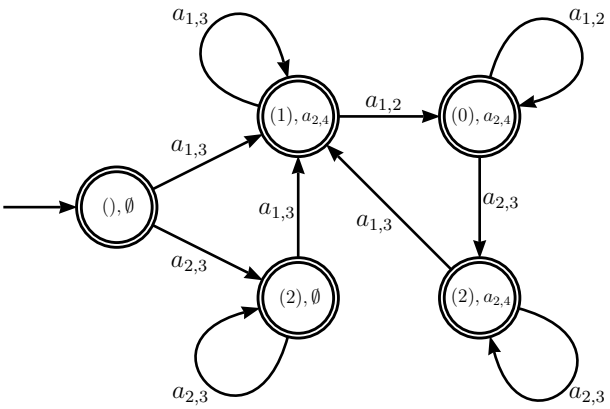


FIG. 3.15 : Simplification de l'automate $\mathcal{A}_3^{\geqslant 2}(a_{2,4})$ de la figure 3.14 : on a supprimé les états inaccessibles.

Pour continuer la construction, nous définissons ce que nous appelons un fragment d'automate.

Définition 4.23. Un *fragment d'automate* $\mathcal{A}$ est un quintuplet $(E, \mathcal{S}, t, Q, I)$, où E, $\mathcal{S}$, t et Q sont les mêmes que dans la définition 4.7 d'un automate fini et $I : \mathcal{S} \to E \cup \{M\}$ est la fonction *des entrées*. De plus on suppose que $*$ n'appartient pas à E et que M désigne l'état mort de $\mathcal{A}$. La *clôture* du fragment d'automate $\mathcal{A}$ est l'automate $(E \cup \{*\}, \mathcal{S}, t', Q, \{*\})$ avec

$$t'(e,x) = \begin{cases} t(e,x) & \text{pour } e \in E, \\ I(x) & \text{pour } e = *. \end{cases}$$

Notre construction de l'automate $\mathcal{A}_n^{\geqslant 2}$ fait intervenir n fragments d'automates notés $\mathcal{A}_n^k$ reliés entre eux. Intuitivement, le fragment $\mathcal{A}_n^k$ reconnaît les mots de la forme $\phi_n^t(w)$, où t est congru à k modulo n et w est un mot de $T_{n-1}^{\geqslant 2}$.

Définition 4.24. On définit un fragment d'automate $\mathcal{A}_n^0 = (E_n^0, A_{n-1}^+, t_n^0, Q_n^0, I_n^0)$ à partir de l'automate $\mathcal{A}_n^* = (E_n^*, A_{n-1}^+, t_n^*, Q_n^0, \{*\})$ en posant

$$E_n^0 = E_n^* - \{*\},\ Q_n^0 = Q_n^0 - \{*\},\ I_n^0 = \{t_n^*(*, x), x \in A_{n-1}^+\} - \{M\},$$

et où la fonction de transition t_n^0 est définie par

$$t_n^0(e,x) = \begin{cases} M & \text{pour } e = *, \\ t_n^*(e,x) & \text{sinon.} \end{cases}$$

Définition 4.25. Soit $e = (p, m)$ un état de F_{n-1}. Pour tout $k \geqslant 0$, on note $\phi_n^k(e)$ l'état de E_n égal à $((k, p_{n-1}, \ldots, p_3), \{\phi_n^k(x), x \in m\})$.

Notons, que, par définition, pour tout e de E_{n-1}, on a $\alpha_n(\phi_n^k(e)) = \phi_n^k(\alpha_{n-1}(e))$. Par convention, on pose $\phi_n^k(M) = M$ pour tout $k \geqslant 0$, où M est un état mort.

Définition 4.26. On définit le fragment d'automate $\mathcal{A}_n^k = (E_n^k, \phi_n^k(A_{n-1}^+), t_n^k, Q_n^k, I_n^k)$ à partir de l'automate $\mathcal{A}_n^0$ en posant

$$E_n^k = \phi_n^k(E_n^0),\ Q_n^k = \phi_n^k(Q_n^0),\ I_n^k = \phi_n^k(I_n^0),$$

et où la fonction de transition est définie par

$$t_n^k(\phi_n^k(e), \phi_n^k(x)) = \phi_n^k(t_n^0(e,x)).$$

Maintenant que nous avons les fragments d'automates $\mathcal{A}_n^k$ pour $k = 1, \dots, n$, il suffit de les relier pour obtenir l'automate $\mathcal{A}_n^{\geqslant 2}$. Le point est que l'on crée une transition reliant l'état e de $\mathcal{A}_n^k$ à l'état $I(e,x)$ de $\mathcal{A}_n^k$ si x appartient à $e(1)$.

Afin d'alléger la définition suivante, on pose $I_n^{n+1} = I_n^1$.

Définition 4.27. On définit $\mathcal{A}_n^{\geqslant 2}$ comme étant l'automate $(E_n^{\geqslant 2}, A_n^+, t_n^{\geqslant 2}, Q_n^{\geqslant 2}, \{*\})$ en posant

$$E_n^{\geqslant 2} = E_n^1 \cup \dots \cup E_n^n,\ Q_n^{\geqslant 2} = Q_n^1 \cup \dots \cup Q_n^n,$$

et où la fonction de transition $t_n^{\geqslant 2}$ est définie par

$$t_n^{\geqslant 2}(e,x) = \begin{cases} t_n^k(e,x) & \text{pour } e \in E_n^k \text{ et } x \in \phi_n^k(A_{n-1}^+), \\ I_n^{k+1}(x) & \text{pour } e \in E_n^k \text{ et } x \in \phi_n^{k+1}(A_{n-1}^+) - \phi_n^k(A_{n-1}^+), \\ I_n^1(x) & \text{pour } e = * \text{ et } x = a_{p,n} \text{ avec } p \neq 1, \\ I_n^2(a_{1,n}) & \text{pour } e = * \text{ et } x = a_{1,n}. \\ M & \text{sinon.} \end{cases}$$

Proposition 4.28. *L'automate $\mathcal{A}_n^{\geqslant 2}$ construit à la définition 4.27 satisfait les propriétés 4.15.*

Démonstration. Soit w un A_n^+-mot. Par construction, la clôture du fragment d'automate $\mathcal{A}_n^k$ reconnaît les mots de la forme $\phi_n^{k'}(w)$, pour k' congru à k modulo n, où w est un A_{n-1}-mot tournant se terminant par $a_{p,n}$ pour un certain p. Ainsi le mot w est reconnu par $\mathcal{A}_n^{\geqslant 2}$ si et seulement si w s'écrit

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

où les w_k sont des A_{n-1}^+-mots satisfaisant les conditions (i), (ii) et (iii) du corollaire 4.5. Par construction de $t_n^{\geqslant 2}$ et par la proposition 4.15, après avoir lu la lettre $w_k^\#$ pour $k \geqslant 3$, l'automate $\mathcal{A}_n^{\geqslant 2}$ n'est pas dans l'état mort si et seulement si le mot w_{k-1} contient une $w_k^\#$-barrière. La condition (iv) du corollaire 4.5 est donc satisfaite. Nous avons ainsi montré que l'automate $\mathcal{A}_n^{\geqslant 2}$ reconnaît le langage $T_n^{\geqslant 2}$. Les autres propriétés de 4.15 sont des conséquences directes de celles de $\mathcal{A}_{n-1}^{\geqslant 2}$ et de la construction des fragments d'automates $\mathcal{A}_n^k$. □

À partir de l'automate $\mathcal{A}_n^{\geqslant 2}$, nous pouvons construire, par induction, un automate $\mathcal{A}_n$ reconnaissant le langage T_n des mots tournants à n brins. Pour cela on insère l'automate $\mathcal{A}_{n-1}$ comme « préfixe » de l'automate $\mathcal{A}_n^{\geqslant 2}$.

Définition 4.29. Pour $n \geqslant 4$, on définit $\mathcal{A}_n$ à partir des automates

$$\mathcal{A}_{n-1} = (E_{n-1}, A_{n-1}^+, t_{n-1}, Q_{n-1}, \{*\}) \text{ et } \mathcal{A}_n^{\geqslant 2} = (E_n^{\geqslant 2}, A_n^+, t_n^{\geqslant 2}, Q_n^{\geqslant 2}, \{*\}),$$

comme étant l'automate $(E_n, A_n^+, t_n; Q_n, \{*\})$ avec

$$E_n = E_n^{\geqslant 2} \cup E_{n-1},\ Q_n = Q_n^{\geqslant 2} \cup Q_{n-1},$$

et où la fonction de transition t_n est définie par

$$t_n(e,x) = \begin{cases} t_n(e,x) & \text{pour } e \in E_n^{\geqslant 2}, \\ t_{n-1}(e,x) & \text{pour } e \in E_{n-1} \text{ et } x \in A_{n-1}^+, \\ I_n^1(x) & \text{pour } e \in E_{n-1} \text{ et } x = a_{p,n} \text{ avec } p \neq 1, \\ I_n^2(a_{1,n}) & \text{pour } e \in E_{n-1} \text{ et } x = a_{1,n} \text{ avec } p \neq 1. \end{cases}$$

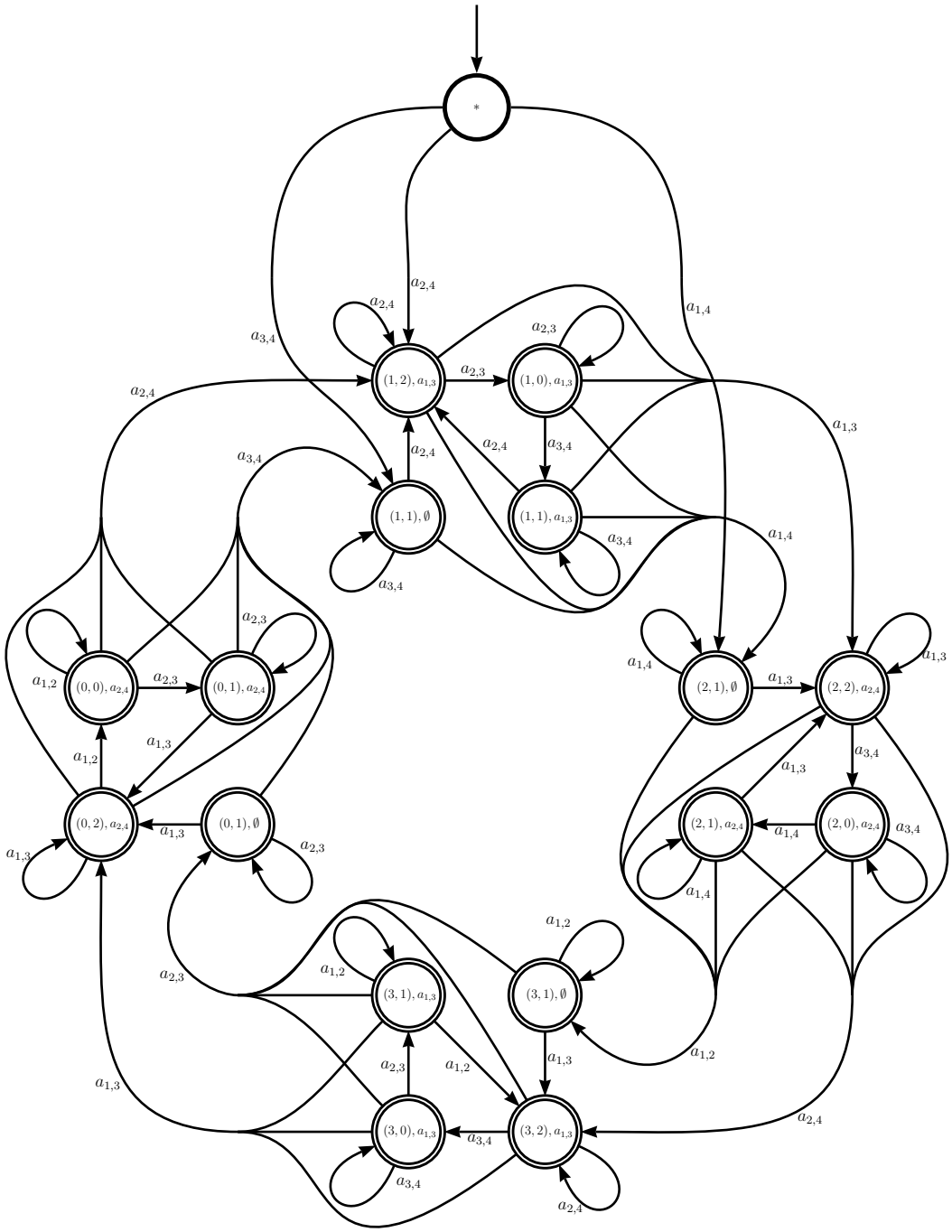


FIG. 3.16 : Automate $\mathcal{A}_4^{\geqslant 2}$ reconnaissant le langage $T_4^{\geqslant 2}$, c'est-à-dire, les mots tournants de A_4 se terminant par $a_{p,4}$ pour $p = 1, 2$ et 3. Sa construction nécessite l'utilisation des quatre fragments d'automate $\mathcal{A}_4^k$ pour $k = 1, 2, 3$ et 4.

Proposition 4.30. *Pour tout $n \geqslant 3$, l'automate $\mathcal{A}_n$ reconnaît le langage T_n.*

Démonstration. Soit w un A_n^+-mot. Notons w_1 le plus grand suffixe de w qui soit un A_{n-1}^+-mot et notons w' le préfixe associé. Comme le mot w_1 est reconnu par l'automate $\mathcal{A}_{n-1}$ si et seulement s'il est tournant, l'automate $\mathcal{A}_n$ se trouve dans un état différent de l'état mort M si et seulement si w_1 est tournant. Le mot w' est ensuite lu par la partie de l'automate $\mathcal{A}_n$ provenant de l'automate $\mathcal{A}_n^{\geqslant 2}$. Ainsi le mot w est reconnu par l'automate $\mathcal{A}_n$ si et seulement si w_1 est un mot tournant à $(n-1)$ brins et w' est le mot vide où un mot tournant à n brins se terminant par une lettre $a_{p,n}$ pour un certain p, c'est-à-dire, si et seulement si w est un mot tournant à n brins. □

Une des conséquences de ce résultat est que le langage T_n est régulier :

Corollaire 4.31. *Pour tout n, la famille des mots tournants à n brins est un langage régulier.*

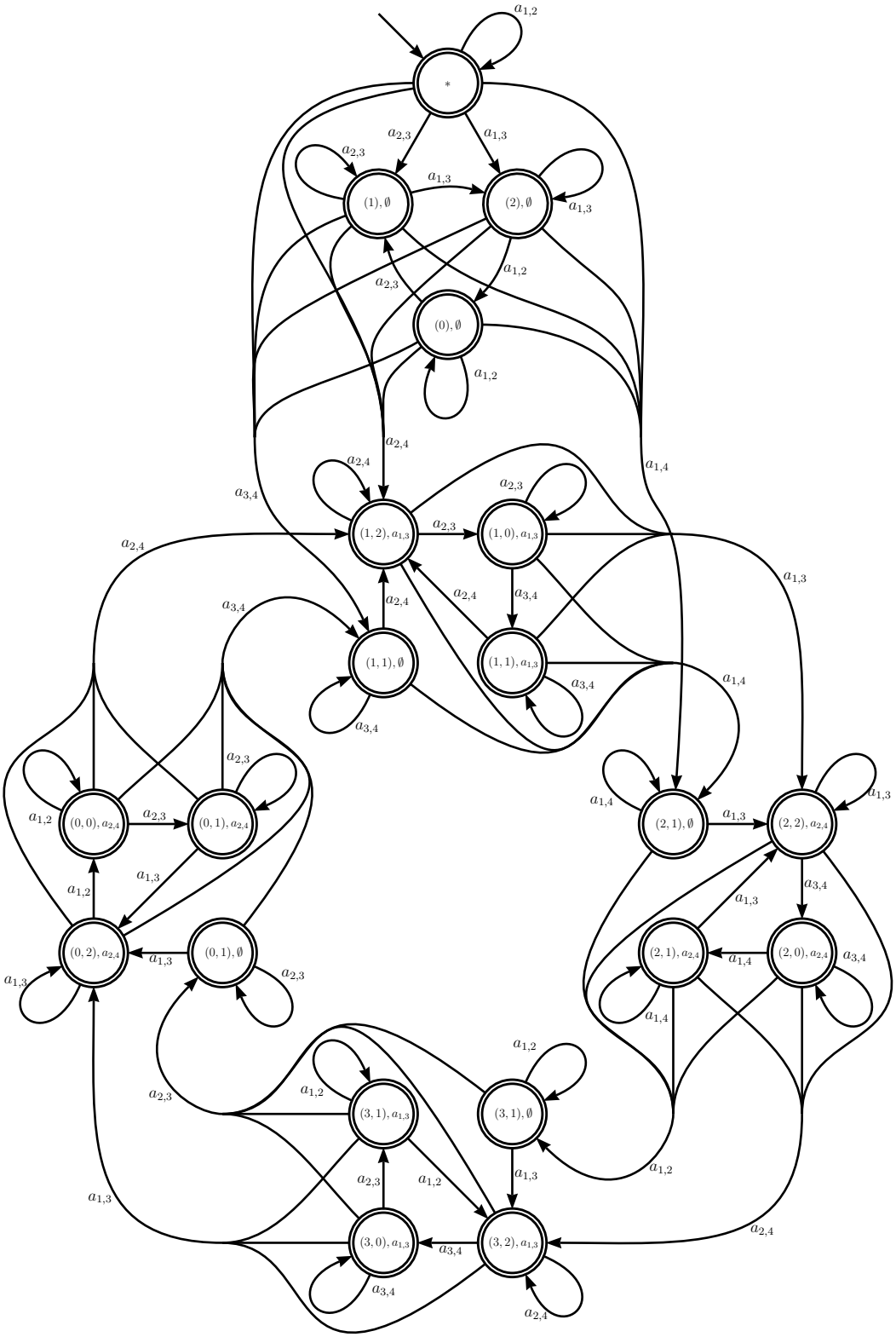


FIG. 3.17 : Automate A_4 reconnaissant le langage T_4.

IV. Expression σ-définie

Le point clé de l'existence de l'ordre des tresses est la propriété C, qui établit que toute tresse non triviale admet au moins une expression σ-définie, c'est-à-dire, une expression dans laquelle le générateur σ_i de plus grand indice i apparaît seulement positivement, ou seulement négativement. Indépendamment de toute considération d'ordre, cette propriété est un résultat fondamental des tresses.

Dans les vingt dernières années, au moins cinq ou six démonstrations d'approches différentes de ce résultat ont été proposées. La première, par P. Dehornoy en 1992, repose sur les algèbres auto-distributives [Deh94]. La suivante, par D. Larue [Lar94], utilise la représentation d'Artin des tresses comme automorphisme du groupe libre, un argument qui a été indépendamment redécouvert part R. Fenn, M. Greene, D. Rolfsen, C. Rourke et B. Wiest [FGR$^+$99] dans un langage topologique. Une démonstration complètement différente utilisant la géométrie du graphe de Cayley de B_n et la théorie de Garside apparaît dans [Deh97a]. Il existe aussi au moins deux démonstrations reposant sur des algorithmes de relaxation, qui sont des stratégies pour simplifier de proche en proche l'image d'une (famille de) courbe(s) dessinée dans un disque et déformée par l'action d'une tresse vue comme un homéomorphisme du disque. Une est décrite par I. Dynnikov et B. Wiest dans [DW07], une autre par X. Bressaud dans [Bre08].

Toutes ces méthodes sont effectives et donnent lieu à des algorithmes. Cependant, en termes de complexité en espace et en temps, aucune n'a une complexité meilleure qu'exponentielle. En particulier, la meilleure borne supérieure obtenue pour la longueur d'un mot σ-défini final équivalent à un mot de tresse initial de longueur ℓ est une exponentielle en ℓ. D'un autre côté, certaines méthodes sont connues comme extrêmement efficaces en pratique, et la conjecture suivante appartient au folklore du sujet :

Conjecture 0.1. *Pour tout n, il existe une constante C_n telle que, pour tout mot de tresse w à n brins de longueur ℓ, il existe un mot σ-défini équivalent de longueur au plus $C_n\ell$.*

Le but de ce chapitre est de démontrer la conjecture 0.1. Le principe de l'argument est le suivant. Etant donnée une tresse β de B_n, on commence d'abord par l'exprimer comme fraction $\delta_n^{-t}\,\beta'$, où, on le rappelle, δ_n est l'élément de Garside de B_n^{+*}, et où β' est un élément de B_n^{+*}. Ceci est possible car B_n est le groupe de fractions de B_n^{+*}. Si l'exposant t est plus grand que la longueur du ϕ_n-éclatement de β', alors le facteur σ-négatif δ_n^{-t} l'emporte sur le facteur σ-positif β et un mot σ-négatif représentant β peut être facilement obtenu par un calcul direct consistant essentiellement à intercaler un δ_n^{-1} entre les termes du ϕ_n-éclatement de β''. Sinon, si l'exposant t est plus petit que la longueur du ϕ_n éclatement de β', on détermine la forme normale tournante w de β' et on essaie d'obtenir un représentant σ-positif de β en poussant le facteur négatif δ_n^{-t} à droite au travers de w. Le problème est que certain mots σ-négatifs d'une forme particulière, appelés *mots dangereux*, apparaissent à chaque étape. Le point clé est que les mots tournants sont des échelles d'après la proposition III.3.10, ce qui nous permet de contrôler l'impact des mots dangereux. L'étape élémentaire de l'opération consiste à échanger un mot dangereux et un mot tournant. Pour cela nous définissons et utilisons un l'algorithme dit de renversement.

Le chapitre est organisé comme suit. Dans une première section nous définissons les mots dangereux et l'algorithme de renversement. À la section 2, nous montrons que l'algorithme de renversement appliqué à un mot consistant en un mot dangereux suivi d'une échelle renvoie un mot σ-nonnégatif équivalent. Nous démontrons la conjecture 0.1 à la section 3. Finalement à la section 4 nous décrivons un algorithme plus simple permettant d'obtenir des mots σ-définis quasis géodésiques.

1 Renversement

Le but de cette section est de décrire l'algorithme dit de *renversement*. Comme l'algorithme de retournement, il est défini sur des mots de tresses et consiste essentiellement au remplacement de sous-mots d'un certain type par un mot donné en fonction des règles de renversement. Néanmoins il nécessite l'introduction de nouveaux alphabets.

1.1 AD_n-mots

Jusqu'à maintenant, nous avons considéré des mots sur deux alphabets différents, à savoir l'alphabet Σ_n^+ des générateurs d'Artin σ_i et l'alphabet A_n des générateurs de Birman–Ko–Lee $a_{p,q}$. À partir de maintenant, nous allons utiliser un troisième alphabet correspondant aux tresses $d_{p,q}$ introduites à la section II.1.2.

Notation 1.1. Notons D_n l'ensemble $\{d_{p,q}^{\pm 1} \mid 1 \leqslant p < q \leqslant n\}$ et AD_n l'ensemble $D_n \sqcup A_n$.

Nous rappelons qu'un mot sur un alphabet S est appelé S-mot. Naturellement les A_n-mots et les D_n-mots sont des AD_n-mots particuliers. Ainsi, les notions définies sur les AD_n-mots (comme la σ-positivité, voir 1.2) seront également définies sur les A_n-mots et les D_n-mots. Nous utilisons la convention que le D_n-mot $d_{p,p}$ est le mot vide ε pour tout p.

Les AD_n-mots représentent naturellement des tresses de B_n et peuvent être traduits en Σ_n-mots. Il est cohérent avec la définition de $a_{p,q}$ et $d_{p,q}$ comme tresses (voir les définitions II.1.1 et II.1.5) de définir des mots $\underline{a}_{p,q}$ et $\underline{d}_{p,q}$ par

$$\underline{a}_{p,q} = \sigma_p \ldots \sigma_{q-2}\, \sigma_{q-1}\, \sigma_{q-2}^{-1} \ldots \sigma_p^{-1}, \quad \underline{d}_{p,q} = \sigma_p \ldots \sigma_{q-1}. \tag{4.1}$$

De cette manière, pour tout AD_n-mot w, la tresse représentée par w coïncide avec celle représentée par le Σ_n-mot $\underline{w}$ obtenu de w en remplaçant tout lettre $a_{p,q}$ par $\underline{a}_{p,q}$ et toute lettre $d_{p,q}$ par $\underline{d}_{p,q}$. Nous pensons qu'avec ces notations il ne devrait pas y avoir de difficulté à utiliser différents alphabets.

Nous redonnons maintenant la définition de Σ_n-mots σ-positifs et σ-négatifs et l'étendons aux AD_n-mots.

Définition 1.2.

- Un Σ_n-mot est dit σ_i-*positif* (*resp.* σ_i-*négatif*) s'il contient au moins une lettre σ_i, pas de lettre σ_i^{-1} (*resp.* au moins une lettre σ_i^{-1} et pas de lettre σ_i) et pas de lettre $\sigma_j^{\pm 1}$ pour $j > i$.
- Un Σ_n-mot est dit σ_i-*nonnégatif* s'il est σ_i-positif ou bien s'il ne contient pas de lettre $\sigma_j^{\pm 1}$ avec $j \geqslant i$.
- Un AD_n-mot est dit σ_i-*positif* (*resp.* σ_i-négatif, *resp.* σ_i-nonnégatif) si le Σ_n-mot $\underline{w}$ est σ_i-positif (*resp.* σ_i-négatif, *resp.* σ_i-nonnégatif).

Exemple 1.3. Un Σ_n-mot ne peut pas être à la fois σ_i-positif et σ_i-négatif, mais, d'un autre côté, un Σ_n-mot peut très bien n'être ni σ_i-positif ni σ_i-négatif pour tout i. Par exemple, $\sigma_2\sigma_1\sigma_2^{-1}$ n'est ni σ_2-positif (car il contient une lettre σ_2^{-1}), ni σ_2-négatif (car il contient une lettre σ_2), ni σ_1-positif ou σ_1-négatif (car il contient la lettre σ_2). Par contre, le mot $\sigma_1^{-1}\sigma_2\sigma_1$ qui lui est équivalent est σ_2-positif. Par ailleurs, le mot vide ε, σ_1^{-1}, et $\sigma_2\sigma_1^{-1}$ sont σ_2-nonnégatifs, car la lettre σ_2^{-1} n'y apparaît pas.

Exemple 1.4. Le A_n-mot $a_{2,3}^{-1}\, a_{1,3}$ n'est pas σ_2-positif, car sa translation par (4.1) est le Σ_n-mot $\sigma_2^{-1}\,\sigma_1\,\sigma_2\,\sigma_1^{-1}$, qui n'est pas σ_2-positif comme il contient la lettre σ_2^{-1}. Le mot $a_{2,3}^{-1}\, a_{1,3}$ est équivalent à $a_{1,3}\, a_{1,2}^{-1}$, qui se traduit en $\sigma_1\,\sigma_2\,\sigma_1^{-1}\,\sigma_1^{-1}$, un mot σ_2-positif. La tresse $a_{2,3}^{-1}\, a_{1,3}$ est donc σ_2-positive.

Une conséquence immédiate de la définition 1.2 est la caractérisation suivante des AD_n-mots σ_i-positifs.

Lemme 1.5. *Un AD_n-mot w est σ_i-positif si w contient au moins une lettre $a_{..,i+1}$ ou $d_{.,i+1}$ et pas de lettre $a_{..,i+1}^{-1}$, $d_{..,i+1}^{-1}$, $a_{..,j}^{\pm 1}$ ou $d_{..,j}^{\pm 1}$ avec $j > i+1$.*

Ce résultat nous permet de redéfinir une notion de AD_n-mot σ_i-positif sans passer par une traduction en termes de Σ_n-mots.

On arrive à la notion clé de cette section. Le problème est d'identifier une forme générique des fragments négatifs que nous devrons contrôler et, si possible, de nous en débarrasser. Il apparaît que la bonne notion est définie en terme des lettres $d_{p,q}^{-1}$, et c'est ce qu'on appelle un *mot dangereux*.

Définition 1.6. Pour $n \geqslant 3$, un D_n-mot est appelé $a_{p,n}$-*dangereux* de type q s'il est de la forme

$$d_{f(k),n-1}^{-1}\; d_{f(k-1),n-1}^{-1} \;...\; d_{f(1),n-1}^{-1} \tag{4.2}$$

avec $q = f(k) \geqslant f(k-1) \geqslant ... \geqslant f(1) = p$.

Par convention l'unique mot $a_{n-1,n}$-dangereux est le mot vide .

Notons qu'un mot dangereux w est entièrement déterminé par le Σ_n-mot $\underline{w}$ en regroupant les lettres σ_i^{-1} à partir de la droite et en coupant devant chaque lettre σ_{n-2}^{-1}. Par exemple, le B_4-mot $\sigma_3^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}$ peut seulement être la traduction du mot $a_{1,5}$-dangereux $d_{2,4}^{-1}d_{1,4}^{-1}$.

À ce point, la définition d'un mot dangereux semble venir de nulle part. Pour le moment, observons que dans l'expression $d_{p,n}\, d_{p,n-1}^{-1}$ de $a_{p,n}$, le fragment négatif $d_{p,n-1}^{-1}$ est $a_{p,n}$-dangereux. Ceci reflète l'intuition que les mots dangereux sont associés aux parties négatives des A_n-mots—donc à leurs parties dangereuses pour notre but, qui est de trouver des expressions σ-positives.

1.2 L'algorithme de renversement

Le but de cette section est de décrire un algorithme qui, partant d'un mot $a_{p,n}$-dangereux u et d'une $a_{p,n}$-échelle w, renvoie un mot σ_{n-2}-positif w' qui est équivalent à $u\, w'$ et qui est presque une $a_{p,n}$-échelle dans un sens que l'on définira plus tard.

L'élément de base est un procédé dit de *renversement* qui transforme certains AD_n-mots avec des lettres $d_{..,n-1}^{-1}$ à gauche en mots avec des lettres $d_{..,n-1}^{-1}$ à droite (ou sans lettre $d_{..,n-1}^{-1}$ du tout). Ainsi le renversement est un procédé permettant de pousser des lettres $d_{..,n-1}^{-1}$ vers la droite.

Définition 1.7. Soient w, w' des AD_n-mots. On dit que la relation $w \curvearrowright^{(1)} w'$ est vraie si w' est obtenu de w en remplaçant un sous mot u de w par un mot u' tel que (u, u') est l'une des paires suivantes

$$(d_{p,n-1}^{-1} a_{r,s}, \quad R_p(a_{r,s})\, d_{p,n-1}^{-1}) \qquad \text{avec } s \leqslant p \leqslant n-2 \text{ ou } p \leqslant r \leqslant n-2, \tag{4.3}$$

$$(d_{p,n-1}^{-1} a_{r,s}, \quad d_{r,n-1} R'_p(a_{r,s})\, d_{s,n-1}^{-1}) \qquad \text{avec } r < p < s \leqslant n-1, \tag{4.4}$$

$$(d_{p,n-1}^{-1} d_{r,n-1}, \quad d_{r,n-1}\, R''_p) \qquad \text{avec } r < p \leqslant n-2, \tag{4.5}$$

avec

$$R_p(a_{r,s}) = \begin{cases} a_{r,n-1} & \text{pour } s = p, \\ a_{r,s} & \text{pour } s < p, \\ a_{s-1,n-1} & \text{pour } r = p, \\ a_{r-1,s-1} & \text{pour } r > p. \end{cases} \qquad \begin{aligned} R'_p(a_{r,s}) &= d_{p-1,n-2}^{-1}\, d_{r,s-1}^{-1}, \\ R''_p &= d_{p-1,n-2}^{-1}. \end{aligned}$$

On dit que w se *renverse en ℓ étapes* en w', noté $w \curvearrowright^{(\ell)} w'$, s'il existe une suite de mots

$$w_0, w_1, \dots, w_\ell,$$

satisfaisant $w_0 = w$, $w_\ell = w'$, et $w_k \curvearrowright^{(1)} w_{k+1}$ pour tout k. On dit que w se *renverse* en w', noté $w \curvearrowright w'$, s'il existe ℓ tel que w se renverse en ℓ étapes en w'.

Formellement, le renversement est similaire à l'opération de retournement à droite introduite à la section II.3.2. Cependant, cette similitude est seulement superficielle : ce qui est commun c'est l'idée de pousser certain facteurs spécifiques à droite, mais les facteurs considérés et les règles d'échanges sont complètement différentes.

Avant de donner un exemple, nous introduisons la notion de diagramme de renversement qui est similaire à la notion de diagramme de retournement à droite et qui est plus commode pour illustrer le processus de renversement. Supposons que $w_0, w_1, \dots, w_\ell$ soit une suite de renversements, c'est-à-dire, une suite de AD_n-mots, tels que $w_k \curvearrowright w_{k+1}$ soit vérifiée pour tout k. D'abord, nous associons à w_0 un chemin étiqueté par ses lettres successives : on associe à toute lettre $d_{p,n-1}^{-1}$ une flèche verticale dirigée vers le bas étiquetée $d_{p,n-1}$, et à toute autre lettre x une flèche horizontale dirigée vers la droite étiquetée x. Alors, on représente successivement les mots $w_1, \dots, w_\ell$ de la manière suivante : si w_{k+1} est obtenu de w_k en remplaçant un sous mot $d_{p,n-1}^{-1} x$ de w_k par $u\, d_{q,n-1}^{-1}$ (où $d_{p,n-1}^{-1} x \curvearrowright^{(1)} u d_{q,n-1}^{-1}$ est satisfaite), alors on complète le schéma associé au sous-mot $d_{p,n-1}^{-1} x$ en utilisant une flèche horizontale dirigée vers la droite étiquetée x et une flèche verticale dirigée vers le bas étiquetée $d_{q,n-1}$, voir figure 4.1.

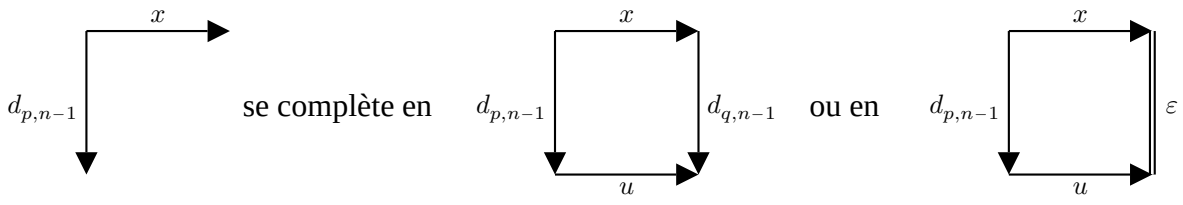


FIG. 4.1 : Renversement de $d_{p,n-1}^{-1} x$ en $u\, d_{q,n-1}^{-1}$. On remplace la flèche dirigée vers le bas étiquetée $d_{q,n-1}$ par une arrête verticale étiquetée ε lorsqu'on a $q = n-1$, c'est-à-dire, lorsque $d_{q,n-1} = \varepsilon$ est vérifiée.

Supposons que w et w' soient deux AD_n-mots et que w se renverse en w'. Alors la suite de renversements allant de w à w' n'est pas unique, mais le diagramme de renversement obtenu

dépend seulement de w et w'. Le renversement donne facilement lieu à un algorithme déterministe en choisissant de toujours retourner le sous-mot possible le plus à droite. L'algorithme termine quand un mot avec aucun sous-mot $d_{p,n-1}^{-1}$ ne pouvant être renversé est obtenu. Cet algorithme est appelé *algorithme de renversement*.

Voir figure 4.2 pour un exemple.

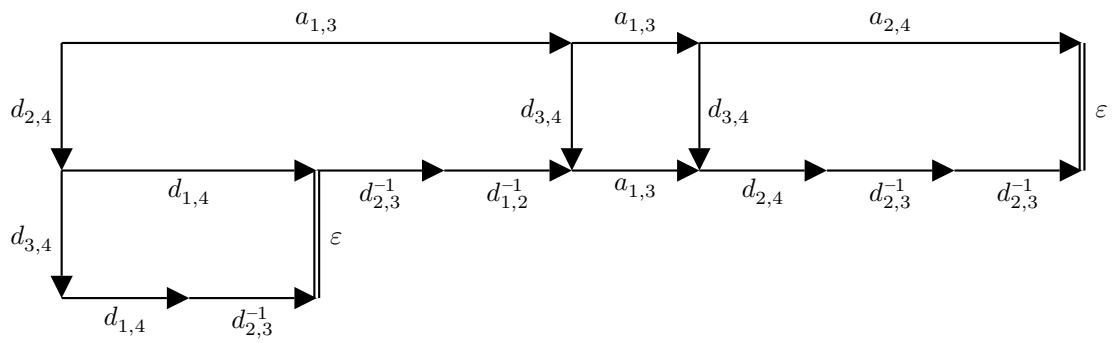


FIG. 4.2 : Diagramme de renversement du AD_4-mot $d_{3,4}^{-1}d_{2,4}^{-1}a_{1,3}a_{1,3}a_{2,4}$. On arrête avec $d_{1,4}d_{2,3}^{-1}d_{2,3}^{-1}d_{1,2}^{-1}a_{1,3}d_{2,4}d_{2,3}^{-1}d_{2,3}^{-1}$. Chaque rectangle dans le diagramme correspond à une relation $u \curvearrowright^{(1)} u'$, donc le nombre de rectangles est la longueur de toute suite de renversement $(w_0, \dots, w_\ell)$: la suite n'est pas unique, mais sa longueur et le diagramme correspondant le sont.

1.3 Premières propriétés

À la section précédente nous avons défini l'algorithme de renversement prenant en entrée un AD_n-mot et renvoyant un AD_n-mot. On peut alors naturellement se demander quels sont les liens entre ces deux mots. Une première étape consiste a montrer que le mot retourné est équivalent à celui d'entrée. Pour cela nous passerons par le résultat technique suivant portant sur les tresses $d_{p,q}$:

Lemme 1.8. *Les relations suivantes sont satisfaites :*

– $\phi_n(d_{p,q}) \equiv d_{p+1,q+1}$ *pour* $p < q \leqslant n-1$, (1.8.i)
– $d_{r,s}^{-1}\, a_{p,q}\, d_{r,s} \equiv \phi_s^{-1}\big(\phi_r(a_{p,q})\big)$ *pour* $p < q \leqslant r < s$. (1.8.ii)

Démonstration. La relation (1.8.i) est une conséquence immédiate de (III.3.6). Pour (1.8.ii), on observe d'abord que la relation (II.2.6) implique l'équivalence $d_{r,s} \equiv d_{1,r}^{-1}\, d_{1,s}$. On déduit que le mot $d_{r,s}^{-1}\, a_{p,q}\, d_{r,s}$ est équivalent à $d_{1,s}^{-1}\, d_{1,r}\, a_{p,q}\, d_{1,r}^{-1}\, d_{1,s}$. Comme, par hypothèse, $a_{p,q}$ appartient au monoïde B_r^{+*}, le sous-mot $d_{1,r}\, a_{p,q}\, d_{1,r}^{-1}$ est équivalent à $\phi_r(a_{p,q})$, nous rappelons que la tresse $d_{1,r}$ est représentée par le D_n-mot $d_{1,r}$. Finalement comme le monoïde B_r^{+*} est inclus dans le monoïde B_s^{+*} et que $\phi_r(a_{p,q})$ appartient à B_r^{+*}, on obtient l'équivalence entre les mots $d_{1,s}^{-1}\, \phi_r(a_{p,q})\, d_{1,s}$ et $\phi_s^{-1}\big(\phi_r(a_{p,q})\big)$. □

Nous pouvons maintenant démontrer que le AD_n-mot renvoyé par l'algorithme de renversement est équivalent au AD_n-mot d'entrée.

Lemme 1.9. *Pour w, w' des AD_n-mots, la relation $w \curvearrowright w'$ implique $w \equiv w'$.*

Démonstration. Il est suffisant de monter que $w \curvearrowright^{(1)} w'$ implique $w \equiv w'$, donc de monter que le mot u est equivalent à u' si (u, u') est une paire de la définition 1.7. On commence avec le couple (4.3). Supposons d'abord $s \leqslant p$. La relation (1.8.ii) implique

$$d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv \phi_{n-1}^{-1}(\phi_p(a_{r,s})). \tag{4.7}$$

Pour $s < p$, nous avons $\phi_p(a_{r,s}) = a_{r+1,s+1}$, puis $\phi_{n-1}^{-1}(\phi_p(a_{r,s})) = a_{r,s}$. La relation (4.7) devient alors $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv a_{r,s}$. On a donc la relation $d_{p,n-1}^{-1} a_{r,s} \equiv a_{r,s}\, d_{p,n-1}^{-1}$, c'est à dire

$$d_{p,n-1}^{-1} a_{r,s} \equiv R_p(a_{r,s})\, d_{p,n-1}^{-1} \quad \text{pour le cas } s < p.$$

Pour $s = p$, nous avons $\phi_p(a_{r,s}) = a_{1,r+1}$, puis $\phi_{n-1}^{-1}(\phi_p(a_{r,s})) = a_{r,n-1}$. La relation (4.7) devient alors $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv a_{r,n-1}$. On a donc la relation $d_{p,n-1}^{-1} a_{r,s} \equiv a_{r,n-1}\, d_{p,n-1}^{-1}$, c'est à dire

$$d_{p,n-1}^{-1} a_{r,s} \equiv R_p(a_{r,s})\, d_{p,n-1}^{-1} \quad \text{pour le cas } s = p.$$

Maintenant, supposons $r \geqslant p$. La relation (II.2.6) implique $d_{p,n-1} \equiv d_{1,p}^{-1}\, d_{1,n-1}$. On a donc

$$d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv d_{1,n-1}^{-1}\, d_{1,p}\, a_{r,s}\, d_{1,p}^{-1}\, d_{1,n-1}. \tag{4.8}$$

Pour $r > p$, les relations (II.2.5) et (II.2.7) impliquent que les tresses $d_{1,p}$ et $a_{r,s}$ commutent. La relation (4.8) assure alors l'équivalence entre $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1}$ et $\phi_{n-1}^{-1}(a_{r,s})$. La relation (4.8) devient $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv a_{r-1,s-1}$ et on obtient

$$d_{p,n-1}^{-1} a_{r,s} \equiv R_p(a_{r,s})\, d_{p,n-1}^{-1} \quad \text{pour le cas } r > p.$$

Pour $r = p$, la relation (II.2.5) implique que la tresse $d_{1,p}\, a_{r,s}\, d_{1,p}^{-1}$ est équivalente à $a_{1,s}$. Ainsi, par (4.8), il y a équivalence entre les tresses $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1}$ et $\phi_{n-1}^{-1}(a_{1,s})$. La relation (4.8) devient $d_{p,n-1}^{-1}\, a_{r,s}\, d_{p,n-1} \equiv a_{s-1,n-1}$ et on obtient

$$d_{p,n-1}^{-1} a_{r,s} \equiv R_p(a_{r,s})\, d_{p,n-1}^{-1} \quad \text{pour le cas } r = p.$$

Considérons maintenant le couple (4.5). La relation (II.2.6) implique $d_{r,n-1} \equiv d_{1,r}^{-1}\, d_{1,n-1}$. On a donc

$$d_{r,n-1}^{-1}\, d_{p,n-1}^{-1}\, d_{r,n-1} \equiv d_{1,n-1}^{-1}\, d_{1,r}\, d_{p,n-1}\, d_{1,r}^{-1}\, d_{1,n-1}. \tag{4.9}$$

Par (II.2.7), les tresses $d_{1,r}$ et $d_{p,n-1}$ commutent. Ainsi $d_{1,r}\, d_{p,n-1}\, d_{1,r}^{-1}$ est équivalente à $d_{p,n-1}$. Par (1.8.i), la relation (4.9) devient donc $d_{r,n-1}^{-1} d_{p,n-1}^{-1} d_{r,n-1} \equiv d_{p-1,n-2}^{-1}$ et on obtient

$$d_{p,n-1}^{-1} d_{r,n-1} \equiv d_{r,n-1} R_p''.$$

Finalement, considérons le couple (4.4). Comme, par (II.2.5), on a $a_{r,s} \equiv d_{r,s}\, d_{r,s-1}^{-1}$ et que la relation (II.2.6) implique $d_{r,s} \equiv d_{r,n-1}\, d_{s,n-1}^{-1}$, on obtient

$$d_{p,n-1}^{-1}\, a_{r,s} \equiv d_{p,n-1}^{-1}\, d_{r,n-1}\, d_{s,n-1}^{-1}\, d_{r,s-1}^{-1}. \tag{4.10}$$

Par (II.2.7), les lettres $d_{s,n-1}$ et $d_{r,s-1}^{-1}$ commutent. De plus, (4.5) implique que le mot $d_{p,n-1}^{-1} d_{r,n-1}$ est équivalent au mot $d_{r,n-1}\, d_{p-1,n-2}^{-1}$. La relation (4.10) devient donc

$$d_{p,n-1}^{-1}\, a_{r,s} \equiv d_{r,n-1}\, d_{p-1,n-2}^{-1}\, d_{r,s-1}^{-1}\, d_{s,n-1}^{-1}$$

et on obtient $d_{p,n-1}^{-1}\, a_{r,s} \equiv d_{r,n-1}\, R_p'(a_{r,s})\, d_{s,n-1}^{-1}$. □

2 Dangereux contre échelle

Nous allons maintenant appliquer l'algorithme de renversement aux mots constitués d'un mot $a_{p,n}$-dangereux suivi d'une $a_{p,n}$-échelle, dans le but d'obtenir un mot σ_i-positif équivalent lorsque c'est possible.

Encore une fois, le problème consiste à identifier la forme générique des mots finaux que nous pouvons obtenir. Une nouveau type de mot de tresses appelé *mur* apparaît ici, et le résultat principal est que le renversement d'un mot constitué d'un mot $a_{p,n}$-dangereux suivi d'une $a_{p,n}$-échelle donne toujours un mot σ-nonnégatif qui est un mur.

Nous proposons ici une description faite par induction sur la longueur du mot dangereux considéré.

2.1 Cas de la longueur 1

La première étape consiste à décrire le mot retourné par l'algorithme de renversement appliqué à un mot dangereux de longueur 1 suivi d'une échelle. Pour cela nous introduisons un nouveau type de AD_n-mot appelé mur, qui est un affaiblissement de la notion d'échelle. Le principal résultat de cette section est que, dans le cas d'un dangereux de longueur 1 suivi d'une échelle, l'algorithme de renversement retourne un mur proche de l'échelle d'entrée.

La notion de mur se décline en deux versions, l'une dite *grand mur* et l'autre dite *petit mur*.

Définition 2.1. Pour $n \geqslant 3$ et $p \leqslant n-2$, on dit qu'un AD_{n-1}-mot w est un *grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$* s'il existe une décomposition

$$w = u \cdot d_{r,n-1} \cdot w' \cdot d_{q-1,n-1} \cdot v$$

satisfaisant les conditions suivantes

- $r < p$, (2.1.i)
- u est un A_{n-1}-mot positif, (2.1.ii)
- w' est un AD_{n-1}-mot σ_{n-2}-nonnégatif sans A_{n-1}-lettre négative, (2.1.iii)
- v est $a_{q-1,n-1}$-dangereux. (2.1.iv)

On dit qu'un AD_{n-1}-mot w est un *petit $a_{p,n}$-mur adossé à $a_{q-1,n-1}$* s'il existe une décomposition

$$w = u \cdot d_{q-1,n-1} \cdot v$$

satisfaisant les conditions suivantes

- $q-1 < p$, (2.1.v)
- u est un A_{n-1}-mot positif, (2.1.vi)
- v est $a_{q-1,n-1}$-dangereux de type $p' < p$. (2.1.vii)

Dans les deux cas, on note $F(w)$ le mot u défini ci-dessus, et $D(w)$ le mot v défini ci-dessus.

On dit qu'un A_{n-1}-mot w est un *$a_{p,n}$-mur* s'il est soit un grand soit un petit $a_{p,n}$-mur.

Notons que la condition satisfaite par la lettre $d_{r,n-1}$ présente dans la décomposition d'un grand mur est la même que celle satisfaite par la $a_{p,n}$-barrière $a_{r,n-1}$. La même propriété est vérifiée pour la lettre $d_{q-1,n-1}$ intervenant dans la décomposition d'un petit mur.

Pour le moment nous avons défini les $a_{p,n}$-murs seulement pour $p \leqslant n-2$. Nous allons maintenant considérer des $a_{n-1,n}$-murs, qui sont tout aussi spéciaux que le sont les $a_{n-1,n}$-échelles.

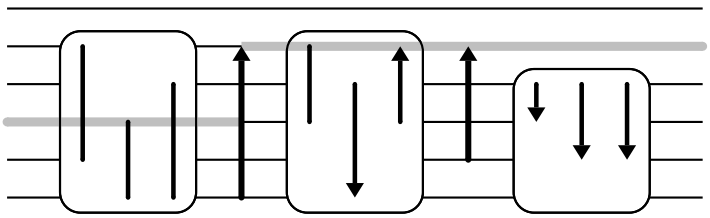


FIG. 4.3 : Un grand $a_{3,6}$-mur adossé à $a_{2,5}$ (celui de l'exemple 2.3). La ligne grise commence à la position 3 et grimpe à la position 5 en utilisant la lettre $d_{1,6}$ (correspondant à la lettre $d_{r,n-1}$ dans la définition d'un mur). La première boîte ne contient pas de flèche (c'est-à-dire, pas de lettre $d^{\pm 1}_{\cdot,\cdot}$, la deuxième boîte ne contient pas de flèche partant de l'avant-dernière ligne dirigée vers le bas (c'est-à-dire, pas de lettre $d^{-1}_{\cdot,5}$), la dernière boîte ne contient que des flèches dirigées vers le bas partant de l'antépénultième ligne.

Définition 2.2. Pour $n \geqslant 3$, on dit qu'un AD_{n-1}-mot w est un *$a_{n-1,n}$-mur adossé à $a_{q-1,n-1}$* si w admet la décomposition $u \cdot d_{q-1,n-1} \cdot v$ avec u un A_{n-1}-mot positif et v un mot $a_{q-1,n-1}$-dangereux. On pose alors $F(w) = u$ et $D(w) = v$.

Par définition, tout $a_{p,n}$-mur adossé à $a_{q-1,n-1}$ est aussi un $a_{r,n}$-mur adossé à $a_{q-1,n-1}$ dès qu'on a $r \geqslant p$. En effet les seules conditions faisant intervenir p dans les définitions 2.1 et 2.2 sont des inégalités de la forme $.. < p$.

Exemple 2.3. Le mot w défini par

$$w = a_{2,4}a_{1,3}a_{1,5}d_{1,5}a_{3,5}d^{-1}_{1,4}d_{3,5}d_{2,5}d^{-1}_{3,4}d^{-1}_{2,4}d^{-1}_{2,4},$$

est un grand $a_{3,6}$-mur adossé à $a_{2,5}$. En effet, en posant

$$u = a_{2,4}a_{1,3}a_{1,5}, \quad w' = a_{3,5}d^{-1}_{1,4}d_{3,5} \quad et \quad v = d^{-1}_{3,4}d^{-1}_{2,4}d^{-1}_{2,4},$$

on a $w = u\, d_{1,5}\, w'\, d_{2,5}\, v$, qui est une décomposition de grand $a_{3,6}$-mur adossé à $a_{2,5}$: u est un mot contenant que des A_5-lettres, w est un AD_5-mot ne contenant pas de A_5-lettres négatives ni de D_5-lettres de la forme $d^{-1}_{\cdot,4}$ et le mot v est $a_{2,5}$-dangereux.

Notons que par définition un $a_{p,n}$-mur ne contient jamais de A_{n-1}-lettres négatives.

La notion de mur peut être facilement illustrée en représentant les lettres sur une partition à n lignes : une lettre $a_{p,q}$ est représentée par une trait vertical allant de la p ème ligne à la q ème (comme pour les échelles), une lettre $d^{-1}_{p,q}$ est représentée par une flèche verticale allant de la p ème ligne à la q ème ligne (donc dirigée vers le haut) et une lettre $d_{p,q}$ est représentée par une flèche verticale reliant la q ème ligne à la $p$ème (donc dirigée vers le bas)—voir figure 4.3.

Lemme 2.4. *Soit w une $a_{p,n}$-échelle adossée à $a_{q-1,n-1}$ avec $p \leqslant n-2$ et $n \geqslant 3$. Notons*

$$w_0\, x_1 \ldots\, x_h\, w_h$$

la décomposition de w en tant qu'échelle. Alors $d^{-1}_{p,n-1}\, w$ est équivalent à un $a_{p,n}$-mur w' adossé à $a_{q-1,n-1}$. Ce dernier est calculé en utilisant au plus ℓ étapes de renversement plus éventuellement une opération élémentaire, et il satisfait

- $|F(w')| = |w_0|$, (2.4.i)
- $|D(w')| \leqslant 2$, (2.4.ii)
- $|w'| \leqslant |w| + 2(h-1) + 2|w_h| + |D(w')|$, (2.4.iii)
- *w' est un grand mur pour $w_h \neq \varepsilon$.* (2.4.iv)

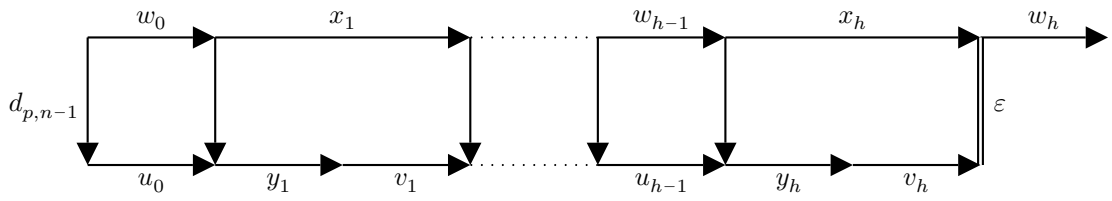


FIG. 4.4 : Renversement de $d_{p,n-1}^{-1}\,w$ en un mur lorsque w est une échelle (démonstration du lemme 2.4).

Démonstration. L'idée principale est illustrée sur la figure 4.4 : partant de $d_{p,n-1}^{-1}\,w$, c'est-à-dire, du AD_{n-1}-mot $d_{p,n-1}^{-1}\,w_0\,x_1\,...\,x_h\,w_h$, nous retournons le diagramme en poussant les flèches verticales vers la droite jusqu'à obtenir un mur équivalent. L'obtention d'un AD_{n-1}-mot équivalent est garantie par le lemme 1.9.

En général, ce que nous obtenons est un grand mur. Cependant, quelques petits cas particulier sont traités à part, à savoir lorsque w_h est le mot vide—dans ce cas on obtient un petit mur si la hauteur h de l'échelle w vaut 1.

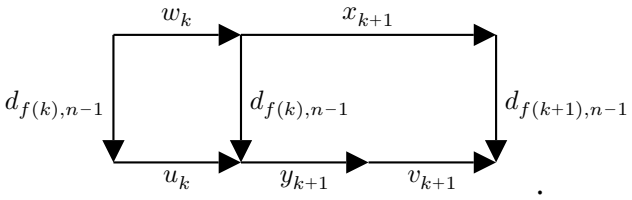
Commençons par décrire les blocs élémentaires du diagramme de la figure 4.4. Pour tout k dans $\{1,\dots,h\}$, notons $a_{e(k),f(k)}$ la lettre x_k et posons $f(0)=p$. Pour k dans $\{0,\dots,h-1\}$, on définit les mots u_k, y_{k+1} et v_{k+1} de la façon suivante :

$$u_k = R_{f(k)}(w_k), \quad y_{k+1} = d_{e(k+1),n-1} \quad \text{et} \quad v_{k+1} = R'_{f(k)}(x_{k+1}).$$

Par définition du renversement $\curvearrowright$ on obtient

$$d_{f(k),n-1}^{-1}\,w_k\,x_{k+1}\curvearrowright^{(|w_k x_{k+1}|)} u_k\,y_{k+1}\,v_{k+1}\,d_{f(k+1),n-1}^{-1},$$

ce qui correspond au diagramme :



.

Regroupant les divers diagrammes de renversement correspondant aux valeurs successives du paramètre k, on obtient exactement le diagramme de la figure 4.4. Pour k dans $\{1,\dots,h-1\}$, on note w'_k le mot $u_k\,y_{k+1}\,v_{k+1}$. À partir de maintenant, nous avons trois cas à considérer.

Supposons d'abord que w_h soit le mot vide ε et qu'on ait $h \geqslant 2$, le cas le plus facile, à partir duquel les autres sont dérivés. Posons $w' = w'_0\,...\,w'_{h-1}$. Par construction, on a $d_{p,n-1}^{-1}\,w\curvearrowright^{(|w|)} w'$. Donc, par le lemme 1.9, le mot $d_{p,n-1}^{-1}\,w$ est équivalent à w'. Nous allons maintenant prouver que le mot w' est un mur du type escompté, et que les énoncés de complexité sont satisfaits. Comme w_h est vide, la dernière lettre de w est x_h. Ceci, par définition d'une échelle, implique les relations $x_h = a_{q-1,n-1}$ et $y_h = d_{q-1,n-1}$. Posons $w'' = v_1\,w'_2\,...\,w'_{h-2}\,u_{h-1}$. On a donc

$$w' = u_0 \cdot d_{e(1),n-1} \cdot w'' \cdot d_{q-1,n-1} \cdot v_h.$$

Montrons que w' est un grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$. Comme l'image d'une A_{n-1}^+-lettre par R_p est une A_{n-1}^+-lettre, le mot u_0 est un A_{n-1}^+-mot de longueur $|w_0|$. Ainsi les conditions (2.1.ii) et (2.4.i) sont satisfaites. Ensuite, par définition d'une échelle, la lettre x_1 est une $a_{p,n}$-barrière, ce qui implique $e(1) < p$, c'est-à-dire que la condition (2.1.i) est satisfaite.

Le mot w'' est aussi σ_{n-2}-nonnégatif et ne contient pas de A_{n-1}-lettre négative car c'est le cas des mots u_k, y_{k+1} et v_{k+1}. La condition (2.1.iii) est donc vérifiée. Rappelons que le mot v_h est égal à $d^{-1}_{f(h-1)-1,n-2}\, d^{-1}_{e(h),n-2}$ avec $e(h) = q-1$. Par définition d'une échelle, le lettre x_h est une $a_{f(h-1),n}$-barrière. Nous avons donc $q-1 < f(h-1)$, ce qui implique $f(h-1)-1 \geqslant q-1$. Ainsi le mot v_h est $a_{q-1,n-1}$-dangereux de longueur 2, et les conditions (2.1.iv) et (2.4.ii) sont vérifiées. Finalement, pour (2.4.iii), on calcule

$$|w'_k| = |u_{k-1}| + |y_k| + |v_k| = |w_{k-1}| + 1 + 2 = |w_{k-1}\, x_k| + 2.$$

Alors, comme w_h est le mot vide, nous obtenons

$$|w'| = \sum_{k=0}^{h-1} |w'_k| = \sum_{k=0}^{h-1} |w_k\, x_{k+1}| + 2h = |w| + 2h.$$

Comme dans le cas que l'on considère w_h est supposé vide et que la longueur de $D(w')$ est 2, c'est-à-dire que la longueur de v_h est 2, la condition (2.4.iii) est satisfaite. Le cas w_h vide avec $h \geqslant 2$ est donc complet ; à l'exception du calcul de complexité en temps.

Supposons toujours que w_h soit le mot vide mais, maintenant, que la hauteur h de l'échelle w soit 1. Alors le mot w' est égal à $u_0 \cdot d_{q-1,n-1} \cdot v_1$. Comme pour le cas précédent, on montre que u_0 est un A^+_{n-1}-mot de longueur w_0 et que nous avons $|w'| = |w|+2$. Le mot v_1 est égal à $d^{-1}_{p-1,n-2}\, d^{-1}_{q-1,n-2}$, qui est un mot $a_{q-1,n-1}$-dangereux de type $p-1$ et de longueur 2. Ainsi, w' est un petit $a_{p,n}$-mur adossé à $a_{q-1,n-1}$ satisfaisant (2.4.i), (2.4.ii) et (2.4.iii).

Supposons finalement que w_h soit non vide. On décompose alors w_h en $w''_h\, a_{q-1,n-1}$. Posons

$$w' = w'_0 \ldots w'_{h-1}\, w''_h\, d_{q-1,n-1}\, d^{-1}_{q-1,n-2} \quad \text{et} \quad w'' = v_1\, w'_2 \ldots w'_{h-1}\, w''_h.$$

Nous avons alors la relation suivante liant w' et w''

$$w' = u_0 \cdot\, d_{f(1),n-1} \cdot\, w'' \cdot\, d_{q-1,n-1} \cdot\, d^{-1}_{q-1,n-2}.$$

Les conditions (2.1.ii), (2.1.i), (2.1.iii) sont vérifiées comme pour les précédents cas. Comme le mot $d^{-1}_{q-1,n-2}$ est $a_{q-1,n-1}$-dangereux et de longueur 1, les conditions (2.1.iv) et (2.4.ii) sont vérifiées. Ensuite, par construction de w', la condition (2.4.iv) est satisfaite. Vérifions la condition (2.4.iii). Partant de la relation $|w'_k| = |w_k\, x_{k+1}|+2$, nous obtenons

$$|w'| = \sum_{k=0}^{h-1} |w'_k| + |w''_h| + 2 = \sum_{k=0}^{h-1} |w_k\, x_{k+1}| + |w_h| + 2h + 1 = |w| + 2h + 1.$$

Comme w_h est non vide, on a $|w_h| \geqslant 1$, donc, $2|w_h| \geqslant 2$. De plus, comme la longueur de $D(w')$ est 1, nous obtenons $3 \leqslant 2|w_h|+|D(w')|$, et finalement

$$|w'| \leqslant |w| + 2(h-1) + 2|w_h| + |D(w')|.$$

Tous les cas sont maintenant traités. Il reste seulement à considérer la complexité en temps. Dans les deux premiers cas, au plus $|w|$ opérations de renversement sont nécessaires. Dans le dernier cas—$w_h \neq \varepsilon$—au plus $|w|$ opérations de renversement sont nécessaires plus la décomposition de $w_h^{\#}$ en produit de deux D_{n-1}-lettres. □

Exemple 2.5. Nous avons vu à l'exemple III.3.12 que le mot $w = a_{3,4}\, a_{1,3}\, a_{1,3}\, a_{2,4}\, a_{3,4}$ est une $a_{2,5}$-échelle adossée à $a_{3,4}$. Calculons le $a_{2,5}$-mur adossé à $a_{3,4}$ qui est équivalent à $d_{2,5}^{-1}\, w$. L'algorithme de renversement appliqué à $d_{2,4}^{-1}\, w$ donne

$$w'' = a_{2,3}\, d_{1,4}\, d_{1,3}^{-1}\, d_{1,2}^{-1}\, a_{1,4}\, d_{2,4}\, d_{2,3}^{-1}\, d_{2,3}^{-1}\, a_{3,4} \quad \text{(voir figure 4.5)}.$$

Le mot w'' n'est pas une échelle car sa dernière lettre n'est pas de la forme requise. Cependant, si nous remplaçons la dernière lettre $a_{3,4}$ de w'' par $d_{3,4}$ nous obtenons un grand mur :

$$w' = a_{2,3} \cdot d_{1,4} \cdot d_{1,3}^{-1}\, d_{1,2}^{-1}\, a_{1,4}\, d_{2,4}\, d_{2,3}^{-1}\, d_{2,3}^{-1} \cdot d_{3,4} \cdot \varepsilon.$$

Le mot $F(w')$ de w' est alors $a_{2,3}$, tandis que $D(w')$ est le mot vide.

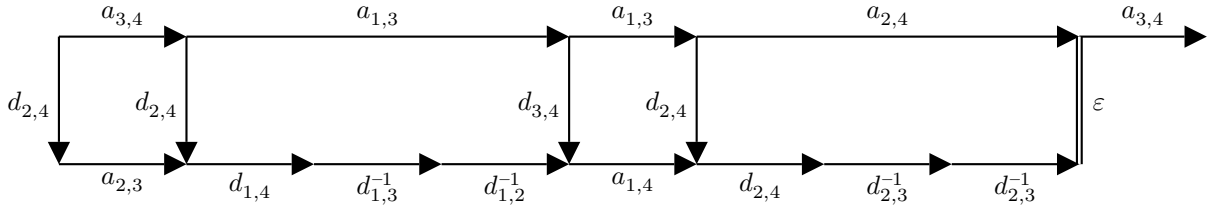


FIG. 4.5 : Diagramme de renversement du mot $d_{2,4}^{-1}\, a_{3,4}\, a_{1,3}\, a_{1,3}\, a_{2,4}\, a_{3,4}$.

2.2 Dangereux de longueur 1 contre mur

À la section précédente, nous avons étudié l'algorithme de renverserment sur un mot $u\, w$ dans le cas particulier où u est un mot $a_{p,n}$-dangereux de longueur 1 et w est une $a_{p,n}$-échelle. Nous avons alors prouvé que le mot renvoyé est un $a_{p,n}$-mur. Avant de nous intéresser au cas général d'un mot constitué d'un mot dangereux initial de longueur arbitraire suivi d'une échelle, nous considérons ici le cas d'un mot $a_{p,n}$-dangereux de longueur 1 suivi d'un $a_{p,n}$-mur. Le résultat est que le mot obtenu après application de l'algorithme de renversement est encore un $a_{p,n}$-mur. Ceci montre que, contrairement aux échelles, la famille des murs admet une bonne propriété de clôture par multiplication à gauche par un mot dangereux suivi d'un retournement. Ceci nous permettra d'utiliser un argument par induction pour le cas général.

Nous commençons par un résultat technique qui sera utilisé deux fois dans la démonstration du lemme 2.7.

Lemme 2.6. *Supposons $n \geqslant 3$, que w est un A_{n-1}-mot positif contenant une $a_{p,n}$-barrière et qu'on ait $r < p$. Alors le mot $d_{p,n-1}^{-1}\, w\, d_{r,n-1}$ se renverse en le AD_{n-1}-mot*

$$u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d_{s-1,n-2}^{-1},$$

qui est obtenu en au plus $|w| + 1$ étapes de renversement et satisfait les condition suivantes :

- *$t < p$ et $r < s$,* (2.6.i)
- *u est un A_{n-1}^{+}-mot avec $|u| < |w|$,* (2.6.ii)
- *u' est un AD_{n-1}-mot σ_{n-2}-nonnégatif sans A_{n-1}-lettre négative,* (2.6.iii)
- *$|u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d_{s-1,n-2}^{-1}| \leqslant |w\, d_{r,n-1}| + 2|w| - 2|u| + 1$.* (2.6.iv)

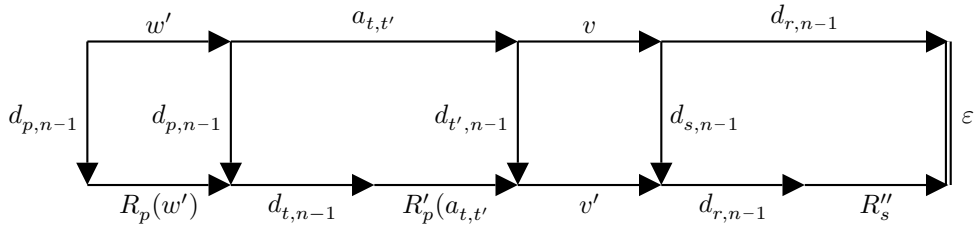


FIG. 4.6 : Renversement de $d_{p,n-1}^{-1}\, w$ en un mur lorsque w est un mur (démonstration du lemme 2.6).

Démonstration. Écrivons w comme le produit $w'\, a_{t,t'}\, v$ où w' est le préfixe maximal de w qui ne contient pas de $a_{p,n}$-barrière, et où $a_{t,t'}$ est une $a_{p,n}$-barrière. L'argument est illustré sur la figure 4.6 : partant de $d_{p,n-1}^{-1}\, w\, d_{r,n-1}$, nous renversons le diagramme en poussant les flèches verticales sur la droite jusqu'à ce qu'un mur soit obtenu. À chaque étape le succès est garanti par le lemme 1.9.

Comme le mot w' ne contient pas de $a_{p,n}$-barrière, on a $d_{p,n-1}^{-1}\, w' \curvearrowright^{(|w''|)} R_p(w')\, d_{p,n-1}^{-1}$. Par construction $a_{t,t'}$ est une $a_{p,n}$-barrière, c'est-à-dire qu'on a $t < p < t'$. Nous en déduisons

$$d_{p,n-1}^{-1}\, a_{t,t'} \curvearrowright^{(1)} d_{t,n-1} R'_p(a_{t,t'})\, d_{t',n-1}^{-1}.$$

Par définition des étapes élémentaires du procédé de renversement, on a $d_{t',n-1}^{-1}\, v \curvearrowright^{(|v|)} v'\, d_{s,n-1}^{-1}$ pour un certain AD_n-mot v' avec $|v'| \leqslant 3|v|$ et $s \geqslant t'$. L'hypothèse $r < p$ combinée à $p < t'$ et $t' \leqslant s$ implique $r < s$. Ainsi $d_{s,n-1}^{-1}\, d_{r,n-1}$ se renverse en une étape en $d_{r,n-1}\, R''_s$, c'est à dire, en $d_{r,n-1}\, d_{s,n-1}^{-1}$.

Posons $u = R_p(w')$ et $u' = R'_p(a_{t,t'})\, v'$. Par construction, on a

$$d_{p,n-1}^{-1}\, w\, d_{r,n} \curvearrowright^{(|w|+1)} u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d_{s-1,n-1}^{-1}.$$

Montrons que le dernier mot vérifie les propriétés attendues. La condition (2.6.i) est une conséquence immédiate des résultats ci-dessus. Comme l'image d'une A_{n-1}^+-lettre par R_p est aussi une A_{n-1}^+-lettre, le mot u est un A_{n-1}^+-mot de longueur $|w'|$. Par définition, le mot w' est un préfixe strict de w. Ce qui implique $|w'| < |w|$, c'est-à-dire que la condition (2.6.ii) est vérifiée. Comme l'image d'un A_{n-1}^+-mot par R et R' est σ_{n-2}-nonnégatif sans A_{n-1}-lettre négative, il en est de même de v' et $R'_p(a_{t,t'})$, donc de u', c'est-à-dire que la condition (2.6.iii) est satisfaite. Pour (2.6.iv), on calcule

$$|u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d_{s-1,n-2}^{-1}| = |w'| + |u'| + 3 = |w'| + |v'| + 5.$$

Par construction de v', nous avons $|v'| \leqslant 3|v|$. De $|w| = |w'|+1+|v|$, nous en déduisons

$$\begin{aligned} |u\, d_{t,n-1}\, u'\, d_{r,n-1}\, d_{s-1,n-2}^{-1}| &\leqslant 3|w| - 2|w'| + 2 \\ &\leqslant |w\, d_{p,n-1}| + 2(|w| - |w'|) + 1, \end{aligned}$$

qui est l'inégalité désirée car $|w'|$ est égale à $|u|$ par (2.6.ii). □

Nous pouvons maintenant établir le résultat principal de cette section.

Lemme 2.7. *Supposons que w soit un $a_{p,n}$-mur adossé à $a_{q-1,n-1}$. Alors $d_{p,n-1}^{-1} w$ se renverse en au plus $|F(w)| + 1$ étapes en un $a_{p,n}$-mur w' satisfaisant les conditions suivantes*

- $|F(w')| \leqslant |F(w)|$, (2.7.i)
- $|D(w')| \leqslant |D(w)| + 1$, (2.7.ii)
- $|w'| \leqslant |w| + 2|F(w)| - 2|F(w')| + 1$, (2.7.iii)
- *w' est un grand mur lorsque w est un grand mur.* (2.7.iv)

Démonstration. Supposons que w soit un petit mur. Le mot w admet alors la décomposition

$$w = F(w)\, d_{q-1,n-1}\, D(w).$$

Par définition d'un mur, on a $q-1 < p$. Supposons de plus que $F(w)$ ne contienne pas de $a_{p,n}$-barrière. Le renversement donne donc

$$d_{p,n-1}^{-1}\, w \curvearrowright^{(|F(w)|)} R_p(F(w))\, d_{p,n-1}^{-1}\, d_{q-1,n-1}\, D(w) \curvearrowright^{(1)} R_p(F(w))\, d_{q-1,n-1}\, d_{p-1,n-2}^{-1}\, D(w).$$

Posons

$$w' = u \cdot d_{q-1,n-1} \cdot v,$$

avec $u = R_p(F(w))$ et $v = d_{p-1,n-2}^{-1}\, D(w)$. Comme l'image d'une A_{n-1}^+-lettre par R est une A_{n-1}^+-lettre, u est un A_{n-1}^+-mot de longueur $|F(w)|$. De la relation $q-1 < p$ nous déduisons que w' est un petit $a_{p,n}$-mur adossé à $a_{q-1,n-1}$ satisfaisant les conditions (2.7.i) et (2.7.ii), car on a $D(w') = v$. La condition (2.7.iii) est une conséquence directe de la construction de w' et de l'égalité $|v| = |D(w)| + 1$.

Supposons maintenant que $F(w)$ contienne une $a_{p,n}$-barrière. Par le lemme 2.6 appliqué au mot $F(w)\, d_{q-1,n-1}$, il existe deux mots u et u', et deux entiers s et t satisfaisant

$$d_{p,n-1}^{-1}\, w \curvearrowright^{(|F(w)|+1)} u\, d_{t,n-1}\, u'\, d_{q-1,n-1}\, d_{s-1,n-2}^{-1}\, D(w).$$

Posons

$$w' = u \cdot d_{t,n-1} \cdot u' \cdot d_{q-1,n-1} \cdot v,$$

avec $v = d_{s-1,n-2}^{-1}\, D(w)$. La condition (2.6.i) implique que v est un mot $a_{q-1,n-1}$-dangereux de longueur au plus $|D(w)|+1$, et qu'on a $t < p$. Les conditions (2.6.ii) et (2.6.iii) impliquent alors que w est un grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$ et qu'il satisfait les conditions (2.7.i) et (2.7.ii). En utilisant (2.6.iv), on calcule

$$|w'| = |F(w)\, d_{q-1,n-1}| + 2|F(w)| - 2|u| + |v|,$$

qui implique (2.7.iii) car on a $F(w') = u$ et $D(w') = d_{s-1,n-2}^{-1}\, D(w) = v$.

Supposons maintenant que w soit un grand mur. Le mot w admet alors la décomposition

$$w = F(w)\, d_{r,n-1}\, w''\, d_{q-1,n-1}\, D(w),$$

avec $r < p$. Supposons d'abord que $F(w)$ ne contienne pas de $a_{p,n}$-barrière. Le renversement donne donc

$$d_{p,n-1}\, w \curvearrowright^{(|F(w)|+1)} R_p(F(w))\, d_{r,n-1}\, d_{p-1,n-2}^{-1}\, w''\, d_{q-1,n-1}\, D(w).$$

Posons

$$w' = R_p(F(w)) \cdot d_{r,n-1} \cdot d_{p-1,n-2}^{-1}\, w'' \cdot d_{q-1,n-1} \cdot D(w).$$

Une vérification directe, reposant sur le fait que w soit un grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$, montre que w' est un grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$ satisfaisant les conditions (2.7.i), (2.7.ii) et (2.7.iv). La condition (2.7.iii) est une conséquence de $|w'| = |w| + 1$.

Supposons maintenant que $F(w)$ contienne une $a_{p,n}$-barrière. Alors, par le lemme 2.6 appliqué au mot $F(w)\, d_{r,n-1}$, il existe deux mots u, u' et deux entiers s, t satisfaisant

$$d_{p,n-1}\, w \curvearrowright^{(|F(w)|+1)} u\, d_{t,n-1}\, u'\, d_{r-1,n-1}\, d_{s-1,n-2}^{-1}\, w''\, d_{q-1,n-1}\, D(w).$$

Posons

$$w' = u \cdot d_{t,n-1} \cdot u'\, d_{r-1,n-1}\, d_{s-1,n-2}^{-1}\, w'' \cdot d_{q-1,n-1} \cdot D(w).$$

La condition (2.6.iii) implique que le mot $u'\, d_{r-1,n-1}\, d_{s-1,n-2}^{-1}\, w''$ est σ_{n-2}-nonnégatif sans A_{n-1}-lettre négative. De plus, comme il contient la lettre $d_{r-1,n-1}$, il est même σ_{n-2}-positif. Ainsi, une vérification directe, basée sur le fait que w soit un grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$, montre que w' est aussi un grand $a_{p,n}$-mur adossé à $a_{q-1,n-1}$ et qu'il satisfait les conditions (2.7.i), (2.7.ii) et (2.7.iv). En utilisant la condition (2.6.iv), on obtient

$$|w'| \leqslant |F(w)\, d_{r,n-1}| + 2|F(w)| - 2|u| + 1 + |w''| + 1 + |D(w)|,$$

qui implique (2.7.iii) car on a $F(w') = u$. □

2.3 Cas général

À la section 2.1, nous avons montré que l'algorithme de renversement appliqué à un mot dangereux de longueur 1 suivi d'une échelle retourne un mur, tandis qu'à la section 2.2, nous avons montré que l'algorithme de renversement appliqué à un mot dangereux de longueur 1 suivi d'un mur retourne un mur. Nous allons maintenant décrire la sortie de l'algorithme de renversement lorsqu'on l'applique à n'importe quel mot dangereux suivi d'une échelle. Le résultat est que l'on obtient toujours un mur.

L'argument n'est pas difficile et la principale difficulté réside dans le calcul de complexité. Une attention particulière doit être apportée au fait que les différents murs considérés ne sont pas de même type.

Proposition 2.8. *Supposons que w soit une $a_{p,n}$-échelle adossée à $a_{q-1,n-1}$ et que u soit un mot $a_{p,n}$-dangereux, avec $n \geqslant 3$. Alors $u\,w$ est équivalent à un $a_{p,n}$-mur w' adossé à $a_{q-1,n-1}$. Il est calculé par au plus $|u|\,|w|$ opérations de renversement, plus éventuellement une opération élémentaire, donc en temps $O(\log(n)(|u||w|+1))$, et il satisfait les conditions suivantes*

- $|D(w')| \leqslant |u| + 1$, (2.8.i)
- $|w'| \leqslant 3|w| + |u| - 1$. (2.8.ii)

De plus, si w est une $a_{p,n}$-échelle adossée à $a_{n-2,n-1}$ mais différente de $a_{n-2,n-1}$, alors w' admet la décomposition $w' = w''\, d_{n-2,n-1}$, où w'' est un mot σ_{n-2}-positif.

Démonstration. Toutes les échelles et tous les murs utilisés dans cette démonstration sont supposés adossés à $a_{q-1,n-1}$, on omettra ainsi de le préciser. Construisons un $a_{p,n}$-mur w' qui est équivalent à $u\,w$ par induction sur la longueur de u.

Supposons d'abord $p \leqslant n-2$. Alors u n'est pas le mot vide ε. Posons

$$u = d_{f(e),n-1}^{-1} \cdot \ldots \cdot d_{f(1),n-1}^{-1}.$$

Notons $w_{(1)}$ le $a_{f(1),n}$-mur équivalent à $d_{f(1),n-1}^{-1}\, w$, donné par le lemme 2.4. Partant de $w_{(1)}$, on note inductivement $w_{(k+1)}$ le AD_{n-1}-mot obtenu en renversant $d_{f(k+1),n-1}^{-1}\, w_{(k)}$.

Montrons par induction que le mot $w_{(k)}$ est un $a_{f(k),n}$-mur. Supposons que le mot $w_{(k-1)}$ soit un $a_{f(k-1),n}$-mur. Par définition d'un mot dangereux on a la relation $f(k) \geqslant f(k-1)$. Le mot $w_{(k-1)}$ est donc aussi un $a_{f(k),n}$-mur. Ainsi, par le lemme 2.7, le mot $w_{(k)}$ est un $a_{f(k),n}$-mur.

Par construction, le mot $u\,w$ est équivalent à $w_{(e)}$. Donnons une borne sur la longueur de $w_{(e)}$. Le lemme 2.4 implique $|D(w_{(1)})| \leqslant 2$. Pour $1 \leqslant k \leqslant e-1$, la condition $(2.7.ii)$

implique $|D(w_{(k+1)})| \leqslant |D(w_{(k)})|+1$. Ainsi la relation $|D(w_{(e)})| \leqslant |u|+1$ est satisfaite, c'est-à-dire que (2.8.i) est vérifiée. Soit $w_0\, x_1 \,...\, x_h\, w_h$ la décomposition de w en tant que $a_{p,n}$-échelle. D'après la condition (2.7.iii), pour $k \geqslant 1$ on a la relation

$$|w_{(k+1)}| \leqslant |w_{(k)}| + 2|F(w_{(k)})| - 2|F(w_{(k+1)})| + 1. \tag{4.17}$$

Combinant les différentes relations (4.17) pour $k = 1, \dots, e-1$, on obtient

$$\begin{aligned} |w_{(e)}| &\leqslant |w_{(1)}| + 2|F(w_{(1)})| - 2|F(w_{(e)})| + e - 1 \\ &\leqslant |w_{(1)}| + 2|F(w_{(1)})| + e - 1. \end{aligned}$$

Comme la condition (2.4.i) donne $|F(w_{(1)})| = |w_0|$, on arrive à

$$|w_{(e)}| \leqslant |w_{(1)}| + 2|w_0| + e - 1.$$

La condition (2.4.iii) implique $|w_{(1)}| \leqslant |w|+2(h-1)+2|w_h|+|D(w_{(1)})|$. Ceci, à partir de la relation $|w| \leqslant |w_0|+h+|w_h|$, donne

$$|w_{(e)}| \leqslant 3|w| + e + |D(w_{(1)})| - 3.$$

Par construction, e est la longueur de u. Comme (2.4.ii) implique $|D(w_{(1)})| \leqslant 2$, nous trouvons

$$|w_{(e)}| \leqslant 3|w| + |u| - 1,$$

qui complète le cas $p \leqslant n-2$ en posant $w' = w_{(e)}$.

Maintenant supposons $p = n-1$. Alors u est le mot vide ε. Posons $w = w''\, a_{q-1,n-1}$ et

$$w' = w''\, d_{q-1,n-1}\, d_{q-1,n-2}^{-1}.$$

Le mot w' est clairement un $a_{n-1,n}$-mur adossé à $a_{q-1,n-1}$ et toutes les propriétés de complexité sont satisfaites. De plus, pour $q = n-1$ et $w \neq a_{n-2,n-1}$, le lemme III.3.2 (iii) implique que w'' se termine par $a_{t,n-1}$ pour un certain t, donc il est σ_{n-2}-positif. Ainsi le mot w' possède les propriétés désirées.

Finalement, supposons $p \neq n-1$, $q = n-1$ et $w \neq a_{n-2,n-1}$. Alors u n'est pas le mot vide. Par hypothèse, la dernière lettre de w est $a_{n-2,n-1}$, qui n'est pas une barrière. Ainsi le mot w_h n'est pas vide et sa dernière lettre est $a_{n-2,n-1}$. La relation (2.4.iv) implique alors que le mur $w_{(1)}$ est grand. La condition (2.7.iv) montre alors que le mur $w_{(k)}$ est grand pour tout k dans $\{1, \dots, e\}$, et, donc, que w' est un grand mur. Par définition d'un grand mur, w' peut être écrit $u\, d_{r,n-1}\, \widehat{w}\, d_{n-2,n-1}$. Le mot $u\, d_{r,n-1}\, \widehat{w}$ étant σ_{n-2}-positif, le mot w' a les propriétées annoncées.

La complexité en temps est une conséquence directe des lemmes 2.4 et 2.7, et le fait qu'une opération élémentaire de renversement est en $O(\log(n))$—une comparaison d'entiers compris entre 0 et n se fait en temps linéaire en $\log(n)$. □

Exemple 2.9. Soit w la $a_{3,7}$-échelle $a_{4,6}\, a_{1,4}\, a_{2,6}$ et u le mot $a_{3,7}$-dangereux $d_{5,6}^{-1}\, d_{3,6}^{-1}\, d_{3,6}^{-1}$. Le diagramme de renversement de $u\, w$ est donné à la figure 4.7.

On conclut cette section avec le résultat technique suivant qui sera utilisé à plusieurs reprises lors de la démonstration du théorème 3.15. Nous mentionnons ce résultat ici, car il est étroitement lié à la notion de mur.

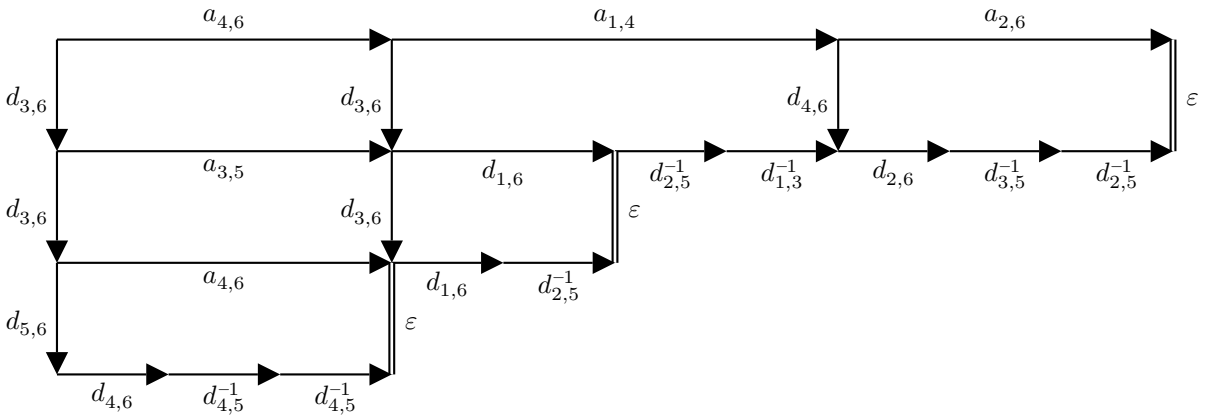


FIG. 4.7 : Renversement de $u\,w$ en un mur. Ici u est le mot $a_{3,7}$-dangereux $d_{5,6}^{-1}\,d_{3,6}^{-1}\,d_{3,6}^{-1}$ et w est la $a_{3,7}$-échelle $a_{4,6}\,a_{1,4}\,a_{2,6}$, qui est adossée à $a_{2,6}$. Avec les notations de la proposition 2.8, $w_{(1)}$ est le mot $a_{3,5}\,d_{1,6}\,d_{2,5}^{-1}\,d_{1,3}^{-1}\,d_{2,6}\,d_{3,5}^{-1}\,d_{2,5}^{-1}$: il peut être lu (de la gauche vers la droite) sur la troisième ligne à partir du bas. Ensuite $w_{(2)}$ est le mot $a_{4,6}\,d_{1,6}\,d_{2,5}^{-1}\,d_{2,5}^{-1}\,d_{1,3}^{-1}\,d_{2,6}\,d_{3,5}^{-1}\,d_{2,5}^{-1}$: il peut être lu sur la seconde ligne puis sur la troisième lorsque l'on rencontre l'arrête verticale étiqueté ε. Finalement $w_{(3)}$ est le mot $d_{4,6}\,d_{4,5}^{-1}\,d_{4,5}^{-1}\,d_{1,6}\,d_{2,5}^{-1}\,d_{2,5}^{-1}\,d_{1,3}^{-1}\,d_{2,6}\,d_{3,5}^{-1}\,d_{2,5}^{-1}$: il peut être lu sur la ligne du bas, puis sur la seconde et enfin sur la troisième. Le point est que nous avons trois lettres négatives $d_{\dots,6}$-au départ et que, à chaque étape, on se débarrasse de l'une d'entre elles, terminant avec un mot contenant seulement des lettres négatives de la forme $d_{\dots,q}^{-1}$ avec $q \leqslant 5$.

Lemme 2.10. *Supposons $n \geqslant 3$, et que*
– *$(w_b, \dots, w_1)$ est le ϕ_n-éclatement d'un mot tournant w, avec $b \geqslant 3$,*
– *u_b est un mot $w_b^{\#}$-dangereux,*
– *c est un entier dans $\{b, \dots, 3\}$.*
Alors il existe
– *un mot σ_{n-1}-nonnégatif w',*
– *un mot $w_c^{\#}$-dangereux u_c,*
tous les deux calculables en temps $O(\log(n)(|u_b||w| + |w|^2))$, et satisfaisant

$$d_{1,n}^{-b+3}\phi_n^{b-1}(u_b)\,\phi_n^{b-2}(w_{b-1})\dots w_1 \equiv w' \cdot d_{1,n}^{-c+3}\phi_n^{c-1}(u_c)\,\phi_n^{b-2}(w_{c-1})\dots w_1, \tag{4.18}$$

avec $|w'| \leqslant 3|w_{b-1}| + \dots + 3|w_c| + |u_b| - |u_c| - b + c$ et $|u_c| \leqslant |u_b| + b$.

Démonstration. L'idée est la suivante : en utilisant une induction sur k de b jusqu'à $c+1$, on calcule un mot σ_{n-1}-nonnégatif w'_{k-1} et un mot $w_k^{\#}$-dangereux u_{k-1} satisfaisant

$$d_{1,n}^{-k+1}\,\phi_n^{k-1}(u_k)\,\phi_n^{k-2}(w_{k-1}) \equiv\; w'_{k-1}\,d_{1,n}^{-k+2}\,\phi_n^{k-2}(u_{k-1}). \tag{4.19}$$

On pose alors $w' = w'_{b-1}\dots w'_c$.

Allons dans les détails. D'abord construisons les mots w'_k et u_k. Fixons k dans $\{b, \dots, c+1\}$ et supposons que u_k soit un mot $w_k^{\#}$-dangereux. Le corollaire III.3.11 garantit que w_{k-1} est une $\phi_n(w_k^{\#})$-échelle adossée à $w_{k-1}^{\#}$. Alors, par la proposition 2.8, le mot $\phi_n(u_k)\,w_{k-1}$ est équivalent au $\phi_n(w_k^{\#})$-mur v_{k-1} adossé à $w_{k-1}^{\#}$. Par définition d'un mur, nous avons

$$v_{k-1} = v'_{k-1}\,d_{p-1,n-1}\,u_{k-1},$$

où v'_{k-1} est un mot σ_{n-2}-nonnégatif, u_{k-1} est un mot $w_{k-1}^{\#}$-dangereux, $a_{p-1,n-1}$ étant la dernière lettre de w_{k-1}. Nous obtenons

$$d_{1,n}^{-k+1}\,\phi_n^{k-1}(u_k)\,\phi_n^{k-2}(w_{k-1}) \equiv d_{1,n}^{-k+1}\,\phi_n^{k-2}(v'_{k-1}\,d_{p-1,n-1}\,u_{k-1}).$$

On pousse les puissances de $d_{1,n}^{-1}$ du dernier mot entre $d_{p-1,n-1}$ et u_{k-1} :

$$d_{1,n}^{-k+1}\,\phi_n^{k-2}(v'_{k-1}\,d_{p-1,n-1}\,u_{k-1}) \equiv \phi_n(v'_{k-1}\,d_{p-1,n-1})\,d_{1,n}^{-k+1}\,\phi_n^{k-2}(u_{k-1}).$$

Par la relation (II.2.6), on a $\phi_n(d_{p-1,n-1})\,d_{1,n}^{-1} \equiv d_{1,p}^{-1}$. À la fin, nous obtenons

$$d_{1,n}^{-k+1}\,\phi_n^{k-1}(u)\,\phi_n^{k-2}(w_{k-1}) \equiv \phi_n(v'_{k-1})\,d_{1,p}^{-1}\,d_{1,n}^{-k+2}\,\phi_n^{k-2}(u'). \tag{4.20}$$

Posant $w'_{k-1} = \phi_n(v'_{k-1})\,d_{1,p}^{-1}$, la relation (4.20) implique (4.19). Par construction, w'_{k-1} est σ_{n-1}-nonnégatif et u_k est un mot $w_k^{\#}$-dangereux. Regroupant les relations (4.19) pour k compris entre b et $c+1$, nous obtenons la relation (4.18) pour $w' = w'_{b-1}\dots w'_c$. Par construction, w'_k est σ_{n-1}-nonnégatif pour tout k, donc w' est aussi σ_{n-1}-nonnégatif.

Il reste à établir le résultat de complexité. Pour chaque k de $\{b,\dots,c+1\}$, la condition (2.8.ii) implique

$$|v_{k-1}| \leqslant 3|w_{k-1}| + |u_k| - 1.$$

Ensuite, par construction de w'_{k-1}, nous avons

$$|w'_{k-1}| \leqslant 3|w_{k-1}| + |u_k| - |u_{k-1}| - 1.$$

On en déduit

$$|w'| = |w'_{b-1}\dots w'_c| \leqslant 3|w_{b-1}\dots w_c| + |u_b| - |u_c| - b + c.$$

Pour chaque valeur de k, la condition (2.8.i) implique $|u_k| \leqslant |u_{k+1}|+1$. On trouve alors

$$|u_k| \leqslant |u_b| + b - k,$$

donc $|u_k| \leqslant |u_b| + b$. Par la proposition 2.8, calculer u_k et v_k à partir de w_k et u_{k+1} requiert au plus $O(\log(n)|u_{k+1}||w| + 1)$ étapes de renversement. Donc, calculer w' et u_c à partir de u_b et le ϕ_n-éclatement de w demande au plus

$$O(\log(n)(|u_b| + b)|w| + b - c)$$

étapes. De la relation $b \leqslant |w| + 2$, nous déduisons que w' et u_c sont calculés à partir de u_b et le ϕ_n-éclatement w en au plus $O(\log(n)(|u_b||w| + |w|^2))$ étapes. □

3 Expression σ-définie quasi-géodésique

Dans cette section nous donnons une démonstration de la conjecture 0.1. Plus précisement nous établissons le résultat qui suit. Pour β dans B_n, on note $\|\beta\|_\sigma$ la longeur d'un plus court Σ_n-mot représentant β.

Théorème 3.1. *Toute tresse β à n brins admet une expression σ-définie en les lettres σ_i de longueur au plus $6(n-1)^2\|\beta\|_\sigma$.*

Pour cela nous allons construire, pour toute tresse β à n brins, un certain AD_n-mot σ-défini, noté $\mathrm{NF}_n(\beta)$, représentant β, c'est-à-dire, un mot en les lettres $a_{p,q}$ et $d_{p,q}$ qui, traduit en les σ_i, est soit σ-positif soit σ-négatif.

La construction du mot $\mathrm{NF}_n(\beta)$ demande deux étapes. La première, décrite à la section 3.1, consiste à étendre la forme normale tournante de la section III.2 à toutes les tresses de B_n en

rajoutant un dénominateur. Ce procédé est basé sur la structure de Garside du monoïde B_n^{+*} ; plus précisément sur le fait que B_n soit le groupe de fractions de B_n^{+*}.

La seconde étape part de la forme normale tournante de la tresse β considérée, et est décrite à la section 3.2. Le procédé se décompose en trois cas suivant la position relative de deux paramètres associés à la tresse β, à savoir la largeur du numérateur et l'exposant du dénominateur apparaissant dans la forme normale tournante de β. L'algorithme de renversement développé à la section 1 sera utilisé pour traiter le cas difficile, qui apparaît lorsque les deux paramètres introduits précédemment sont proches l'un de l'autre.

En particulier la démonstration du théorème 3.17 est algorithmique. Son analyse en complexité donne :

Théorème 3.2. *La complexité en temps de l'algorithme impliqué dans la démonstration du théorème 3.17 est quadratique : pour tout mot de tresse à n brins de longueur ℓ, le temps d'exécution de l'algorithme appartient à $O(\ell^2)$.*

3.1 Généralisation de la forme normale tournante

À ce stade, la forme normale n'est définie que sur le monoïde B_n^{+*}. Nous allons maintenant la définir sur B_n tout d'entier. Pour cela nous allons utiliser le fait que B_n soit le groupe de fractions de B_n^{+*}.

Proposition 3.3. *Toute tresse β peut être exprimée de manière unique sous la forme $d_{1,n}^{-t} w$ où t est un entier positif, w est un mot tournant, et où la tresse $\overline{w}$ n'est pas divisible à gauche par δ_n, sauf peut-être si t est nul.*

Démonstration. Par le corollaire II.3.20, le groupe B_n est le groupe de fractions de B_n^{+*}. Il existe donc un entier t tel que la tresse $\delta_n^t \beta$ appartienne au monoïde B_n^{+*}. Si t est positif, l'hypothèse de minimalité implique que δ_n n'est pas un diviseur à gauche de $\delta_n^t \beta$. Notons w la forme normale tournante de la tresse duale $\delta_n^{-t} \beta$. Le couple (t, w) est alors du type désiré—nous rappelons que le mot $d_{1,n}$ est un représentant de δ_n.

Supposons que (t', w') soit un autre couple avec les mêmes propriétés. Alors $\delta_n^{t'} \beta$ appartient à B_n^{+*}, ce qui implique $t' \geqslant t$. Si on a $t' > t$, l'hypothèse $\delta_n^{-t} \overline{w} = \delta_n^{-t'} \overline{w'}$ doit alors impliquer $\delta_n^{t'-t} \overline{w} = \overline{w'}$, et donc $\overline{w'}$ est divisible à gauche par δ_n, ce qui contredit $t' > 0$. On a donc $t' = t$, puis $w' = w$ par unicité de la forme normale tournante. □

Définition 3.4. Le AD_n-mot $d_{1,n}^{-t} w$ introduit dans la Proposition 3.3 est appelé *n-forme normale tournante* de la tresse β. On appelle *n-profondeur* de β, notée $\mathrm{dp}_n(\beta)$, le nombre t ; on appelle *n-largeur* de β, notée $\mathrm{br}_n(\beta)$, la n-largeur de w ; on appelle *n-longueur* de β, notée $|\beta|_n$, le nombre $t + |w|$, c'est-à-dire, la longueur du AD_n-mot $d_{1,n}^{-t} w$.

Par définition, la forme normale tournante d'une tresse de B_n est un AD-mot, c'est-à-dire, un mot en les lettres $a_{p,q}$ et les lettres $d_{p,q}$. La terminologie est cohérente car, pour β dans B_n^{+*}, la n-forme normale tournante que nous venons de décrire coïncide avec celle de la définition III.2.12 : en effet, une tresse β appartient à B_n^{+*} si et seulement si sa n-profondeur est 0.

À l'aide de la proposition 3.5 et de la structure de Garside de B_n^{+*}, nous vérifions facilement que la forme normale d'une tresse quelconque peut être calculée en temps quadratique. Pour β dans B_n, on note $\|\beta\|_a$ la longueur d'un plus court A_n-mot représentant β.

Proposition 3.5. *Pour toute tresse à n brins β, on a $|\beta|_n \leqslant (n-1)\, \|\beta\|_a$.*

Démonstration. Le cas $n = 2$ est trivial. Partant d'un Σ_2-mot, on le réduit librement à un mot de la forme σ_1^k en supprimant les facteurs $a_{1,2}a_{1,2}^{-1}$ et $a_{1,2}^{-1}a_{1,2}$. La forme normale tournante est $a_{1,2}^k$ dans le cas $k \geqslant 0$, et $d_{1,2}^k$ dans le cas $k < 0$, et est géodésique.

Supposons maintenant $n \geqslant 3$. Pour x une A_n-lettre notons $\alpha_n(x)$ un A_n^+-mot tel que δ_n soit équivalent à $\alpha_n(x)\, x$. Un tel mot existe car toute tresse $a_{p,q}$ est un simple de B_n^{+*} et donc un diviseur à droite de δ_n. Soit w un Σ_n-mot de tresse représentant la tresse β. Alors la forme normale tournante de β est obtenue de la manière suivante :

- Repérer les lettres négatives de w :

$$w = w_0 x_1^{-1} w_1 \dots w_{c-1} x_{c-1}^{-1} w_c;$$

- Poser $v = \phi_n^c(w_0)\, \phi_n^{c-1}(\alpha_n(x_1)\, w_1) \dots \phi_n(\alpha_n(x_{c-1})\, w_{c-1})\, \alpha_n(x_c)\, w_c$;

- Soit s le plus grand entier tel que δ_n^s divise à gauche $\overline{v}$ dans B_n^{+*}, et soit v' le A_n-mot positif satisfaisant $v \equiv \delta_n^s v'$;

- Si $s \geqslant c$ est vérifiée, poser $t = 0$ et $w'' = \delta_n^{s-c}\, v'$; sinon poser $t = c - s$ et $w'' = v'$.

- Soit w' la forme normale tournante de la tresse représentée par w''. Alors la forme normale tournante de β est $d_{1,n}^{-t}\, w'$.

En effet, la construction de α_n et la relation $\delta_n \equiv d_{1,n}$ impliquent

$$w \equiv w_0\, d_{1,n}^{-1}\, \alpha_n(x_1)\, w_1 \dots\, d_{1,n}^{-1}\, \alpha_n(x_{c-1})\, w_{c-1}\, d_{1,n}^{-1}\, \alpha_n(x_c)\, w_c$$

En poussant les lettres $d_{1,n}^{-1}$ à gauche, on obtient

$$w \equiv d_{1,n}^{-c}\, \phi_n^c(w_0)\, \phi_n^{c-1}(\alpha_n(x_1)\, w_1) \dots \phi_n(\alpha_n(x_{c-1})\, w_{c-1})\, \alpha_n(x_c)\, w_c = d_{1,n}^{-c}\, v.$$

Puis, en utilisant la relation $d_{1,n} \equiv \delta_n$ et la construction de w', nous obtenons $w \equiv d_{1,n}^{-t}\, w'$, où la tresse représentée par w' n'est pas divisible à gauche par $d_{1,n}$ sauf pour $t = 0$.

Pour la longueur, remplacer x_k^{-1} par $d_{1,n}^{-1}\, \alpha_n(x_k)$ la multiplie par au plus $n-1$. Appliquant le procédé sur un plus petit représentant de β vis-à-vis de la longueur en les A_n-lettres on a

$$|\beta|_n \leqslant (n-1)\|\beta\|_a.$$

□

Exemple 3.6. Considérons la tresse β représentée par le Σ_4-mot $\sigma_1\, \sigma_3^{-2}\, \sigma_2\, \sigma_3$. Nous utilisons les notations de la démonstration de la proposition 3.5. D'abord on pose

$$u = w_0\, \sigma_3^{-1}\, w_1\, \sigma_3^{-1}\, w_2 \text{ avec } w_0 = a_{1,2},\ w_1 = \varepsilon \text{ et } w_2 = a_{2,3}\, a_{3,4}.$$

Comme δ_4 est égale à $a_{1,2}a_{2,3}a_{3,4}$, on pose $\alpha_4(a_{3,4}) = a_{1,2}a_{2,3}$. On obtient donc

$$v = \phi_4^2(w_0)\, \phi_4(\alpha_4(a_{3,4})\, w_1)\, \alpha_4(a_{3,4})\, w_2 = a_{3,4}\, a_{2,3}\, a_{3,4}\, a_{1,2}\, a_{2,3}\, a_{2,3}\, a_{3,4}.$$

La puissance maximale de δ_4 qui divise à gauche la tresse représentée par v est 1 et on a

$$v \equiv \delta_4\, a_{2,3}\, a_{1,2}\, a_{2,3}\, a_{2,4}.$$

Ainsi on obtient $s = 1$ et $v' = a_{2,3}\, a_{1,2}\, a_{2,3}\, a_{2,4}$. Ici on a $c = 2$ et s vaut 1, nous posons donc $t = 1$ et $w'' = a_{2,3}\, a_{1,2}\, a_{2,3}\, a_{2,4}$. La forme normale tournante w' de $\overline{w''}$ s'avère être $a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}$. Donc, finalement, la forme normale tournante de β est

$$d_{1,4}^{-1}\, a_{1,2}\, a_{1,4}\, a_{2,3}\, a_{1,2}.$$

La 4-profondeur de β est donc 1, sa longueur est 5, et sa 4-largeur est 4, car nous avons vu à l'exemple III.2.22 que la 4-largeur de la tresse $a_{1,2}\,a_{1,4}\,a_{2,3}\,a_{1,2}$ est 4 : son ϕ_4-éclatement est

$$(a_{2,3}, a_{2,3}, 1, a_{2,3}\,a_{1,2}),$$

une suite de longueur 4.

En suivant la trame de la démonstration de la proposition, nous proposons l'algorithme suivant permettant de calculer la forme normale de n'importe quelle tresse de B_n.

Algorithme 7 (`FormeTournanteG`)**.**
Entrée : Un couple (n, w) où w est un A_n-mot
1. $\varepsilon \to v$; $0 \to t$;
2. `Pour` k de $|w|$ jusqu'à 1 `faire`
3. `Si` la lettre $w(k)$ est positive `faire`
4. `Phi(`n`,`t`,`$w(k)$`)` $\cdot\, v \to v$;
5. `Sinon faire`
6. `DivD(`n`,`δ_n`,`$w(k)$`)` $\to u$;
7. `Phi(`n`,`t`,`u`)` $\cdot\, v \to v$;
8. $t+1 \to t$;
9. `DivG(`n`,`δ_n`,`v`)` $\to v'$;
10. `Tant que` v' != $\otimes$ et $t \geqslant 0$ `faire`
11. $t-1 \to t$;
12. $v' \to v$;
13. `DivG(`n`,`δ_n`,`v`)` $\to v'$;
14. `FormeTournante(`v`)` $\to v$;
15. `Renvoyer` $d_{1,n}^{-t} v$;

Sortie : Un AD_n-mot

Proposition 3.7. *L'algorithme* `FormeTournanteG` *appliqué à* (n, w) *retourne en temps* $O(n^6|w|^2)$ *la* n*-forme normale tournante de* $\overline{w}$*.*

Démonstration. La ligne `4` est en $O(\log(n))$ et la ligne `6` est en $O(n)$. Comme la longueur de u est $(n-2)$, la ligne `7` est en $O(n\log(n))$. Les lignes `2` à `8` sont donc en $O(n\log(n)|w|)$. Au début de la ligne `9` le mot v est celui de la démonstration de la proposition 3.5 et est donc de longueur au plus $(n-2)|w|$. Les lignes `9` et `13` sont donc en $O(n|\delta_n||v|)$, c'est à dire, en $O(n^2|v|)$. Ainsi l'exécution des lignes `9` à `13` est en $O(n^2|v|^2)$, c'est à dire, en $O(n^2|w|^2)$. Par la proposition III.2.20, la ligne `14` est en $O(n^4|v|^2)$, c'est à dire en $O(n^6|w|^2)$. On obtient donc la complexité annoncée. □

3.2 Le cas facile

Partant de la forme normale tournante, nous allons maintenant définir pour toute tresse β de B_n un nouveau représentant distingué $\mathrm{NF}_n(\beta)$. Le mot $\mathrm{NF}_n(\beta)$ sera un AD_n-mot σ-défini.

La construction de $\mathrm{NF}_n(\beta)$ dépend de la position relative des paramètres $\mathrm{dp}_n(\beta)$ et $\mathrm{br}_n(\beta)$. Le premier cas, qui est très facile, a lieu lorsque $\mathrm{dp}_n(\beta)$ vaut 0, c'est-à-dire, lorsque la tresse β appartient à B_n^{+*}, ou lorsqu'on a $\mathrm{dp}_n(\beta) = |\beta|_n$, c'est-à-dire, lorsque β est une puissance négative de δ_n. Notons que ce cas est le seul possible pour B_2.

Définition 3.8. Supposons que β est une tresse de B_n vérifiant $\mathrm{dp}_n(\beta) = 0$ ou $\mathrm{dp}_n(\beta) = |\beta|_n$. On définit alors $\mathrm{NF}_n(\beta)$ comme étant la forme normale tournante de β.

Proposition 3.9. *Sous les hypothèses de la définition 3.8, le mot* $\mathrm{NF}_n(\beta)$ *est un représentant* σ*-défini de* β*, et sa longueur est au plus* $|\beta|_n$*. De plus, si* β *est spécifié par un* Σ_n*-mot de longueur* ℓ*, le mot* $\mathrm{NF}_n(\beta)$ *peut être calculé en temps* $O(n^6\ell^2)$*.*

Démonstration. Si $|\beta|_n$ est 0, alors β est la tresse triviale 1 et sa forme normale tournante est le mot vide ε. Si β est non triviale et de n-profondeur nulle, alors sa forme normale tournante est un A_n^+-mot, et donc, un mot σ-positif. Si β est non triviale et qu'on a $\mathrm{dp}_n(\beta) = |\beta|_n$, alors la forme normale tournante de β est $d_{1,n}^{-\mathrm{dp}_n(\beta)}$, qui est un mot σ_{n-1}-négatif. La complexité est évidente à partir de la proposition 3.7. □

Le second cas, qui est aussi facile, se produit lorsque la n-profondeur est grande. Pour un A_n^+-mot tournant w, nous rappelons que nous appelons ϕ_n-éclatement de w la suite de mots tournants représentant les entrées du ϕ_n-éclatement de la tresse représentée par w.

Définition 3.10. Supposons que β soit une tresse non triviale de B_n pour $n \geqslant 3$ satisfaisant

$$0 \neq \mathrm{dp}_n(\beta) > \mathrm{br}_n(\beta) - 2.$$

Soit $d_{1,n}^{-t}\, w$ la forme normale tournante de β et $(w_b, \dots, w_1)$ le ϕ_n-éclatement de w. Alors on pose

$$\mathrm{NF}_n(\beta) = d_{1,n}^{-t+b-1} \cdot w_b\, d_{1,n}^{-1} \cdot \dots \cdot w_2\, d_{1,n}^{-1} \cdot w_1.$$

Proposition 3.11. *Sous les hypothèses de la définition 3.10, le mot* $\mathrm{NF}_n(\beta)$ *est un représentant* σ_{n-1}*-négatif de* β*, et sa longueur est au plus* $|\beta|_n$*. De plus, si* β *est spécifiée par un* Σ_n*-mot de longueur* ℓ*, le mot* $\mathrm{NF}_n(\beta)$ *peut être calculé en temps* $O(n^6\ell^2)$*.*

Démonstration. D'abord, montrons que $\mathrm{NF}_n(\beta)$ est un représentant de β. Notons $d_{1,n}^{-t}\, w$ la forme normale tournante de β et $(w_b, \dots, w_1)$ le ϕ_n-éclatement de w. On a

$$d_{1,n}^{-t}\, w = d_{1,n}^{-t} \cdot \phi_n^{b-1}(w_b) \cdot \dots \cdot \phi_n(w_2) \cdot w_1. \tag{4.21}$$

En poussant $(b-1)$ puissances de $d_{1,n}$ à droite dans (4.21) et en les intercalant entre les facteurs w_k, nous obtenons

$$\begin{aligned} d_{1,n}^{-t}\, w &= d_{1,n}^{-t} \cdot \phi_n^{b-1}(w_b) \cdot \dots \cdot \phi_n(w_2) \cdot w_1 \\ &= d_{1,n}^{-t+b-1} \cdot d_{1,n}^{-b+1} \cdot \phi_n^{b-1}(w_b) \cdot \dots \cdot \phi_n(w_2) \cdot w_1 \\ &\equiv d_{1,n}^{-t+b-1} \cdot w_b \cdot d_{1,n}^{-1} \cdot d_{1,n}^{-b+2} \cdot \dots \cdot \phi_n(w_2) \cdot w_1 \\ &\equiv \dots \equiv d_{1,n}^{-t+b-1} \cdot w_b \cdot d_{1,n}^{-1} \cdot \dots \cdot w_2 \cdot d_{1,n}^{-1} \cdot w_1 = \mathrm{NF}_n(\beta). \end{aligned}$$

Ensuite, exactement $\mathrm{dp}_n(\beta)$ puissances de $d_{1,n}^{-1}$ apparaissent dans $\mathrm{NF}_n(\beta)$. Donc, comme la n-profondeur $\mathrm{dp}_n(\beta)$ est non nulle, au moins un facteur $d_{1,n}^{-1}$ apparaît dans $\mathrm{NF}_n(\beta)$. Les mots w_k intermédiaires ne contenant pas de lettre $a_{p,n}$, le mot $\mathrm{NF}_n(\beta)$ est σ_{n-1}-négatif.

Pour le résultat sur la longueur, nous trouvons

$$\begin{aligned} |\mathrm{NF}_n(\beta)| &= t - b + 1 + |w_b| + 1 + \dots + |w_2| + 1 + |w_1| \\ &= t - b + 1 + |w| + b - 1 = |d_{1,n}^{-t}\, w'| = |\beta|_n. \end{aligned}$$

Finalement, supposons que β est spécifié par un Σ_n-mot de longueur ℓ. Alors, par la proposition 3.7, on peut calculer la forme normale tournante de la tresse β en au plus $O(n^6\ell^2)$ étapes. Par le lemme III.2.21, calculer le ϕ_n-éclatement de w peut être fait en $O(|w|)$ étapes. Donc, le mot $\mathrm{NF}_n(\beta)$ peut être calculé en temps $O(n^6\ell^2)$. □

3.3 Le cas difficile

Nous n'avons pas encore traité le cas de la tresse β de profondeur non nulle avec

$$\mathrm{dp}_n(\beta) \leqslant \mathrm{br}_n(\beta) - 2.$$

C'est le cas difficile. Dans ce cas, il est impossible de prédire directement si la tresse β est σ-positive ou bien σ-négative ou même triviale, et c'est le point où nous allons utiliser la notion d'échelle et l'algorithme de renversement.

Définition 3.12. Supposons que β soit une tresse non triviale de B_n pour $n \geqslant 3$ satisfaisant $\mathrm{dp}_n(\beta) \neq 0$ et $\mathrm{dp}_n(\beta) \leqslant \mathrm{br}_n(\beta)-2$. Notons $d_{1,n}^{-t}\, w$ la forme normale tournante de β, et $(w_b, \dots, w_1)$ le ϕ_n-éclatement de w. Posons $w_{t+2} = w'_{t+2}\, a_{p-1,n-1}$ et

$$v = \phi_n^{b-1-t}(w_b) \dots \phi_n^2(w_{t+3})\ \phi_n(w'_{t+2})\ d_{1,p}^{-1}, \quad u_{t+2} = d_{p-1,n-2}^{-1}.$$

Cas 1 : $w_2 \neq \varepsilon$. Alors on pose

$$\mathrm{NF}_n(\beta) = v\, w''\, \phi_n(w'_2)\, w_1,$$

où w'' et u_3 sont les mots produits par le lemme 2.10 appliqué à la suite $(w_{t+2}, \dots, w_1)$, le mot u_{t+2} et l'entier 3, et où w'_2 est le mot produit par la proposition 2.8 appliquée aux mots w_2 et $\phi_n(u_3)$;
Cas 2 : $w_2 = \varepsilon$, $w_3 = \dots = w_{k-1} = a_{n-2,n-1}$ et $w_k \neq a_{n-2,n-1}$ pour un certain $k \leqslant t+1$. Alors, on pose

$$\mathrm{NF}_n(\beta) = v\, w''\, \phi_n(w'_k)\, d_{1,n-1}^{-c+2}\, w_1,$$

où w'' et u_{k+1} sont les mots donnés par le lemme 2.10 appliqué à la suite $(w_{t+2}, \dots, w_1)$, au mot u_{t+2} et à l'entier $k+1$, et où $w'_k\, a_{n-2,n-1}$ est le mot produit par la proposition 2.8 appliquée aux mots w_k et $\phi_n(u_{k+1})$;
Cas 3 : $w_2 = \varepsilon$, $w_3 = \dots = w_{t+1} = a_{n-2,n-1}$ et $v \neq d_{1,n-1}^{-1}$. Alors on pose

$$\mathrm{NF}_n(\beta) = v\, d_{1,n-1}^{-t+1}\, w_1;$$

Cas 4 : $w_2 = \varepsilon$, $w_3 = \dots = w_{t+1} = a_{n-2,n-1}$ et $v = d_{1,n-1}^{-1}$. Alors on pose

$$\mathrm{NF}_n(\beta) = \mathrm{NF}_{n-1}(\delta_{n-1}^{-t}\, \overline{w}_1).$$

Proposition 3.13. *Sous les hypothèses de la définition 3.12, le mot* $\mathrm{NF}_n(\beta)$ *est un représentant* σ*-défini (non* σ_{n-1}*-négatif) de* β*, et sa longueur est au plus* $3\,|\beta|_n$*. De plus, si* β *est spécifiée par un* Σ_n*-mot de longueur* ℓ*, le mot* $\mathrm{NF}_n(\beta)$ *peut être calculé en temps* $O(n^6\ell^2)$*.*

Démonstration. On utilise les notations de la définition 3.12. Montrons que l'équivalence suivante est satisfaite :

$$d_{1,n}^{-t}\, w \equiv v\, d_{1,n}^{-t+1}\, \phi_n^{t+1}(u_{t+2})\, \phi_n^t(w_{t+1}) \dots \phi_n(w_2)\, w_1. \tag{4.22}$$

En effet, comme la suite $(w_b, \dots, w_1)$ est le ϕ_n-éclatement de w, on a

$$d_{1,n}^{-t}\, w = d_{1,n}^{-t}\, \phi_n^{b-1}(w_b) \dots \phi_n^{t+1}(w_{t+2}) \dots \phi_n(w_2)\, w_1. \tag{4.23}$$

Par construction, w_{t+2} vaut $w'_{t+2}\, a_{p-1,n-1}$. La relation (II.2.5) implique $a_{p-1,n-1} \equiv d_{p-1,n-1}\, u_{t+2}$, donc $w_{t+2} \equiv w'_{t+2}\, d_{p-1,n-1}\, u_{t+2}$. Alors, le mot $d_{1,n}^{-t}\, w$ est équivalent à

$$d_{1,n}^{-t}\, \phi_n^{b-1}(w_b) ... \, \phi_n^{t+1}(w'_{t+2}\, d_{p-1,n-1})\, \phi_n^{t+1}(u_{t+2})\, \phi_n^t(w_{t+1}) \, ... \, \phi_n(w_2)\, w_1. \tag{4.24}$$

On pousse les facteurs $d_{1,n}^{-t}$ apparaissant dans (4.24) vers la droite, jusqu'à ce qu'ils arrivent à gauche du facteur $\phi_n^{t+1}(u_{t+2})$. De cette manière, nous obtenons

$$d_{1,n}^{-t}\, w \equiv \phi_n^{b-t-1}(w_b) ... \, \phi_n(w'_{t+2}\, d_{p-1,n-1})\; d_{1,n}^{-t}\, \phi_n^{t+1}(u_{t+2})\, \phi_n^t(w_{t+1}) \, ... \, \phi_n(w_2)\, w_1.$$

Les relations (II.2.6) et (1.8.i) impliquent $\phi_n(d_{p-1,n-1})\, d_{1,n}^{-t} \equiv d_{1,p}^{-1}$. En substituant la dernière valeur dans la relation ci-dessus, nous obtenons (4.22).

Ensuite, par construction, le mot v est σ_{n-1}-nonnégatif, et sa longueur satisfait

$$|v| = |w_b| + ... + |w_{t+2}|. \tag{4.25}$$

Pour aller plus loin, nous considérons les quatre cas de la définition 3.12 séparément. Dans les trois premiers cas, nous allons montrer que le mot $\mathrm{NF}_n(\beta)$ est σ_{n-1}-positif ; dans le quatrième cas, nous allons établir que $\mathrm{NF}_n(\beta)$ est σ-défini en utilisant une induction sur n et en utilisant dans certains sous-cas les propositions 3.9 et 3.11.

Cas 1. D'abord, $\mathrm{NF}_n(\beta)$est équivalent à $d_{1,n}^{-t} w$. En effet, le lemme 2.10 implique

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, \phi_n^2(u_3)\, \phi_n(w_2)\, w_1,$$

tandis que la proposition 2.8 implique $\phi_n(u_3)\, w_2 \equiv w'_2$. Nous déduisons

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, \phi_n(w'_2)\, w_1 = \mathrm{NF}_n(\beta).$$

Ensuite, par construction, w'_2 est un mur adossé à $w_2^{\#}$, donc, par définition, il est σ_{n-2}-positif. Il s'ensuit que $\phi_n(w'_2)$ est σ_{n-1}-positif. Comme les mots v, w'' et w_1 sont σ_{n-1}-nonnégatifs, le mot $\mathrm{NF}_n(\beta)$ est σ_{n-1}-positif.

Pour la longueur, le lemme 2.10 et la proposition 2.8 impliquent

$$|w''| \leqslant 3|w_{t+1}| + ... + 3|w_3| - |u_3| - t + 2, \quad |w'_2| \leqslant 3|w_2| + |u_3| - 1.$$

Regroupant ces valeurs avec (4.25), et $t > 0$, nous obtenons $|\mathrm{NF}_n(\beta)| \leqslant 3|w|$.

Cas 2. D'abord, observons que la dernière lettre du A_{n-1}^+-mot w_k doit être $a_{n-2,n-1}$: ceci est une conséquence du corollaire III.3.7 car, par construction de k, le mot w_{k-1} est soit le mot vide ε soit se termine par la lettre $a_{n-2,n-1}$.

Maintenant, vérifions que $\mathrm{NF}_n(\beta)$ est équivalent à $d_{1,n}^{-t} w$. Par le lemme 2.10, on a

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, d_{1,n}^{-k+2}\, \phi_n^k(u_{k+1})\, \phi_n^{k-1}(w_k)\, \phi_n^{k-2}(a_{n-2,n-1}) ... \, \phi_n^2(a_{n-2,n-1})\, w_1.$$

La proposition 2.8 garantissant que w'_k est un $\phi_n(w_{k+1}^{\#})$-mur satisfaisant

$$\phi_n(u_{k+1})\, w_k \equiv w'_k\, a_{n-2,n-1},$$

nous obtenons

$$d_{1,n}^{-t}\, w \;\equiv v\, w''\, d_{1,n}^{-k+2}\, \phi_n^{k-1}(w'_k)\, \phi_n^{k-1}(a_{n-2,n-1}) \, ... \, \phi_n^2(a_{n-2,n-1})\, w_1. \tag{4.26}$$

En poussant les puissances négatives de $d_{1,n}$ apparaissant dans (4.26) vers la droite et en les intercalant entre les $\phi_n^{\cdot}(a_{n-2,n-1})$, nous obtenons

$$\begin{aligned} d_{1,n}^{-t}\, w &\equiv v\, w''\, \phi_n(w'_k)\, d_{1,n}^{-k+2}\, \phi_n^{k-1}(a_{n-2,n-1}) \dots \phi_n^2(a_{n-2,n-1})\, w_1 \\ &\equiv v\, w''\, \phi_n(w'_k)\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, d_{1,n}^{-k+3} \dots \phi_n^2(a_{n-2,n-1})\, w_1 \\ &\equiv \ \dots \ \equiv v\, w''\, \phi_n(w'_k)\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \dots \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, w_1. \end{aligned}$$

Alors, l'équivalence $\phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \equiv d_{1,n-1}^{-1}$ implique

$$d_{1,n}^{-t}\, w \equiv v\, w''\, \phi_n(w'_k)\, d_{1,n-1}^{-k+2}\, w_1 = \mathrm{NF}_n(\beta).$$

Ensuite, par construction, le mot w'_k est un $\phi_n(w_{k+1}^{\#})$-mur, donc, par définition, il est σ_{n-2}-positif. Ainsi $\phi_n(w'_k)$ est σ_{n-1}-positif. Comme les mots v, w'', et $d_{1,n-1}^{-k+2}\, w_1$ sont σ_{n-1}-nonnégatifs, le mot $\mathrm{NF}_n(\beta)$ est σ_{n-1}-positif.

Pour le résultat sur la longueur, le lemme 2.10 et la proposition 2.8 impliquent

$$|w''| \leqslant 3|w_{t+1}| + \dots + 3|w_3| - |u_{k+1}| - t + 2, \quad |w'_k\, a_{n-2,n-1}| \leqslant 3|w_k| + |u_{k+1}| - 1.$$

En regroupant ces valeurs avec (4.25) et l'hypothèse $t > 0$, on obtient $|\mathrm{NF}_n(\beta)| \leqslant 3|w|$.

Cas 3. Comme dans le cas 2, on observe que la dernière lettre de w_{t+2} est $a_{n-2,n-1}$, ce qui est une conséquence du corollaire III.3.7, car w_{t+1} est soit le mot vide ε soit $a_{n-2,n-1}$.

Vérifions que $\mathrm{NF}_n(\beta)$ est équivalent à $d_{1,n}^{-t}\, w$. Comme la dernière lettre de w_{t+2} est $a_{n-2,n-1}$, le mot u_{t+2} est vide. Nous trouvons alors

$$d_{1,n}^{-t}\, w \ \equiv v\, d_{1,n}^{-t+1}\, \phi_n^t(a_{n-2,n-1}) \dots \phi_n^2(a_{n-2,n-1})\, \phi_n(\varepsilon)\, w_1. \tag{4.27}$$

En poussant encore les puissances négatives de $d_{1,n}$ intervenant dans (4.27) vers la droite et en les distribuant entre les $\phi_n^{\cdot}(a_{n-2,n-1})$, on obtient

$$\begin{aligned} d_{1,n}^{-t}\, w &\equiv v\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, d_{1,n}^{-t+2}\, \phi_n^{t-1}(a_{n-2,n-1}) \dots \phi_n^2(a_{n-2,n-1})\, w_1 \\ &\equiv \ \dots \ \equiv v\, \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \dots \phi_n(a_{n-2,n-1})\, d_{1,n}^{-1}\, w_1. \end{aligned}$$

Alors, la relation $\phi_n(a_{n-2,n-1})\, d_{1,n}^{-1} \equiv d_{1,n-1}^{-1}$ implique

$$d_{1,n}^{-t}\, w \equiv v\, d_{1,n-1}^{-t+1}\, w_1 = \mathrm{NF}_n(\beta)$$

Maintenant, vérifions que $\mathrm{NF}_n(\beta)$ est σ_{n-1}-positif. La dernière lettre de w_{t+2} étant $a_{n-2,n-1}$, on a la relation

$$v = \phi_n^{b-1-t}(w_b) \dots \phi_n^2(w_{t+3})\ \phi_n(w''_{t+2})\ d_{1,n-1}^{-1}$$

Par le lemme III.3.2, si le mot w'_{t+2} est non vide, il se termine par une lettre de la forme $a_{\cdot,n-1}$. Le mot v est donc σ_{n-1}-positif. Supposons que w'_{t+2} soit le mot vide et qu'on ait $t \leqslant b-3$. Comme le mot w_{t+2} est $a_{n-2,n-1}$, le corollaire III.3.7 implique que w_{t+3} se termine par $a_{n-2,n-1}$. Ainsi, le mot v se termine par $\phi_n^2(a_{n-2,n-1})\, d_{1,n-1}^{-1}$, qui est $a_{1,n}\, d_{1,n-1}^{-1}$. Le mot v est donc σ_{n-1}-positif.

La relation (4.25) implique directement $|\mathrm{NF}_n(\beta)| = |w|$.

Cas 4. Par construction, on a $v = d_{1,n-1}^{-1}$. La même analyse que celle faite dans le cas 3 donne la relation $t = b-2$ et

$$d_{1,n}^{-t}\, w \equiv d_{1,n-1}^{-t}\, w_1.$$

L'hypothèse d'induction accompagnée des propositions 3.9 et 3.11 établit

$$d_{1,n-1}^{-t}\, w_1 \equiv \mathrm{NF}_{n-1}(\delta_{n-1}^{-t}\, \overline{w_1}),$$

donc $d_{1,n}^{-t}\, w \equiv \mathrm{NF}_n(\beta)$ par définition.

Toujours grâce à l'hypothèse d'induction et les propositions 3.9 et 3.11, nous obtenons

$$|\mathrm{NF}_n(\beta)| = |\mathrm{NF}_{n-1}(\delta_{n-1}^{-t}\, \overline{w_1})| \leqslant 3|\delta_{n-1}^{-t}\, \overline{w_1}|_{n-1}.$$

Par définition, on a

$$|\beta|_n = t + |w_b| + \ldots + |w_1|,$$

et $|\delta_{n-1}^{-t}\, \overline{w_1}|_{n-1} \leqslant t + |w_1|$, donc $|\delta_{n-1}^{-t}\, \overline{w_1}|_{n-1} \leqslant |\beta|_n$. Ainsi nous obtenons $|\mathrm{NF}_n(\beta)| \leqslant 3|\beta|_n$.

Tous les cas ont été considérés et il ne reste plus qu'à établir la complexité en temps. Par la proposition 3.7 et le lemme III.2.21, la forme normale tournante de β et le ϕ_n-éclatement de w peuvent être calculés en temps $O(n^6\ell^2)$. Dans les cas 1 et 2, le lemme 2.10 est utilisé une fois sur $(w_{t+2}, \ldots, w_1)$ et u_{t+2} avec un coût en $O(\log(n)(|u_{t+2}|\ell + \ell^2))$. De plus, la proposition 2.8 est utilisée au plus une fois sur $\phi_n(u_{k+1})$ et w_k, avec un coût en $O(\log(n)(|u_{k+1}|\ell + 1))$. Le lemme 2.10 garantit

$$|u_{k+1}| \leqslant |u_{k+1}| + t + 1 - c,$$

c'est-à-dire, $|u_{t+2}| \leqslant t$ et donc $|u_{t+1}| \leqslant \ell$. Le coût de l'appel à la proposition 2.8 est donc au plus $O(\log(n)\ell^2)$. Les autres opérations des cas 1, 2, et 3 nécessitent $O(\log(n)\ell)$ étapes et, donc, le coût total du calcul de $\mathrm{NF}_n(\beta)$ est $O(n^6\ell^2)$ dans ces cas. Le résultat est similaire pour le cas 4, en utilisant l'hypothèse d'induction ainsi que les propositions 3.9 et 3.11 et le fait que le mot w_1 est déjà sous forme normale. □

3.4 On recolle les morceaux

À l'aide des mots σ-définis $\mathrm{NF}_n(\beta)$ construits aux sections 3.2 et 3.3, nous sommes maintenant prêts à démontrer les théorèmes 3.17 et 3.18. Remarquons d'abord que les mots $\mathrm{NF}_n(\beta)$ ne dépendent pas réellement de l'indice n.

Lemme 3.14. *Si β appartient à B_{n-1}, les mots $\mathrm{NF}_n(\beta)$ et $\mathrm{NF}_{n-1}(\beta)$ coïncident.*

Démonstration. Une simple vérification montre que, si β appartient à B_{n-1}, alors ou bien la n-largeur de β est nulle (si β appartient à B_{n-1}^{+*}), ou bien nous sommes dans le cas 4 de la définition 3.12. Dans les deux cas, la définition de $\mathrm{NF}_n(\beta)$ implique $\mathrm{NF}_n(\beta) = \mathrm{NF}_{n-1}(\beta)$. □

Donc, à partir de maintenant, nous pouvons retirer l'indice n et écrire $\mathrm{NF}(\beta)$ sans ambiguïté. Le principal résultat, duquel les théorèmes 3.17 et 3.18 sont des conséquence,s est le suivant.

Théorème 3.15. *Pour toute tresse β de B_n, le AD_n-mot $\mathrm{NF}(\beta)$ est un représentant σ-défini de β, et sa longueur est au plus $3\,(n-1)\,\|\beta\|_a$. De plus, si β est spécifiée par un A_n-mot de longueur ℓ, le mot $\mathrm{NF}(\beta)$ peut être calculé en temps $O(n^6\ell^2)$.*

Démonstration. Pour $n = 2$, tout est évident, supposons donc $n \geqslant 3$. D'après la proposition 3.3, ainsi que les propositions 3.9, 3.11, et 3.13, le mot $\mathrm{NF}(\beta)$ est, dans tous les cas, un représentant σ-défini de β, et sa longueur est au plus $3|\beta|_n$. D'un autre côté, la proposition 3.5 implique la relation $|\beta|_n \leqslant (n-1)\|\beta\|_\sigma$. Nous obtenons ainsi la majoration désirée :

$$|\mathrm{NF}(\beta)| \leqslant 3(n-1)\|\beta\|_\sigma. \tag{4.28}$$

Finalement, les complexités en temps des propositions 3.5, 3.9, 3.11, et 3.13 montrent, que dans tous les cas, $\mathrm{NF}(\beta)$ peut être calculé en temps $O(n^6\ell^2)$ lorsque la tresse β est spécifiée par un A_n-mot de longueur ℓ. □

Comme conséquence immédiate du théorème 3.15 nous avons :

Théorème 3.16. *Toute tresse β à n brins admet une expression σ-définie en les lettres $a_{p,q}$ de longueur au plus $3(n-1)\|\beta\|_a$.*

Si maintenant nous considérons l'alphabet des lettres σ_i nous obtenons :

Théorème 3.17. *Toute tresse β à n brins admet une expression σ-définie en les lettres σ_i de longueur au plus $6(n-1)^2\|\beta\|_\sigma$.*

Démonstration. Soit $\underline{\mathrm{NF}}(\beta)$ la traduction du AD_n-mot $\mathrm{NF}(\beta)$ en un Σ_n-mot. Les formules données en (4.1) montrent que la traduction d'une A_n-lettre ou d'une D_n-lettre a une longueur au plus $2n-3$. Ainsi la relation (4.28) implique $|\underline{\mathrm{NF}}(\beta)| \leqslant 6(n-1)^2\|\beta\|_\sigma$. □

Le résultat de complexité en temps du théorème 3.15 donne

Théorème 3.18. *La complexité en temps de l'algorithme impliqué dans la démonstration des théorèmes 3.16 et 3.17 est quadratique en la longueur du mot d'entrée : pour tout mot de tresse à n brins de longueur ℓ, le temps d'exécution de l'algorithme appartient à $O(n^6\ell^2)$.*

Démonstration. La traduction d'un A_n-mot de longueur ℓ en Σ_n-mot à un coût en $O(n\ell)$. On conclut par le théorème 3.15. □

Nous donnons pas plus de détails sur l'algorithme étudié au théorème 3.18, notamment parce que nous allons en introduire un plus simple à la section suivante et avec une meilleure complexité. Néanmoins, donnons un exemple concret de la construction précédente.

Exemple 3.19. Considérons encore la tresse $\beta = \sigma_1\,\sigma_3^{-2}\,\sigma_2\,\sigma_3$ de l'exemple 3.6. Nous avons déjà vu que sa forme normale tournante est le AD_n-mot

$$d_{1,4}^{-1}\,a_{1,2}\,a_{1,4}\,a_{2,3}\,a_{1,2}.$$

D'après l'exemple III.2.22, le ϕ_4-éclatement de $a_{1,2}a_{1,4}a_{2,3}a_{1,2}$ est $(w_4, ..., w_1)$, avec

$$w_4 = a_{2,3}, \quad w_3 = a_{2,3}, \quad w_2 = \varepsilon, \quad \text{et} \quad w_1 = a_{2,3}a_{1,2}.$$

On a donc $\mathrm{dp}_4(\beta) = 1$ et $\mathrm{br}_4(\beta) = 4$, donc $\mathrm{dp}_4(\beta) \leqslant \mathrm{br}_4(\beta) - 2$, et nous nous trouvons dans le cas difficile. Avec les notations de la définition 3.12, on a $t = 1$ et $w_3 = \varepsilon \cdot a_{2,3}$, nous commençons donc par poser $w_3' = \varepsilon$, $p = 3$, $v = \phi_4^2(w_4)\,\phi_4(w_3')\,d_{1,p}^{-1}$, et $u_3 = d_{p-1,2}^{-1}$, c'est-à-dire, dans notre cas, $v = a_{1,4}\,d_{1,3}^{-1}$ et $u_3 = \varepsilon$. Alors, comme on a $w_2 = \varepsilon$, $w_3 = a_{2,3}$ et $v \neq d_{1,3}^{-1}$, nous sommes dans le cas 3 de la définition 3.12. En suivant ce dernier, on définit $\mathrm{NF}(\beta) = v\,d_{1,3}^{0}\,w_1$, c'est-à-dire, $\mathrm{NF}(\beta) = a_{1,4}\,d_{1,3}^{-1}\,a_{2,3}\,a_{1,2}$. Cet AD_4-mot est σ_3-positif : en effet sa σ-traduction est le Σ_4-mot

$$\underline{\mathrm{NF}}(\beta) = \sigma_1\,\sigma_2\,\sigma_3\,\sigma_2^{-1}\,\sigma_1^{-1}\,\sigma_2^{-1}\,\sigma_1^{-1}\,\sigma_2\,\sigma_1$$

qui contient un σ_3, pas de σ_3^{-1}, et pas de $\sigma_i^{\pm 1}$ avec $i \geqslant 4$.

Dans le cas très simple de l'exemple 3.19, l'algorithme de renversement n'est pas utilisé. Cependant, des phénomènes compliqués peuvent apparaître en général, en particulier lorsque le nombre de brins est au moins 5, qui correspond à la plus petite valeur pour laquelle il existe une échelle avec plus d'une barre. Les exemples illustrant réellement l'algorithme dans toute sa complexité, typiquement ceux demandant plus d'une étape de renversement, reposent sur des mots trop longs pour être donnés ici.

3.5 Un algorithme plus simple

Dans cette section, on donne un algorithme plus simple permettant d'obtenir des expressions σ-définies quasi-géodésiques. L'idée de cet algorithme est de toujours se ramener au cas facile et nous a été suggérée par L. Paris.

Prenons une tresse β de B_n. La première étape consiste à calculer le plus petit m tel que β soit une tresse de B_m. De ce fait β est soit σ_{m-1}-positive ou bien σ_{m-1}-négative, ce qui revient à dire que β ou son inverse est σ_{m-1}-négative. Pour calculer l'entier m, on peut utiliser la forme normale de Garside–Thurston de β qui ne dépend que de β et pas du groupe de tresse dans lequel nous la voyons.

Proposition 3.20 ([DP99])**.** *Toute tresse β de B_n^{+*} admet une unique décomposition $\beta'^{-1}\beta''$ où β', β'' appartiennent à B_n^{+*} tel que le pgcd à gauche de β' et β'' soit trivial. De plus si β est représentée par un A_n-mot w alors β' et β'' sont représentée par des A_n^+-mots u' et v' vérifiant*

$$w \curvearrowright_d u v^{-1} \curvearrowright_g u'^{-1} v'.$$

La décomposition $\beta'^{-1}\beta''$ introduite dans la proposition 3.20 est la forme normale dite de *Garside–Thurston* de la tresse β.

On définit l'indice d'un A_n-mot comme étant l'entier maximal q tel que w contient une lettre $a_{p,q}^{\pm 1}$. L'indice d'une tresse β est le plus petit indice d'un A_n-mot représentant β.

L'algorithme suivant permet de calculer l'indice d'une tresse à l'aide du retournement.

Algorithme 8 (`IndiceRet`)**.**
Entrée : Un A_n-mot w
1. `RevD(`w`)` $\rightarrow w'$;
2. `RevG(`w'`)` $\rightarrow w''$;
3. $2 \rightarrow i$;
4. `Pour` k de 1 jusqu'à $|w''|$ `faire`
5. $\quad w''[k] \rightarrow a_{p,q}$;
6. $\quad$ `Si` $q > i$ `faire`
7. $\quad\quad q \rightarrow i$;
8. `Renvoyer` i;

Sortie : Un entier

Proposition 3.21. *L'algorithme* `IndiceRet` *appliqué à un A_n-mot w de longueur ℓ retourne l'indice de $\overline{w}$ en temps $O(\ell^2)$.*

Démonstration. Soit $\beta'^{-1}\beta''$ la forme normale de Garside–Thurston de $\overline{w}$. D'après la proposition 3.20 la partie négative du mot w'' représente la tresse β' tandis que sa partie positive représente la tresse β''. L'indice de w'' est alors celui de la tresse β. La complexité en temps est une conséquence directe du corollaire II.3.26. □

Comme dans le cas de l'algorithme `DivDRet` la complexité en temps en fonction du nombre de brins n de l'algorithme `IndiceRet` n'est pas bonne.

Cependant, il existe un autre algorithme permettant de cacluler la forme normale de Garside–Thurston avec une bonne complexité en fonction du nombre de brins.

Proposition 3.22. (D.B.A. Epstein et al, [ECH+92]) *Pour w un A_n^+-mot, il existe un algorithme permettant de calculer la forme normale de Garside–Thurston de $\overline{w}$ en temps $O(K \cdot |w|^2)$ où K est la compléxité en temps d'un algorithme calculant le pgcd de deux simples de B_n^{+*}.*

À partir des propositions 3.22 et III.2.16, on construit, comme pour `IndiceRet`, un algorithme `Indice` permettant de calculer l'indice d'une tresse dont la complexité est donné par :

Proposition 3.23. *L'algorithme* `Indice` *appliqué à un A_n^+-mot w retourne l'indice de la tresse $\overline{w}$ en temps $O(n \cdot |w|^2)$.*

Nous pouvons maintenant définir un algorithme simple permettant, pour une tresse donnée, de trouver un représentant σ-défini.

Algorithme 9 (`SigmaDef`)**.**

Entrée : Un A_n-mot w

1. $1 \to e$;
2. `Indice`$(w) \to m$;
3. `FormeTournanteG`$(n, w^e) \to \delta_n^{-t} u$;
4. `Si` $t = 0$ ou $n = 2$ `faire`
5. `Renvoyer` $(\delta_n^{-t} u)^e$;
6. `Eclatement`$(n, u) \to (u_b, \dots, u_1)$;
7. `Si` $t \geqslant b-1$ `faire`
8. `Renvoyer` $(\delta_n^{-t+b-1}\, u_b\, \delta_n^{-1}\, u_{b-1}\, \delta_n^{-1} \dots\, u_2\, \delta_n^{-1}\, u_1)^e$;
9. $-1 \to e$;
10. `Goto ligne` 3;

Sortie : Un A_n-mot

Théorème 3.24. *L'algorithme* `SigmaDef` *se termine et retourne en temps $O(n^6 \cdot |w|^2)$ un mot σ-défini w' équivaeant à w avec $|w'| \leqslant (n-1)^2 \cdot \|\overline{w}\|_a$.*

Démonstration. On utilise l'algorithme `Indice` pour calculer l'indice m de la tresse $\overline{w}$. En particulier la tresse $\overline{w}$ est soit σ_{m-1}-positive soit σ_{m-1}-négative.

Ensuite, on utilise l'algorithme `FormeTournanteG` pour calculer la forme normale tournante $d_{1,m}^{-t} u$ de la tresse $\overline{w}$. Par la proposition 3.5, on a $|d_{1,m}^{-t} u| \leqslant (m-1)\|\overline{w}\|_a$. Si t vaut 0 alors la forme normale tournante de $\overline{w}$ est un A_n-mot positif, donc un mot σ-défini. Si m vaut 2 avec $t \neq 0$ alors u est le mot vide ε et la forme normale tournante de $\overline{w}$ est une puissance de $d_{1,2}^{-1}$, donc un mot σ-défini.

Ensuite, on utilise l'algorithme `Eclatement` pour calculer le ϕ_n-éclatement $(\overline{u}_b, \dots, \overline{u}_1)$ de $\overline{u}$. Alors la forme normale tournante de $\overline{w}$ est équivalente à v avec

$$v = d_{1,m}^{-t+b-1}\, u_b\, d_{1,m}^{-1}\, u_{b-1}\, d_{1,m}^{-1} \dots\, u_2\, d_{1,m}^{-1}\, u_1, \tag{4.29}$$

Si la relation $t \geqslant b-1$ est satisfaite alors le mot v est σ_{n-1}-négatif par la proposition 3.11, donc σ-défini. Dans ce cas l'algorithme retourne un mot σ-défini équivalent à w.

Supposons maintenant que la relation $t \geqslant b-1$ ne soit pas satisfaite. Dans ce cas on refait la même chose avec le mot w^{-1}. Notons que les indices de $\overline{w}$ et $\overline{w}^{-1}$ sont les mêmes, on peut donc directement aller à la ligne 2 de l'algorithme. Dans ce cas, par la proposition 3.13, la tresse $\overline{w}$ est σ_{m-1}-nonnégative. Ainsi, comme m est l'indice de $\overline{w}$, elle est σ_{m-1}-positive. La tresse représentée par w^{-1} est donc σ_{n-1}-négative et les nouveaux entiers t et b calculés satisfont la relation $t \geqslant b-1$ et l'algorithme se termine.

La complexité en longueur est une conséquence des propositions 3.5 et 3.11 et 3.23. □

V. Bon ordre du monoïde de tresses dual

Nous avons vu au chapitre I.1 que le groupe de tresses B_n est ordonnable à gauche. D'après un résultat de R. Laver [Lav96] la restriction de cet ordre aux monoïdes de tresses positives est un bon ordre. Malheureusement la méthode donnée par Laver ne permet pas de calculer la longueur du bon ordre $(B_n^+, <)$. Dans sa thèse S. Burckel, montre que la longueur de $(B_n^+, <)$ est l'ordinal $\omega^{\omega^{n-2}}$. L'argument utilisé est astucieux et nécessite une induction transfinie assez technique. À l'aide des résultats de S. Burckel, P. Dehornoy donne une caractérisation plus simple du bon ordre à l'aide de la forme normale alternante définie à la section III.1.3.

Dans ce chapitre nous allons étudier la restriction de l'ordre des tresses aux monoïdes de Birman–Ko–Lee. D'après le théorème I.3.16, on sait déjà que $(B_n^{+*}, <)$ est un bon ordre. Le but est donc de calculer la longueur du bon ordre $(B_n^{+*}, <)$. Plus précisement nous allons démontrer le théorème suivant

Théorème 0.1. *Pour β, β' dans B_n^{+*}, la relation $\beta < \beta'$ est vraie si et seulement si le ϕ_n-éclatement de β est plus petit que le ϕ_n-éclatement de β' par rapport à l'extension* `ShortLex` *de l'ordre $<$ sur B_{n-1}^{+*}.*

Comme conséquence immédiate nous obtiendrons le résultat suivant donnant la longueur du bon ordre $(B_n^{+*}, <)$.

Corollaire 0.2. *La restriction de $<$ au monoïde est un bon ordre de longueur $\omega^{\omega^{n-2}}$.*

À part pour quelques exemples et applications, nous n'avons pas besoin de savoir que la relation $<$ est un ordre total invariant à gauche. Nous allons juste utiliser sa définition plus le fait évident que la relation $<$ est transitive. Ceci nous permet notamment de redémontrer la Propriété **C**, qui établit que toute tresse non triviale admet au moins une expression σ-définie, c'est-à-dire, une expression dans laquelle le générateur σ_i de plus grand indice i apparaît seulement positivement, ou seulement négativement.

1 Ordre tournant

Avant toute chose commençons par quelques relations élémentaires portant sur la restriction de l'ordre standard $<$ au monoïde B_n^{+*}.

Lemme 1.1. *Toute tresse β de B_n^{+*} exceptée 1 satisfait $\beta > 1$.*

Démonstration. Par définition, la tresse $a_{p,q}$ est σ_{q-1}-positive et donc σ-positive. □

Lemme 1.2. *Pour tout $n \geqslant 2$, on a*

$$1 < a_{1,2} < a_{2,3} < a_{1,3} < \ldots < a_{1,n-1} < a_{n-1,n} < a_{n-2,n} < \ldots < a_{1,n}. \tag{5.1}$$

Démonstration. Montrons qu'on a $a_{p,q} < a_{r,s}$ si et seulement si on a soit $q < s$, soit $q = s$ avec $p > r$. Supposons d'abord $q < s$. Alors la tresse $a_{p,q}^{-1}$ est σ_{q-1}-négative tandis que $a_{r,s}$ est σ_{s-1}-positive avec $q < s$. Le quotient $a_{p,q}^{-1}\, a_{r,s}$ est donc σ_{s-1}-positif, ce qui implique $a_{p,q} < a_{r,s}$. Supposons maintenant $q = s$ avec $p > r$. Alors, par la relation (II.2.5), le quotient $a_{p,q}^{-1}\, a_{r,s}$ est égal à $d_{p,s-1}\, d_{p,s}^{-1}\, d_{r,s}\, d_{r,s-1}^{-1}$. En appliquant la relation (II.2.6) sur $d_{r,s}$, on obtient

$$a_{p,q}^{-1}\, a_{r,s} = d_{p,s-1}\, d_{p,s}^{-1}\, d_{r,p-1}\, d_{p-1,s}\, d_{r,s-1}^{-1}.$$

Alors, en appliquant la relation (II.2.7) sur $d_{p,s}^{-1}\, d_{r,p-1}$, on obtient

$$a_{p,q}^{-1}\, a_{r,s} = d_{p,s-1}\, d_{r,p-1}\, d_{p,s}^{-1}\, d_{p-1,s}\, d_{r,s-1}^{-1}.$$

Finalement, la relation (II.2.8) sur $d_{p,s}^{-1}\, d_{p-1,s}$ implique $d_{p,s}^{-1}\, d_{p-1,s} \equiv d_{p,s+1}\, d_{p,s}^{-1}$ et donc par la relation (II.2.5) on a

$$a_{p,q}^{-1}\, a_{r,s} = d_{p,s-1}\, d_{r,p-1}\, a_{p-1,s}\, d_{r,s-1}^{-1}.$$

La tresse $a_{p-1,s}$ est σ_{s-1}-positive, tandis que les tresses $d_{p,s-1}$, $d_{r,p-1}$ et $d_{r,s-1}^{-1}$ sont σ_t-positives ou σ_t-négatives pour $t < s-1$. Ainsi, le quotient $a_{p,q}^{-1}\, a_{r,s}$ est σ_{s-1}-positif, ce qui implique la relation $a_{p,q} < a_{r,s}$.

Comme $<$ est un ordre total, c'est suffisant pour conclure, c'est-à-dire que les implications que l'on vient de montrer sont des équivalences. □

Afin de démontrer le théorème 0.1, nous commençons par introduire un ordre dit *tournant* sur B_n^{+*} construit à partir de la forme normale tournante.

1.1 Définition

Grâce au ϕ_n-éclatement de la définition III.2.8, toute tresse de B_n^{+*} est caractérisée par une unique suite de tresses de B_{n-1}^{+*}. De cette manière, tout ordre défini sur B_{n-1}^{+*} peut être étendu à B_n^{+*} en utilisant une extension `ShortLex` de cet ordre. En itérant ce procédé, et partant de l'ordre standard défini sur B_2^{+*}, c'est-à-dire, celui des entiers, on définit par induction un ordre total sur B_n^{+*}.

Nous rappelons que, si $(A, \prec)$ est un ensemble ordonné, une suite finie s de A est dite `ShortLex`-plus petite qu'une autre suite finie s' si la longueur de s est plus petite que celle de s', ou si les deux sont égales et que s est lexicographiquement $\prec$-plus petite que s', c'est-à-dire, lorsque les deux suites sont lues à partir de la gauche, le premier terme dans s qui ne coïncide pas avec son homologue dans s' est $\prec$-plus petit.

Définition 1.3. Pour $n \geqslant 2$, on définit inductivement une relation $<_n^*$ sur B_n^{+*} comme suit :
– Pour β, γ dans B_2^{+*}, on déclare que $\beta <_2^* \gamma$ est vraie pour $\beta = a_{1,2}^b$ et $\gamma = a_{1,2}^c$ avec $b < c$;
– Pour β, γ dans B_n^{+*} avec $n \geqslant 3$, on déclare que $\beta <_n^* \gamma$ est vraie si le ϕ_n-éclatement de β est plus petit que le ϕ_n-éclatement de γ pour l'extension `ShortLex` de $<_{n-1}^*$.

L'ordre $<_n^*$ est applé *ordre tournant*.

Exemple 1.4. Comme nous l'avons vu à l'exemple III.2.10, la n-largeur de $a_{p,q}$ avec $q \leqslant n-1$ est 1 tandis que la n-largeur de $a_{q,n}$ est 2 pour $p \neq 1$ ou 3 pour $p = 1$. Une induction facile sur n donne $a_{p,q} <_n^* a_{r,s}$ lorsque $q < s \leqslant n$ est vérifiée. On établie alors

$$1 <_n^* a_{1,2} <_n^* a_{2,3} <_n^* a_{1,3} <_n^* a_{3,4} <_n^* a_{2,4} <_n^* a_{1,4} <_n^* \ldots <_n^* a_{n-1,n} <_n^* \ldots <_n^* a_{1,n}.$$

On observe que d'après le lemme 1.2 et l'exemple 1.4, les relations $<$ et $<_n^*$ sont d'accord sur les générateurs de B_n^{+*}.

Proposition 1.5. *Pour $n \geqslant 2$, la relation $<_n^*$ est un bon ordre de B_n^{+*}. Pour toute tresse β de B_n^{+*}, le $<_n^*$-successeur immédiat de β est $\beta\, a_{1,2}$, c'est-à-dire, $\beta\, \sigma_1$.*

Démonstration. Le monoïde ordonné $(B_2^{+*}, <_2^*)$ est isomorphe à $\mathbb{N}$ muni de l'ordre usuel. C'est donc un bon ordre. Comme une extension `ShortLex` d'un bon ordre est un bon ordre [Lév79] on déduit inductivement que $<_n^*$ est un bon ordre.

Le résultat portant sur les successeurs est une conséquence directe du fait que si le ϕ_n-éclatement de β est $(\beta_p, \dots, \beta_1)$, alors le ϕ_n-éclatement de $\beta a_{1,2}$ est $(\beta_p, \dots, \beta_1 a_{1,2})$. □

Le lien entre la relation d'ordre $<_n^*$ et sa restriction à B_{n-1}^{+*} est simple : B_{n-1}^{+*} est un segment initial de B_n^{+*}.

Proposition 1.6. *Pour $n \geqslant 3$, le monoïde B_{n-1}^{+*} est le segment initial de $(B_n^{+*}, <_n^*)$ déterminé par $a_{n-1,n}$, c'est-à-dire qu'on a*

$$B_{n-1}^{+*} = \{\beta \in B_n^{+*} \mid \beta <_n^* a_{n-1,n}\}.$$

De plus $a_{n-1,n}$ est la plus petite tresse de n-largeur 2.

Démonstration. D'abord, par construction, toute tresse β de B_{n-1}^{+*} est de n-largeur 1, tandis que, par (III.2.10), la n-largeur de $a_{n-1,n}$ est 2. Donc par définition de $<_n^*$, la relation $\beta <_n^* a_{n-1,n}$ est satisfaite.

Réciproquement, supposons que β est une tresse de B_n^{+*} satisfaisant $\beta <_n^* a_{n-1,n}$. Comme la n-largeur de $a_{n-1,n}$ est 2, l'hypothèse $\beta <_n^* a_{n-1,n}$ implique que la n-largeur de β est au plus 2. Montrons, en utilisant une induction sur n, que β est de n-largeur au plus 1, ce qui, par construction, implique que la tresse β appartient à B_{n-1}^{+*}.

Supposons $n = 3$. Par définition, tout ϕ_3-éclatement de longueur 2 est de la forme $(a_{1,2}^b, a_{1,2}^c)$ avec $b \neq 0$. La $<_3^*$-plus petite suite de ce type est $(a_{1,2}, 1)$, qui se trouve être le ϕ_3-éclatement de $a_{2,3}$. Ainsi $a_{2,3}$ est le plus $<_3^*$-petit élément de B_3^{+*} de 3-largeur valant 2. La relation $\beta <_3^* a_{2,3}$ implique donc que β appartient à B_2^{+*}.

Supposons maintenant $n > 3$. Supposons de plus pour obtenir une contradiction que la n-largeur de β soit 2. Notons (β_2, β_1) le ϕ_n-éclatement de β. Comme le ϕ_n-éclatement de $a_{n-1,n}$ est la suite $(a_{n-2,n-1}, 1)$, et que la relation $\beta_1 <_{n-1}^* 1$ est impossible, l'hypothèse $\beta <_n^* a_{n-1,n}$ implique $\beta_2 <_{n-1}^* a_{n-2,n-1}$. Par hypothèse d'induction, ceci implique que β_2 appartient à B_{n-2}^{+*}, donc que $\phi_n(\beta_2)$ est un élément de B_{n-1}^{+*}. Ceci contredit la condition (III.3.15) : une suite (β_2, β_1) avec β_2 appartenant à B_{n-2}^{+*} ne peut pas être le ϕ_n-éclatement d'une tresse B_n^{+*}. Ainsi l'hypothèse que la n-largeur de β soit 2 est contradictoire, et β appartient nécessairement à B_{n-1}^{+*}. □

Le résultat de compatibilité de la proposition 1.6 montre que l'on peut ôter l'indice n sans ambiguïté du symbole $<_n^*$ et simplement écrire $<^*$. Notons que $<^*$ est en fait un ordre total (et même un bon ordre) sur B_∞^{+*}, la limite inductive des monoïdes B_n^{+*} par un plongement canonique de B_{n-1}^{+*} dans B_n^{+*}.

1.2 Tresses séparatrices

Par définition de $<^*$, pour $b < c$, toute tresse de B_n^{+*} dont la n-largeur vaut b est $<^*$-plus petite que toute tresse dont la n-largeur vaut c. Comme l'ordre $<^*$ est un bon ordre, il doit

exister, pour tout b, une $<^*$-plus petite tresse de n-largeur b. Ces tresses, qui sont en quelque sorte des séparateurs pour $<^*$, sont facilement identifiées. Elles joueront un rôle important dans la suite de ce chapitre.

La proposition 1.6 affirme que la plus petite tresse de n-largeur 1 est $a_{n-1,n}$. À partir de la n-largeur 2, un schéma périodique apparaît.

Définition 1.7. Pour $n \geqslant 3$ et $b \geqslant 1$, on pose $\widehat{\delta}_{n,b} = \phi_n^{b+1}(a_{n-2,n-1}) \cdot \ldots \cdot \phi_n^2(a_{n-2,n-1})$.

Les tresses $\widehat{\delta}_{n,b}$ sont dites *séparatrices*. Par exemple, on trouve

$$\widehat{\delta}_{6,4} = \phi_6^5(a_{4,5}) \cdot \phi_6^4(a_{4,5}) \cdot \phi_6^3(a_{4,5}) \cdot \phi_6^2(a_{4,5}),$$

et donc $\widehat{\delta}_{6,4} = a_{3,4}\, a_{2,3}\, a_{1,2}\, a_{1,6}$, et, de la même façon, $\widehat{\delta}_{5,3} = a_{2,3}\, a_{1,2}\, a_{1,5}$.

Proposition 1.8. *Pour $n \geqslant 3$ et $b \geqslant 1$,*
- *(i) le ϕ_n-éclatement de $\widehat{\delta}_{n,b}$ est la suite $(a_{n-2,n-1}, \ldots, a_{n-2,n-1}, 1, 1)$ de longueur $b+2$;*
- *(ii) on a l'égalité $\widehat{\delta}_{n,b} = \delta_n^b \delta_{n-1}^{-b}$;*
- *(iii) la tresse $\widehat{\delta}_{n,b}$ est la $<^*$-plus petite tresse appartenant à B_n^{+*} de n-largeur $b+2$—elle est donc le plus petit majorant des tresses de n-largeur $\leqslant b+1$.*

Démonstration. (i) D'abord, observons qu'il n'existe pas de relation $a_{n-1,n}\, a_{n-2,n-1} = \ldots$ dans la présentation du monoïde B_n^{+*} donné en (II.2.13). Ainsi, le mot $a_{n-1,n}a_{n-2,n-1}$, qui est égal au mot $\phi_n(a_{n-2,n-1})\, a_{n-2,n-1}$, est seul dans sa classe d'équivalence sous les relations de B_n^{+*}. De même, le mot

$$\phi_n^{b-1}(a_{n-2,n-1}) \cdot \ldots \cdot a_{n-2,n-1},$$

noté w, est seul dans sa classe d'équivalence, car aucune relation ne peut être appliquée à n'importe quel sous mot de longueur 2 de ce mot. Comme ϕ_n est un isomorphisme, on a la même propriété pour le mot $\phi_n^2(w)$, qui représente la tresse $\widehat{\delta}_{n,b}$. Comme la tresse $\widehat{\delta}_{n,b}$ est représentée par au moins un mot tournant, nous déduisons que $\phi_n^2(w)$ est le mot tournant représentant $\widehat{\delta}_{n,b}$, c'est-à-dire, sa forme normale tournante.

(ii) Nous utilisons une induction sur b. La relation (II.2.5) implique que la tresse $a_{1,n}$ est égale à $\delta_n \delta_{n-1}^{-1}$. En utilisant (III.2.1), on déduit

$$\widehat{\delta}_{n,1} = \phi_n^2(a_{n-2,n-1}) = a_{1,n} = \delta_n\, \delta_{n-1}^{-1}.$$

Supposons $b \geqslant 2$. Par définition, on a $\widehat{\delta}_{n,b} = \phi_n^{b+1}(a_{n-2,n-1})\, \widehat{\delta}_{n,b-1}$. Alors, par hypothèse d'induction on a

$$\widehat{\delta}_{n,b} = \phi_n^{b+1}(a_{n-2,n-1})\, \delta_n^{b-1}\, \delta_{n-1}^{-b+1}.$$

En poussant δ_n^{b-1} vers la gauche à l'aide de la relation (III.3.5), on obtient :

$$\widehat{\delta}_{n,b} = \delta_n^{b-1}\, \phi_n^2(a_{n-2,n-1})\, \delta_{n-1}^{-b+1}.$$

La relation (III.2.1) implique $\phi_n^2(a_{n-2,n-1}) = a_{1,n}$. Donc, en utilisant la relation (II.2.5), on obtient finalement

$$\widehat{\delta}_{n,b} = \delta_n^{b-1}\, \delta_n\, \delta_{n-1}^{-1}\, \delta_{n-1}^{-b+1} = \delta_n^b\, \delta_{n-1}^{-b}.$$

(iii) Soit $(\beta_{b+2}, \ldots, \beta_1)$ le ϕ_n-éclatement d'une tresse appartenant à B_n^{+*} et qui satisfait la relation $\beta \leqslant^* \widehat{\delta}_{n,b}$. Par définition de $<^*$, on a $\beta_{b+2} \leqslant^* a_{n-2,n-1}$. Par le lemme III.3.2 (i) et (ii),

la B^{+*}_{n-2}-fin de β_{b+2} est triviale, donc sa $(n-1)$-largeur est au moins 2. Ainsi la proposition 1.6 montre que β_{b+2} est égale à $a_{n-2,n-1}$. Encore par définition de $<^*$, on a $\beta_{b+1} \leqslant^* a_{n-2,n-1}$. En utilisant le précédent argument, on obtient $\beta_k = a_{n-2,n-1}$ pour $k \geqslant 3$. Utiliser l'argument une fois de plus donne $\beta_2 \leqslant^* 1$, ce qui implique $\beta_2 = 1$. Finalement, par définition de $<^*$, on a l'égalité $\beta_1 = 1$. On conclut par (i) et l'unicité du ϕ_n-éclatement. □

D'après la proposition 1.8, il est cohérent d'étendre la définition 1.7 en posant $\widehat{\delta}_{n,0} = a_{n-1,n}$. De cette manière, les résultats de la proposition 1.8 (iii) s'étendent au cas $b = 0$.

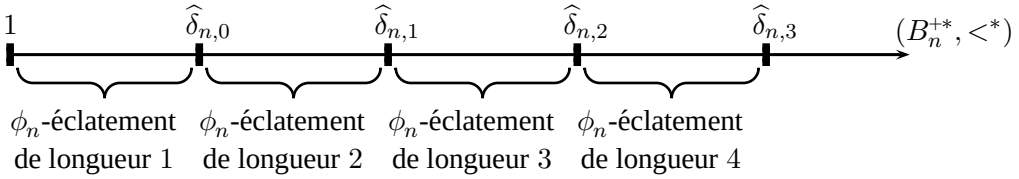


FIG. 5.1 : La tresse $\widehat{\delta}_{n,r}$ vue comme séparatrice dans $(B^{+*}_n, <^*)$—donc dans $(B^{+*}_n, <)$ dès qu'on aura démontré le théorème 1.10.

Observons maintenant que les ordres $<$ et $<^*$ s'accordent sur les tresses séparatrices $\widehat{\delta}_{n,b}$.

Lemme 1.9. *Supposons $n \geqslant 3$. Alors la relation $0 \leqslant b < c$ implique $\widehat{\delta}_{n,b} < \widehat{\delta}_{n,c}$.*

Démonstration. Supposons $0 < b < c$. Par la proposition 1.8 (ii), on a

$$\widehat{\delta}_{n,b}^{-1} \cdot \widehat{\delta}_{n,c} = \delta_{n-1}^{b}\, \delta_n^{-b} \cdot \delta_n^{c}\, \delta_{n-1}^{-c} = \delta_{n-1}^{b}\, \delta_n^{c-b}\, \delta_{n-1}^{-c}.$$

L'hypothèse $c - b > 0$ implique que la tresse $\widehat{\delta}_{n,b}^{-1}\, \widehat{\delta}_{n,c}$ est σ_{n-1}-positive, car la tresse δ_k est σ_{k-1}-positive. On a donc $\widehat{\delta}_{n,b} < \widehat{\delta}_{n,c}$.

Il reste à établir le résultat pour $b = 0$. Le cas précédent donne $\widehat{\delta}_{n,1} \leqslant \widehat{\delta}_{n,c}$. Comme la relation $<$ est transitive, il est suffisant de montrer $\widehat{\delta}_{n,0} < \widehat{\delta}_{n,1}$. En utilisant la proposition 1.8 (ii) et en insérant $\delta_n \delta_n^{-1}$ à gauche, on obtient

$$\widehat{\delta}_{n,0}^{-1}\, \widehat{\delta}_{n,1} = a_{n-1,n}^{-1}\, \delta_n\, \delta_{n-1}^{-1} = \delta_n\, \delta_n^{-1} a_{n-1,n}^{-1} \delta_n\, \delta_{n-1}^{-1}.$$

La relation (III.2.1) implique $\delta_n^{-1} a_{n-1,n}^{-1} \delta_n = \phi_n^{-1}(a_{n-1,n}^{-1}) = a_{n-2,n-1}^{-1}$. On en déduit

$$\widehat{\delta}_{n,0}^{-1}\, \widehat{\delta}_{n,1} = \delta_n\, a_{n-2,n-1}^{-1}\, \delta_{n-1}^{-1},$$

et la dernière écriture est explicitement σ_{n-1}-positive. □

1.3 Le résultat principal

À ce stade, nous avons *a priori* deux ordres distincts sur le monoïde B^{+*}_n, à savoir l'ordre standard des tresses $<$, et l'ordre tournant $<^*$ de la définition 1.3. Le principal résultat de ce chapitre est :

Théorème 1.10. *Pour toutes tresses β, β' de B^{+*}_n, la relation $\beta <^* \beta'$ implique $\beta < \beta'$.*

Avant de commencer la démonstration de ce résultat, nous en listons quelques conséquences. Tout d'abord, nous obtenons une nouvelle démonstration de la propriété **C**.

Corollaire 1.11 (Propriété **C**)**.** *Toute tresse non triviale est σ-positive ou σ-négative.*

Démonstration. Supposons que β soit une tresse non triviale de B_n. Comme par le corollaire II.3.20, B_n est le groupe de fractions de B_n^{+*}, il existe β', β'' de B_n^{+*} satisfaisant $\beta = \beta'^{-1}\,\beta''$. La tresse β étant supposée non triviale, on a $\beta' \neq \beta''$. Comme $<^*$ est un ordre total, une des relations $\beta' <^* \beta''$ ou $\beta'' <^* \beta'$ est vraie. Dans le premier cas, le théorème 1.10 implique que la tresse quotient $\beta'^{-1}\,\beta''$, c'est-à-dire, β, est σ-positive. Dans le second cas, le théorème 1.10 implique que la tresse quotient $\beta''^{-1}\,\beta'$ est σ-positive, donc que β est σ-négative. □

Corollaire 1.12. *La relation $<^*$ coïncide avec la restriction de $<$ à B_n^{+*}.*

Démonstration. Soient β, γ dans B_n^{+*}. Par le théorème 1.10, la relation $\beta <^* \gamma$ implique $\beta < \gamma$. Réciproquement, supposons $\beta \not<^* \gamma$. Comme $<^*$ est un ordre total, on a soit $\gamma <^* \beta$, et donc $\gamma < \beta$, soit $\beta = \gamma$. Dans les deux cas, la propriété **A** introduite à la section I.3.1 implique que la relation $\beta < \gamma$ est fausse. □

Le corollaire 1.12 implique directement le théorème 0.1. En effet, la caractérisation de l'ordre des tresses donnée au théorème 0.1 n'est rien d'autre que la définition inductive de la relation d'ordre $<^*$.

Finalement, nous obtenons une nouvelle démonstration d'un résultat de Laver, ainsi que la détermination de la longueur de $(B_n^{+*}, <)$.

Corollaire 1.13. *La restriction de l'ordre des tresses au monoïde de tresses dual B_n^{+*} est un bon ordre, et sa longueur est l'ordinal $\omega^{\omega^{n-2}}$.*

Démonstration. Il est standard que, si $(X, <)$ est un bon ordre de longueur λ, alors l'extension `ShortLex` de $<$ aux suites finies d'éléments de X est un bon ordre de longueur λ^ω—voir [Lév79]. La longueur $(B_2^{+*}, <^*)$ est ω, la longueur de $\mathbb{N}$ muni de l'ordre standard des entiers. Ainsi, une induction immédiate montre que, pour tout $n \geqslant 2$, la longueur de $(B_n^{+*}, <^*)$ est au plus $\omega^{\omega^{n-2}}$.

A priori, c'est seulement une borne supérieure, car il n'est pas vrai que toute suite de tresses de B_{n-1}^{+*} est le ϕ_n-éclatement d'une tresse de B_n^{+*}. Cependant, par construction, le monoïde B_n^{+*} inclut le monoïde de tresses positives B_n^+, et il est montré dans [Bur97]—ou dans [CDW08]—que la longueur de $(B_n^+, <)$ est $\omega^{\omega^{n-2}}$. Ainsi la longueur de $(B_n^{+*}, <)$ est au moins cet ordinal, et, finalement, on a l'égalité. □

Remarque 1.14. Par construction, l'ordre $<$ est invariant par multiplication à gauche. Une autre conséquence du corollaire 1.12 est que l'ordre $<^*$ est aussi invariant par multiplication à gauche. Notons que ce dernier résultat n'est pas évident à partir de la définition de la relation $<^*$.

2 Preuve de la coïncidence

Le but de cette section est de montrer que l'ordre tournant $<^*$ de la définition 1.3 et l'ordre standard des tresses $<$ coïncident. Le résultat sera une conséquence de propriétés portant sur la forme normale tournante.

2.1 Tresses σ-positives de type $a_{p,n}$

Nous allons démontrer le théorème 1.10 en utilisant une induction sur le nombre de brins n. Dans le but de maintenir une hypothèse d'induction, nous allons montrer un résultat plus fort : à la place de seulement monter que, si β est $<^*$-plus petite que γ, alors la tresse quotient $\beta^{-1}\gamma$ est σ-positive, nous allons montrer la conclusion plus précise que la tresse $\beta^{-1}\gamma$ est *σ-positive de type* $a_{p,n}$ pour un certain p dépendant de la dernière lettre de γ.

Définition 2.1. Supposons $n \geqslant 3$.
- Une tresse de B_n est dite *$a_{p,n}$-dangereuse* si elle est représentée par au moins un mot $a_{q,n}$-dangereux avec $q \geqslant p$.
- Une tresse de B_n est dite *σ_{n-1}-nonnégative* si elle peut être représentée par un Σ_n-mot σ_{n-1}-nonnégatif.
- Pour $p \leqslant n-2$, une tresse β est dite *σ-positive de type* $a_{p,n}$ si elle peut être exprimée par
$$\beta^+ \cdot d_{p,n} \cdot \beta^-,$$
où β^+ est σ_{n-1}-nonnégative et où β^- est $a_{p,n}$-dangereuse.
- Une tresse β est dite *σ-positive de type* $a_{n-1,n}$ si elle est égale à
$$\beta' \cdot a_{n-1,n},$$
où β' est une tresse σ-positive de type $a_{1,n}$ ou bien triviale.

Notons qu'une tresse σ-positive de type $a_{p,n}$ avec $p \neq n-1$ n'est pas triviale, c'est-à-dire, est différente de 1, car elle contient $d_{p,n-1}$, qui est non triviale.

Observons que la définition d'une tresse σ-positive de type $a_{n-1,n}$ est différente de celle d'une tresse σ-positive de type $a_{p,n}$ pour $p < n-1$ (des raisons techniques rendent cette distinction nécessaire).

Dire qu'une tresse est σ-positive de type $a_{p,n}$ est motivé par le fait que $a_{p,n}$ est la plus simple tresse σ-positive de ce type.

Lemme 2.2. *Supposons que β soit une tresse σ-positive de type $a_{p,n}$. Alors*
- *(i) β est σ_{n-1}-positive,*
- *(ii) $\phi_{n+1}(\beta)$ est σ-positive de type $a_{p+1,n+1}$,*
- *(iii) si $p = 1$ alors $\beta\,\delta_{n-1}^{-t}$ est σ-positive de type $a_{1,n}$ pour tout $t \geqslant 0$,*
- *(iv) si $\beta \neq a_{n-1,n}$ est vérifiée, alors $\gamma\,\beta$ est σ-positive de type $a_{p,n}$ pour toute tresse σ_{n-1}-nonnégative γ.*

Démonstration. (i) Une tresse $a_{p,n}$-dangereuse est σ_{n-1}-nonnégative (en fait σ_{n-2}-négative), et la tresse $d_{p,n}$ est σ_{n-1}-positive. Ainsi la tresse β est σ_{n-1}-positive.

(ii) Avec les notations de la définition 2.1, soit $d_{f(e),n-1}^{-1} \ldots d_{f(1),n-1}^{-1}$ la décomposition de la tresse β^-, avec $f(1) = p$. Alors on a
$$\phi_{n+1}(\beta^-) = d_{f(e)+1,n}^{-1} \ldots d_{f(1)+1,n}^{-1},$$
qui est un mot $a_{p+1,n+1}$-dangereux. Par définition, la tresse β^+ peut être représentée par un A_{n-2}-mot. Comme, pour $i \leqslant n-2$, l'image de σ_i par ϕ_{n+1} est σ_{i+1}, la tresse $\phi_{n+1}(\beta^+)$ est σ_n-nonnégative. Ainsi la relation
$$\phi_{n+1}(\beta) = \phi_{n+1}(\beta^+) \cdot d_{p+1,n+1} \cdot \phi_{n+1}(\beta^-)$$

témoigne que la tresse $\phi_{n+1}(\beta)$ soit σ-positive de type $a_{p+1,n+1}$.

Le point (iii) est une conséquence directe du fait que, si γ^- est une tresse $a_{1,n}$-dangereuse, alors, pour tout $t \geqslant 0$, la tresse $\gamma^- \, \delta_{n-1}^{-t}$ est aussi $a_{1,n}$-dangereuse.

(iv) Supposons $p \leqslant n-2$. Alors, par définition, on a $\beta = \beta^+ \cdot d_{p,n} \cdot \beta^-$, où β^+ est σ_{n-1}-nonnégative et β^- est $a_{p,n}$-dangereuse. On obtient donc $\gamma\,\beta = \gamma\,\beta^+ \cdot d_{p,n} \cdot \beta^-$. Comme le produit de tresses σ_{n-1}-nonnégatives est σ_{n-1}-nonnégatif, la tresse $\gamma\,\beta$ est σ-positive de type $a_{p,n}$.

Supposons $p = n-1$. Comme, par hypothèse, β est différente de $a_{n-1,n}$, elle se décompose en $\beta' \cdot a_{n-1,n}$, où β' est une tresse σ-positive de type $a_{1,n}$. Le cas $p \leqslant n-2$ implique que la tresse $\gamma\,\beta'$ est σ-positive de type $a_{1,n}$. Ainsi la tresse $\gamma\,\beta$, qui est égale à $\gamma\,\beta' \cdot a_{n-1,n}$, est σ-positive de type $a_{n-1,n}$. □

Remarque 2.3. Pour $t \geqslant 1$, la tresse $\widehat{\delta}_{n,t}$ est σ-positive de type $a_{1,n}$. En effet, par la proposition 1.8 (ii), on a $\widehat{\delta}_{n,t} = \delta_n^{t-1} \cdot \delta_n \cdot \delta_{n-1}^{-t}$, le membre de droite étant une tresse σ-positive de type $a_{1,n}$ explicite.

Montrons maintenant que les termes d'un ϕ_n-éclatement donnent lieu à des tresses σ-positives de type $a_{p,n}$, pour un certain entier p que l'on contrôle.

Lemme 2.4. *Pour $n \geqslant 3$, toute tresse dont la dernière lettre est $a_{p,n}$ est σ-positive de type $a_{p,n}$.*

Démonstration. Soit β une tresse de B_n^{+*} dont la dernière lettre $\beta^{\#}$ est $a_{p,n}$. Posons $\beta = \beta' \cdot a_{p,n}$. Supposons d'abord $p \leqslant n-2$. Alors, par (II.2.5), on a $\beta = \beta' \cdot d_{p,n} \cdot d_{p,n-1}^{-1}$, une tresse σ-positive de type $a_{p,n}$, car la tresse β' appartient à B_n^{+*}, donc σ_{n-1}-nonnégative, et la tresse $d_{p,n-1}^{-1}$ est $a_{p,n}$-dangereuse.

Supposons maintenant $p = n-1$. Le cas où la tresse β' est triviale est évident. Pour $\beta' \neq 1$, par le lemme III.3.2 (iii), il existe une tresse β'' de B_n^{+*} satisfaisant $\beta' = \beta'' \cdot a_{q,n}$ pour un certain q. La relation $a_{1,q}\, a_{q,n} = a_{q,n}\, a_{1,n}$ implique $a_{q,n} = a_{1,q}^{-1}\, a_{q,n}\, a_{1,n}$. Utilisant (II.2.5) sur la tresse $a_{1,n}$ on obtient

$$\beta' = \beta''\, a_{1,q}^{-1}\, a_{q,n} \cdot d_{1,n} \cdot d_{1,n-1}^{-1},$$

une tresse σ-positive de type $a_{1,n}$. Ainsi, β est σ-positive de type $a_{1,n}$. □

Lemme 2.5. *Supposons $n \geqslant 3$ et soit β une tresse représentée par une $a_{p,n}$-échelle adossée à $a_{q-1,n-1}$ avec $q \neq n-1$ et γ une tresse $a_{p,n}$-dangereuse. Alors $\gamma\,\beta$ est une tresse σ-positive de type $a_{q-1,n-1}$.*

Démonstration. La proposition IV.2.8 implique que la tresse $\gamma\,\beta$ est représentée par un mur adossé à $a_{q-1,n-1}$. Il existe donc un mot σ_{n-2}-nonnégatif w et un mot $a_{q-1,n-1}$-dangereux telle qu'on ait

$$\gamma\,\beta = \overline{w} \cdot d_{q-1,n-1} \cdot \overline{v},$$

qui est une tresse σ-positive de type $a_{q-1,n-1}$ (ici q est différent de $n-1$). □

Nous sommes maintenant prêts pour montrer que les termes non terminaux d'un ϕ_n-éclatement $(\beta_b, \dots, \beta_1)$ ont la propriété désirée, à savoir que la tresse β_k protège contre une tresse $\phi_n(\beta_{k+1}^{\#})$-dangereuse, dans le sens que si γ_{k+1} est une tresse $\beta_{k+1}^{\#}$-dangereuse, alors $\phi_n(\gamma_{k+1})\,\beta_k$ est σ-positive de type $\beta_k^{\#}$.

Proposition 2.6. *Supposons que $(\beta_b, \dots, \beta_1)$ soit un ϕ_n-éclatement. Alors, pour tout k de l'ensemble $\{b-1, \dots, 3\}$ et toute tresse $\beta_{k+1}^{\#}$-dangereuse γ_{k+1}, la tresse $\phi_n(\gamma_{k+1})\,\beta_k$ est σ-positive de type $\beta_k^{\#}$. De plus la tresse $\gamma_{k+1}\,\beta_k$ est différente de $a_{n-2,n-1}$, sauf si β est elle-même $a_{n-2,n-1}$. Le même résultat est satisfait pour $k = 2$, sauf si β_2 est la tresse triviale.*

Démonstration. Prenons k dans $\{b-1, \dots, 3\}$. Par définition de γ_{k+1}, la tresse $\phi_n(\gamma_{k+1})$ est $\phi_n(\beta^{\#}_{k+1})$-dangereuse. Supposons $\beta^{\#}_k \neq a_{n-2,n-1}$. Par la proposition III.3.10, la forme normale tournante de β_k est une $\phi_n(\beta^{\#}_{k+1})$-échelle adossée à $\beta^{\#}_k$. Par le lemme 2.5, la tresse $\phi_n(\gamma_{k+1})\,\beta_k$ est donc σ-positive de type $\beta^{\#}_k$.

Supposons maintenant $\beta^{\#}_k = a_{n-2,n-1}$ avec $\beta_k \neq a_{n-2,n-1}$. Par la proposition III.3.10, la forme normale tournante de β_k est une $\phi_n(\beta^{\#}_{k+1})$-échelle adossée à $a_{n-2,n-1}$. Soit $w'\,a_{n-2,n-1}$ la forme normale tournante de β. Par définition d'une échelle, comme la lettre $a_{n-2,n-1}$ ne satisfait pas la condition (i) de la définition III.3.8, le mot w' est une $a_{p,n}$-échelle adossée à $a_{q-1,n-1}$ pour un certain q—lemme III.3.2 (iii). On note β'_k la tresse représentée par w'. Alors, par le lemme 2.5, la tresse $\phi_n(\gamma_{k+1})\,\beta'_k$ est σ-positive de type $a_{p,n-1}$. Elle est alors le produit

$$\beta'^{+}_k \cdot d_{q-1,n-1} \cdot\ \beta'^{-}_k.$$

La relation $d_{1,q-1}\,d_{q-1,n-1} = d_{1,n-1}$ implique que la tresse $\phi_n(\gamma_{k+1})\,\beta'_k$ est égale à

$$\beta'^{+}_k\, d^{-1}_{1,q-1} \cdot d_{1,n-1} \cdot\ \beta'^{-}_k,$$

où $\beta'^{+}_k\, d^{-1}_{1,p}$ est σ_{n-2}-nonnégative et β'^{-}_k est $a_{..,n-1}$-dangereuse. Alors $\phi_n(\gamma_{k+1})\,\beta'_k$ est σ-positive de type $a_{1,n-1}$. Ainsi $\phi_n(\gamma_{k+1})\,\beta_k$ est σ-positive de type $a_{n-2,n-1}$.

Supposons finalement $\beta_k = a_{n-2,n-1}$. Comme la seule tresse $a_{n-2,n-1}$-dangereuse est triviale, la tresse $\phi_n(\gamma_{k+1})\,\beta_k$ est égale à $a_{n-2,n-1}$, une tresse σ-positive de type $a_{n-2,n-1}$.

Le même argument établit le cas $k = 2$ avec $\beta_2 \neq 1$. □

Nous arrivons au résultat technique de ce chapitre. Ce résultat affirme que, si une tresse β de B^{+*}_n à pour n-largeur b, alors la tresse $\widehat{\delta}^{-1}_{n,b-2} \cdot \beta$ est soit σ-positive soit triviale. En fait, le résultat est plus fort : l'information supplémentaire est premièrement que l'on peut contrôler le type du quotient ci-dessus, et deuxièmement qu'un résultat similaire est satisfait lorsqu'on remplace le terme le plus à gauche du ϕ_n-éclatement de β par une autre tresse de B^{+*}_{n-1} lui ressemblant suffisamment. Ce résultat plus fort, qui malheureusement rend l'énoncé plus compliqué, sera utilisé à la section 2 pour l'induction finale sur le nombre de brins n.

Proposition 2.7. *Supposons $n \geqslant 3$ et que $(\beta_b, \dots, \beta_1)$ soit le ϕ_n-éclatement d'une tresse β de B^{+*}_n avec $b \geqslant 3$. Notons $a_{q,n}$ la dernière lettre de $\beta\,\beta_1^{-1}$. Lorsque γ_b est une tresse σ-positive de type $\beta^{\#}_b$, la tresse*

$$\widehat{\delta}^{-1}_{n,b-2} \cdot \phi_n^{b-1}(\gamma_b) \cdot \phi_n^{b-2}(\beta_{b-1}) \cdot \dots \cdot \phi_n(\beta_2) \tag{5.2}$$

est triviale ou σ-positive de type $a_{q,n}$—le premier cas se produisant seulement pour $q = 1$.

Démonstration. Posons $\beta^* = \widehat{\delta}^{-1}_{n,b-2} \cdot \phi_n^{b-1}(\gamma_b) \cdot \phi_n^{b-2}(\beta_{b-1}) \cdot \dots \cdot \phi_n(\beta_2)$ et $a_{p-1,n-1} = \beta^{\#}_b$ (lemme III.3.2). D'abord décomposons le membre fragment gauche $\widehat{\delta}^{-1}_{n,b-2} \cdot \phi_n^{b-1}(\gamma_b)$ de β^* comme produit d'une tresse σ_{n-1}-nonnégative et d'une tresse dangereuse. Par définition d'une tresse σ-positive de type $\beta^{\#}_b$, on a

$$\gamma_b = \gamma_b^+\, d_{p-1,n-1}\, \gamma_b^-,$$

où γ_b^- est une tresse $\beta^{\#}_b$-dangereuse et où γ_b^+ est σ_{n-2}-nonnégative. En utilisant la proposition 1.8 (ii), on obtient

$$\widehat{\delta}^{-1}_{n,b-2} \cdot \phi_n^{b-1}(\gamma_b) = \delta_{n-1}^{b-2}\, \delta_n^{-b+2} \phi_n^{b-1}(\gamma_b^+\, d_{p-1,n-1})\, \phi_n^{b-1}(\gamma_b^-). \tag{5.3}$$

Par la relation (III.3.5), on a $\delta_n^{-b+2}\phi_n^{b-1}(\gamma_b^+\, d_{p-1,n-1}) = \phi_n(\gamma_b^+\, d_{p-1,n-1})\delta_n^{-b+2}$. En utilisant la relation $d_{p,n}\,\delta_n^{-1} = \delta_p^{-1}$, une conséquence directe de la relation (II.2.6), on obtient

$$\delta_n^{-b+2}\phi_n^{b-1}(\gamma_b^+\, d_{p-1,n-1}) = \phi_n(\gamma_b^+)\,\delta_p^{-1}\,\delta_n^{-b+3}. \tag{5.4}$$

En substituant (5.4) dans (5.3), on trouve

$$\widehat{\delta}_{n,b-2}^{-1}\cdot\phi_n^{b-1}(\gamma_b) = \delta_{n-1}^{b-2}\,\phi_n(\gamma_b^+)\,\delta_p^{-1}\,\delta_n^{-b+3}\,\phi_n^{b-1}(\gamma_b^-). \tag{5.5}$$

À partir de là, on déduit que β^* est égale à

$$\delta_{n-1}^{b-2}\,\phi_n(\gamma_b^+)\,\delta_p^{-1}\;\cdot\;\delta_n^{-b+3}\,\phi_n^{b-1}(\gamma_b^-)\,\phi_n^{b-2}(\beta_{b-1})\,...\,\phi_n(\beta_2). \tag{5.6}$$

Écrivons $\beta^{**} = \delta_n^{-b+3}\,\phi_n^{b-1}(\gamma_b^-)\,\phi_n^{b-2}(\beta_{b-1})\,...\,\phi_n(\beta_2)$. Notons que le facteur de gauche de (5.6), qui est $\delta_{n-1}^{b-2}\,\phi_n(\gamma_b^+)\,\delta_p^{-1}$, est σ_{n-1}-nonnégatif. À partir d'ici, quatre cas peuvent se produire.

Cas 1 : $\beta_2 \notin \{1, a_{n-2,n-1}\}$. Par le lemme IV.2.10, la tresse β^{**} est égale à $\beta''\,\phi_n^2(\gamma_3^-)\,\phi_n(\beta_2)\,\beta_1$, où β'' est une tresse σ_{n-1}-nonnégative et où γ_3^- est une tresse $\beta_3^{\#}$-dangereuse. Notons β_2' la tresse $\phi_n(\gamma_3^-)\,\beta_2$. Par la proposition 2.6, la tresse β_2' est σ-positive de type $\beta_2^{\#}$ et différente de $a_{n-2,n-1}$. On déduit que β^* est égale à

$$\delta_{n-1}^{b-2}\,\phi_n(\gamma_b')\,\delta_p^{-1}\,\beta''\;\cdot\;\phi_n(\beta_2'), \tag{5.7}$$

où le facteur de gauche est σ_{n-1}-nonnégatif, et où le facteur de droite, à savoir $\phi_n(\beta_2')$, est différent de $a_{n-1,n}$ et est σ-positif de type $\phi_n(\beta_2^{\#})$ par le lemme 2.2 (ii). Comme, dans ce cas, la dernière lettre de $\beta\,\beta_1^{-1}$ est $\phi_n(\beta_2^{\#})$, on conclut en utilisant le lemme 2.2 (iv).

Cas 2 : $\beta_2 \in \{1, a_{n-2,n-1}\}$, $\beta_3 = ... = \beta_{k-1} = a_{n-2,n-1}$ et $\beta_k \neq a_{n-2,n-1}$ pour $k \leqslant b-1$. Si β_2 est triviale, alors la dernière lettre de $\beta\,\beta_1^{-1}$ est $a_{1,n}$; sinon la dernière lettre de $\beta\,\beta_1^{-1}$ est $\phi_n(a_{n-2,n-1})$, c'est-à-dire, $a_{n-1,n}$—une conséquence directe du lemme III.3.2. Comme le produit d'une tresse σ-positive de type $a_{1,n}$ avec $a_{n-1,n}$ est une tresse σ-positive de type $a_{n-1,n}$, il est suffisant de montrer que la tresse β^* est le produit d'une tresse σ-positive de type $a_{1,n}$ avec la tresse $\phi_n(\beta_2)$. Par le lemme IV.2.10, la tresse β^{**} est égale à

$$\beta''\,\delta_n^{-k+2}\phi_n^k(\gamma_{k+1}^-)\,\phi_n^{k-1}(\beta_k)\,\phi_n^{k-2}(a_{n-2,n-1})\,...\,\phi_n^2(a_{n-2,n-1})\,\phi_n(\beta_2), \tag{5.8}$$

avec β'' une tresse σ_{n-1}-nonnégative et γ_{k+1}^- une tresse $\beta_{k+1}^{\#}$-dangereuse. La proposition 2.6 implique que la tresse $\phi_n(\gamma_{k+1}^-)\,\beta_k$ est σ-positive de type $\beta_k^{\#}$. Par le corollaire III.3.7, la dernière lettre de β_k est $a_{n-2,n-1}$. Alors, par le lemme 2.2 (ii) la tresse $\phi_n^2(\gamma_{k+1})\,\phi_n(\beta_k)$ est σ-positive de type $a_{n-1,n}$. Donc, par définition d'une tresse σ-positive de type $a_{n-1,n}$, on a la relation

$$\phi_n^2(\gamma_{k+1}^-)\,\phi_n(\beta_k) = \beta_k'\,\phi_n(a_{n-2,n-1}), \tag{5.9}$$

où β_k' est une tresse σ-positive de type $a_{1,n}$. Substituant (5.9) dans (5.8) on a que β^{**} est égale à

$$\beta''\,\delta_n^{-k+2}\phi_n^{k-2}(\beta_k')\,\phi_n^{k-1}(a_{n-2,n-1})\,\phi_n^{k-2}(a_{n-2,n-1})\,...\,\phi_n^2(a_{n-2,n-1})\,\phi_n(\beta_2).$$

En utilisant $\phi_n(a_{n-2,n-1})\,\delta_n^{-1} = \delta_{n-1}^{-1}$ et la relation (III.3.5), on obtient que le facteur de gauche de (5.6) est

$$\beta''\,\beta_k'\,\delta_{n-1}^{-k+2}\,\phi_n(\beta_2).$$

Comme β_k' est une tresse σ-positive de type $a_{1,n}$, le lemme 2.2 (iii) implique que $\beta_k'\,\delta_{n-1}^{-k+2}$ est σ-positive de type $a_{1,n}$, donc aussi $\beta''\beta_k'\,\delta_{n-1}^{-k+2}$, par le lemme 2.2 (iv). Ainsi, d'après la relation (5.6), la tresse β^* est le produit d'une tresse σ-positive de type $a_{1,n}$ avec $\phi_n(\beta_2)$.

Cas 3 : $\beta_2 \in \{1, a_{n-2,n-1}\}$, $\beta_3 = \ldots = \beta_{b-1} = a_{n-2,n-1}$ et $\gamma_b \neq a_{n-2,n-1}$. Comme dans le cas 2, il est suffisant de montrer que la tresse β^* est le produit d'une tresse σ-positive de type $a_{1,n}$ avec la tresse $\phi_n(\beta_2)$. En utilisant le lemme 1.8 (ii) et la relation (III.3.5) dans sa définition, la tresse β^* est égale à

$$\delta_{n-1}^{b-2} \cdot \phi_n(\gamma_b)\, \delta_n^{-1} \cdot \phi_n(a_{n-2,n-1})\, \delta_n^{-1} \cdot \ \ldots \ \cdot \phi_n(a_{n-2,n-1})\, \delta_n^{-1}\, \phi_n(\beta_2).$$

Par le corollaire III.3.7, la dernière lettre de β_b est $a_{n-2,n-1}$. La tresse γ_b est donc σ-positive de type $a_{n-2,n-1}$. Ainsi $\phi_n(\gamma_b)$ est σ-positive de type $a_{n-1,n}$ et est différente de $a_{n-1,n}$. Alors par définition d'une tresse σ-positive de type $a_{n-1,n}$, il existe une tresse σ-positive β'_b de type $a_{1,n}$ satisfaisant $\phi_n(\gamma_b) = \beta'_b\, a_{n-1,n}$. En utilisant $\phi_n(a_{n-2,n-1})\, \delta_n^{-1} = \delta_{n-1}^{-1}$, on déduit que la tresse β^* est égale à

$$\delta_{n-1}^{b-2} \cdot \beta'_b\, \delta_{n-1}^{-b+2} \cdot \phi_n(\beta_2). \tag{5.10}$$

Par le lemme 2.2 (iii), le facteur du milieu de (5.10), à savoir $\beta'_b\, \delta_{n-1}^{-b+2}$, est σ-positif de type $a_{1,n}$. La tresse β^* est donc le produit d'une tresse σ-positive de type $a_{1,n}$ avec $\phi_n(\beta_2)$.

Cas 4 : $\beta_2 \in \{1, a_{n-2,n-1}\}$, $\beta_3 = \ldots = \beta_{b-1} = a_{n-2,n-1}$ et $\gamma_b = a_{n-2,n-1}$. Par définition, on a

$$\beta^* = \delta_{n-1}^{b-2} \cdot \phi_n(a_{n-2,n-1})\, \delta_n^{-1} \ldots\ \phi_n(a_{n-2,n-1})\, \delta_n^{-1}\, \phi_n(\beta_2). \tag{5.11}$$

En utilisant $\phi_n(a_{n-2,n-1})\, \delta_n^{-1} = \delta_{n-1}^{-1}$ une fois de plus, on déduit $\beta^* = \phi_n(\beta_2)$. La tresse $\phi_n(\beta_2)$ est soit triviale soit égale à $a_{n-1,n}$, une tresse σ-positive de type $a_{n-1,n}$, comme désiré. □

Nous sommes maintenant prêts à démontrer le théorème 1.10, qui établit que si β, γ sont des tresses de B_n^{+*}, alors

$$\beta <^* \gamma \quad \text{implique} \quad \beta < \gamma, \tag{5.12}$$

où $<^*$ est l'ordre de la définition 1.3 et $<$ est l'ordre standard des tresses, c'est-à-dire, $\beta < \gamma$ signifie que la tresse quotient $\beta^{-1}\gamma$ est σ-positive.

Nous allons décomposer l'argument en trois étapes. On commence d'abord par remplacer le problème initial portant sur deux tresses arbitraires β, γ par deux autres, chacun d'eux ne faisant intervenir qu'une seule tresse. Pour cela, on utilise les tresses séparatrices $\widehat{\delta}_{n,t}$ de la définition 1.7, et on s'intéresse au problème de comparer une tresse arbitraire avec une tresse séparatrice $\widehat{\delta}_{n,t}$. Nous allons monter que

$$\beta <^* \widehat{\delta}_{n,t} \quad \text{implique} \quad \beta < \widehat{\delta}_{n,t} \tag{5.13}$$

$$\widehat{\delta}_{n,t} \leqslant^* \beta \quad \text{implique} \quad \widehat{\delta}_{n,t} \leqslant \beta \tag{5.14}$$

On a donc essentiellement trois choses à faire : montrer (5.13), montrer (5.14), et voir comment en déduire l'implication générale (5.12).

2.2 Démonstrations de (5.13) et (5.14)

On commence par l'implication (5.13). Afin de maintenir un argument d'induction dans la démonstration du théorème 1.10, nous allons démontrer une implication plus forte.

Proposition 2.8. *Pour $n \geqslant 3$, l'implication (5.13) est vraie. De plus la relation $\beta <^* \widehat{\delta}_{n,t}$ implique que $\beta^{-1}\, \widehat{\delta}_{n,t}$ est σ-positive de type $a_{1,n}$, pour $t \geqslant 1$.*

Démonstration. Prenons β dans B_n^{+*} et supposons $\beta <^* \widehat{\delta}_{n,t}$ pour $t \geqslant 0$. Soit $(\beta_b, \dots, \beta_1)$ le ϕ_n-éclatement de β. Par la proposition 1.8 (iii), on a nécessairement $b \leqslant t+1$. Si t vaut 0, alors la tresse β appartient à B_{n-1}^{+*} et le quotient $\beta^{-1}\widehat{\delta}_{n,0}$, qui est $\beta^{-1}\, a_{n-1,n}$, est σ-positif. Si les relations $t \geqslant 1$ et $b \leqslant 1$ sont satisfaites, alors la tresse β^{-1} est σ_{n-1}-nonnégative, et, comme la tresse $\widehat{\delta}_{n,t}$ est σ-positive de type $a_{1,n}$, le lemme 2.2 implique que le quotient $\beta^{-1}\widehat{\delta}_{n,t}$ est σ-positif de type $a_{1,n}$. Supposons maintenant $t \geqslant 1$ et $b \geqslant 2$. Alors, par la proposition 1.8 (ii), on trouve

$$\beta^{-1}\widehat{\delta}_{n,t} = \beta^{-1}\, \delta_n^t\, \delta_{n-1}^{-t} = \beta_1^{-1} \cdot \phi_n(\beta_2^{-1}) \dots\ \phi_n^{b-1}(\beta_b^{-1}) \cdot \delta_n^t \cdot \delta_{n-1}^{-t}.$$

En utilisant la relation (III.3.5), on pousse $(b-1)$ facteurs δ_n vers la gauche et on les intercale entre les facteurs β_k^{-1} :

$$\begin{aligned}\beta^{-1}\widehat{\delta}_{n,t} &= \beta_1^{-1}\, \phi_n(\beta_2^{-1}) \dots\ \phi_n^{b-2}(\beta_{b-1}^{-1})\, \phi_n^{b-1}(\beta_b^{-1})\, \delta_n^{b-1}\, \delta_n^{t-b+1}\, \delta_{n-1}^{-t}\\ &= \beta_1^{-1}\, \phi_n(\beta_2^{-1}) \dots\ \phi_n^{b-2}(\beta_{b-1}^{-1})\, \delta_n^{b-2}\, \delta_n\, \beta_b^{-1}\, \delta_n^{t-b+1}\, \delta_{n-1}^{-t}\\ &\dots\\ &= \beta_1^{-1}\, \delta_n\, \beta_2^{-1} \dots\ \delta_n\, \beta_{b-1}^{-1}\, \delta_n\, \beta_b^{-1}\, \delta_n^{t-b+1}\, \delta_{n-1}^{-t}.\end{aligned}$$

Comme B_{n-1}^{+*} est un monoïde de Garside, il existe un entier k tel que $\beta_b^{-1}\delta_{n-1}^k$ appartienne à B_{n-1}^{+*}. Notons la dernière tresse β_b'. Ainsi, on a $\delta_n\, \beta_b^{-1} = \delta_n\, \beta_b'\, \delta_{n-1}^{-k}$. La relation (III.3.5) implique $\delta_n\, \beta_b'\, \delta_{n-1}^{-k} = \phi_n(\beta_b')\, \delta_n\, \delta_{n-1}^{-k}$. Alors la tresse $\beta^{-1}\, \widehat{\delta}_{n,t}$ est égale à

$$\beta_1^{-1}\, \delta_n\, \beta_2^{-1} \dots\ \delta_n\, \beta_{b-1}^{-1}\, \phi_n(\beta_b')\ \cdot\ \delta_n\, \delta_{n-1}^{-k}\, \delta_n^{t-b+1}\, \delta_{n-1}^{-t}. \tag{5.15}$$

Comme chaque tresse β_k appartient à B_{n-1}, il en est de même de leurs inverses. Ainsi le facteur de gauche de (5.15), à savoir $\beta_1^{-1}\, \delta_n\, \beta_2^{-1} \dots\ \delta_n\, \beta_{b-1}^{-1}\, \phi_n(\beta_b')$, est σ_{n-1}-nonnégatif. Si b est égal à $t+1$, le facteur de droite de (5.15), à savoir $\delta_n\, \delta_{n-1}^{-k}\, \delta_n^{t-b+1}\, \delta_{n-1}^{-t}$, est égal à $\delta_n \cdot \delta_{n-1}^{-t-k}$, ce qui montre que c'est une tresse σ-positive de type $a_{1,n}$. Si $b \leqslant t$ est vérifiée, le facteur de droite dans le produit (5.15) se termine par $\delta_n\, \delta_{n-1}^{-t}$, qui est une tresse σ-positive de type $a_{1,n}$, et le facteur $\delta_n\, \delta_{n-1}^{-k}\delta_n^{t-b}$ est σ_{n-1}-nonnégative. Dans tous les cas, on conclut en utilisant le lemme 2.2 (iii) que $\beta^{-1}\widehat{\delta}_{n,t}$ est σ-positive de type $a_{1,n}$. □

En utilisant le lemme clé de la section 2.1, c'est-à-dire, la proposition 2.7, montrons maintenant l'implication (5.14).

Proposition 2.9. *Pour $n \geqslant 3$, l'implication (5.14) est vraie.*

Démonstration. Prenons β dans B_n^{+*} et supposons $\widehat{\delta}_{n,t} \leqslant^* \beta$. Soit $(\beta_b, \dots, \beta_1)$ le ϕ_n-éclatement de β. Par définition de $<^*$, la relation $\widehat{\delta}_{n,t} \leqslant^* \beta$ implique $t \leqslant b-2$. Alors $\widehat{\delta}_{n,t}^{-1}\, \beta$ est égale à

$$\widehat{\delta}_{n,t}^{-1}\, \widehat{\delta}_{n,b-2} \cdot \widehat{\delta}_{n,b-2}^{-1}\beta. \tag{5.16}$$

Par le lemme 1.9, le facteur $\widehat{\delta}_{n,t}^{-1}\, \widehat{\delta}_{n,b-2}$ de (5.16) est σ-positif ou trivial. Par le lemme 2.4, la tresse β_b est σ-positive de type $\beta_b^{\#}$. Alors, la proposition 2.7 assure que le facteur de droite de (5.16), à savoir $\widehat{\delta}_{n,b-2}^{-1}\, \beta$, est σ-positif ou trivial. □

2.3 Démonstration du théorème 1.10

À ce stade, nous savons que les implications (5.13) et (5.14) sont vraies. Il n'est alors pas difficile de montrer que l'implication (5.12), qui est notre but, est vraie lorsque la largeur de β est strictement plus petite que celle de γ, c'est-à-dire, lorsqu'on est dans le cas « `Short` » de l'ordre `ShortLex`.

Il reste donc à traiter le cas « `Lex` » , c'est-à-dire, lorsque β et γ ont la même n-largeur, et c'est ce que nous allons faire maintenant. En fait, comme on l'a déjà mentionné, pour maintenir une hypothèse d'induction, nous allons montrer une implication plus forte : au lieu de seulement montrer que la tresse quotient $\beta^{-1}\gamma$ est σ-positive, nous allons montrer le résultat plus précis que $\beta^{-1}\gamma$ est σ-positive de type $a_{p,n}$ pour un certain p dépendant de la dernière lettre de γ. C'est pourquoi nous devons considérer les cas « `Short` » et « `Lex` » simultanément.

Proposition 2.10. *Si β et γ sont deux tresses non triviales de B_n^{+*}, la relation $\beta <^* \gamma$ implique $\beta < \gamma$. De plus, si la B_{n-1}^{+*}-fin de γ est triviale, alors la tresse $\beta^{-1}\gamma$ est σ-positive de type $\gamma^{\#}$.*

Démonstration. Nous utilisons une induction sur n. Pour $n = 2$, tout est clair car les ordres $<$ et $<^*$ coïncident avec l'ordre usuel des entiers naturels.

Supposons $n \geqslant 3$, et $\beta <^* \gamma$ où β, γ appartiennent à B_n^{+*} et que β soit non triviale. La tresse γ est alors aussi non triviale. Soient $(\beta_b, \dots, \beta_1)$ et $(\gamma_c, \dots, \gamma_1)$ les ϕ_n-éclatements respectifs de β et γ. Comme la relation $\beta <^* \gamma$ est vérifiée, on a $b \leqslant c$. Posons $\beta_c = \dots = \beta_{b+1} = 1$. Soit t le plus grand entier dans $\{1, \dots, c\}$ satisfaisant $\beta_t <^* \gamma_t$. Par définition de $<^*$, un tel t existe. Posons $\gamma'_t = \beta_t^{-1}\,\gamma_t$. Par hypothèse d'induction, la tresse γ'_t est σ-positive. De plus, si on a $t \geqslant 2$, alors la tresse γ'_t est σ-positive de type $\gamma_t^{\#}$.

Supposons $t = 1$. Alors la tresse $\beta^{-1}\gamma$ est égale à γ'_t. Elle est donc σ-positive. Comme la B_{n-1}^{+*}-fin de γ_1 est non triviale, nous n'avons rien de plus à montrer.

Supposons maintenant $t \geqslant 2$. Soit $a_{q,n}$ la dernière lettre de

$$\phi_n^{t-1}(\gamma_t) \cdot \dots \cdot \phi_n(\beta_2).$$

La suite $(\beta_{t-1}, \dots, \beta_1)$ est un ϕ_n-éclatement d'une tresse de n-largeur $t-1$. Alors la proposition 2.8 implique que la tresse β', qui est égale à

$$\beta_1^{-1} \cdot \dots \cdot \phi_n^{t+1}(\beta_{t-1}^{-1}) \cdot \widehat{\delta}_{n,t-2},$$

est σ-positive de type $a_{1,n}$. Soit γ' la tresse

$$\widehat{\delta}_{n,t-2}^{-1} \cdot \phi_n^{t-1}(\gamma'_t) \cdot \phi_n^{t-2}(\gamma_{t-1}) \cdot \dots \cdot \phi_n(\gamma_2).$$

Comme γ'_t est σ-positive de type $\gamma_t^{\#}$, la proposition 2.7 implique que la tresse γ' est σ-positive de type $a_{q,n}$ ou triviale (le dernier cas se produisant seulement pour $q = 1$). Alors, dans tous les cas, la tresse $\beta'\,\gamma'$ est σ-positive de type $a_{q,n}$. Comme, par construction, on a $\beta^{-1}\gamma = \beta' \cdot \gamma' \cdot \gamma_1$, la tresse $\beta^{-1}\gamma$ est σ-positive. Supposons de plus que la B_{n-1}^{+*}-fin de γ est triviale. Alors γ_1 est triviale et la tresse γ se termine par $a_{q,n}$. Dans ce cas, on a $\beta^{-1}\gamma = \beta' \cdot \gamma'$, une tresse σ-positive de type $a_{q,n-1}$. Ainsi $\beta^{-1}\gamma$ est une tresse σ-positive de type $\gamma^{\#}$. □

La démonstration de la proposition 2.10 est donc terminée, et donc aussi la démonstration du théorème 1.10, qui en est une conséquence immédiate.

Nous avons donc une description complète de la restriction de l'ordre standard des tresses aux monoïdes de Birman–Ko–Lee B_n^{+*}. La caractérisation du théorème 0.1, qui est inductive, lie l'ordre $<$ sur B_n^{+*} à sa restriction sur B_{n-1}^{+*}. Une version non inductive est facilement réalisable. En effet, on peut définir *l'éclatement* itéré $T(\beta)$ d'une tresse β de B_n^{+*} comme étant un arbre obtenu en remplaçant les ϕ_{n-1}-éclatements des termes du ϕ_n-éclatement, et ainsi de suite, jusqu'à arriver à B_2^{+*}, c'est-à-dire, aux entiers naturels. De cette manière, on associe à toute tresse β de B_n^{+*} un arbre $T(\beta)$ avec des branches de hauteur $n-2$ et des feuilles étiquetées par les entiers naturels —voir [Deh08] pour une construction analogue. Alors le théorème 0.1 implique directement que, pour β, γ dans B_n^{+*}, la relation $\beta < \gamma$ est satisfaite si et seulement si l'arbre $T(\beta)$ est `ShortLex`-plus petit que l'arbre $T(\gamma)$.

Le point de départ de notre approche étant similaire à celui de [Deh08] et [Bur97], on peut se demander si les outils utilisés ici peuvent être adaptés au cas de B_n^+. Pour le moment cette question n'a pas de réponse. Cependant il semble que les notions d'échelles et de tresses dangereuses soient spécifiques aux monoïdes B_n^{+*} et dépendent de la redondance des relations liant les générateurs de Birman–Ko–Lee.

3 Application au problème de conjugaison

Le problème de conjugaison du groupe B_n est le problème de décider si deux tresses β, β' de B_n sont conjuguées, c'est-à-dire, s'il existe une tresse γ de B_n satisfaisant $\beta = \gamma^{-1}\,\beta\,\gamma$.

Depuis les travaux de F.A. Garside [Gar69], il est connu que le problème de conjugaison est algorithmiquement faisable. Cependant, à ce jour, toutes les solutions connues sont exponentielles en complexité. C'est la cas pour la solution originale de F.A. Garside, comme pour toutes les améliorations successives décrites par E.A. El-Rifai et H.R. Morton dans [ERM94], par N. Franco et J. González-Meneses dans [FGM03], et par J. González-Meneses et V. Gebhardt dans [GMG08].

Toutes les solutions citées ci-dessus sont basées sur la structure de Garside de B_n, soit celle associée au monoïde B_n^+ et à la tresse Δ_n, ou celle associée au monoïde B_n^{+*} et à la tresse δ_n.

Ce qui suit est un regroupement d'observations vraiment préliminaires, mais apparemment prometteuses, sur le lien entre l'ordre de Dehornoy $<$ des tresses et le problème de conjugaison des tresses. C'est un travail en commun avec V. Gebhardt.

3.1 Idée générale

L'idée est d'utiliser le fait que $(B_n^{+*}, <)$ soit bien ordonné pour essayer de résoudre le problème de conjugaison. Pour cela nous devons donc ramener le problème de conjugaison du groupe B_n au monoïde B_n^{+*}.

Définition 3.1. Pour β une tresse de B_n^{+*}, on note $C^{+*}(\beta)$ la famille de toutes les tresses $\gamma^{-1}\beta\gamma$ appartenant à B_n^{+*}, avec γ dans B_n^{+*}.

Comme la restriction de l'ordre standard des tresses à B_n^{+*} est un bon ordre, l'ensemble non vide $C^{+*}(\beta)$ contient un unique élément $<$-minimal. Cet élément sera noté $\mu^*(\beta)$ dans la suite.

Proposition 3.2. *Calculer μ^* sur B_n^{+*} permet de résoudre le problème de conjugaison sur B_n.*

Démonstration. Soient deux tresses β et β' de B_n. Comme B_n est le groupe de fractions du monoïde de Garside B_n^{+*}, il existe un entier k tel que les tresses $\delta_n^{nk}\beta$ et $\delta_n^{nk}\beta'$ appartiennent

à B_n^{+*}. Comme δ_n^{nk} est un élément du centre de B_n, pour une tresse γ de B_n on a

$$\beta = \gamma^{-1}\beta'\gamma \Leftrightarrow \delta_n^{nk}\delta_n^{-nk}\beta = \gamma^{-1}\beta'\gamma \Leftrightarrow (\delta_n^{nk}\beta) = \gamma^{-1}(\delta_n^{nk}\beta')\gamma.$$

Ainsi β et β' sont conjuguées si et seulement si $\delta_n^{nk}\beta$ et $\delta_n^{nk}\beta'$ le sont. Supposons qu'il existe γ dans B_n vérifiant

$$(\delta_n^{nk}\beta) = \gamma^{-1}(\delta_n^{nk}\beta')\gamma.$$

Montrons qu'il existe γ' dans B_n^{+*} vérifiant $(\delta_n^{nk}\beta) = \gamma'^{-1}(\delta_n^{nk}\beta')\gamma'$. Il existe ℓ tel que $\delta_n^{n\ell}\gamma$ soit une tresse de B_n^{+*}. Posons $\gamma' = \delta_n^{n\ell}\gamma$, alors, comme $\delta_n^{n\ell}$ est un élément du centre de B_n, on a

$$\gamma'^{-1}(\delta_n^{nk}\beta')\gamma' = \gamma^{-1}\delta_n^{-n\ell}(\delta_n^{nk}\beta')\delta_n^{n\ell}\gamma = \gamma^{-1}(\delta_n^{nk}\beta')\delta_n^{-n\ell}\delta_n^{n\ell}\gamma = \gamma^{-1}(\delta_n^{nk}\beta')\gamma.$$

On a donc montré que les tresses β et β' sont conjuguées si et seulement si β' appartient à l'ensemble $C^{+*}(\delta_n^{nk}\beta)$, ce qui revient à $C^{+*}(\delta_n^{nk}\beta) = C^{+*}(\delta_n^{nk}\beta')$, c'est-à-dire, à $\mu^{+*}(\beta) = \mu^{+*}(\beta')$. □

Construire un algorithme calculant la fonction μ^* sur B_n^{+*} donne une solution au problème de conjugaison sur B_n, avec la même complexité dès que la dernière est au moins quadratique. Réciproquement, la solution au problème de conjugaison décrite dans [GMG08] peut être utilisée en pratique pour calculer la fonction μ^*, en temps exponentiel.

3.2 Une idée qui n'aboutit pas

Ici nous présentons les idées que nous avons essayées afin de calculer μ^* pour $n = 3$ et qui n'aboutissent pas.

La notation suivante nous permettera d'alléger le texte :

Notation 3.3. Pour β une tresse de B_3^{+*} et x une A_3^+-lettre, on note β^x, la tresse $x^{-1}\beta x$.

Soit β une tresse de B_3^{+*}, les calculs de l'annexe A nous permettent de déterminer quelles lettres x de A_3^+ satisfont $\beta^x \in A_3^+$.

L'idée est, pour β une tresse de B_3^{+*}, d'obtenir la tresse $\mu^*(\beta)$ en conjuguant successivement par une lettre x de B_3^{+*} vérifiant $\beta^x \in B_3^{+*}$ et $\beta^x < \beta$. Plus précisement, on construit une suite $<$-décroissante $\beta_1, \dots, \beta_\ell$ de B_3^{+*} avec $\beta_1 = \beta$, telle que pour tout k il existe x dans A_3^+ vérifiant l'égalité $\beta_{k+1} = \beta_k^x$ et telle que β_ℓ^x soit plus grand que β_ℓ pour toute A_3^+-lettre x vérifiant la relation $\beta_\ell^x \in B_3^{+*}$.

Question 3.4. A-t-on $\beta_\ell = \mu(\beta)$?

Malheureusement la réponse est non. En effet, si on pose $\beta = a_{2,3}^2 a_{1,2}$, alors, grâce à l'annexe A, on a $\beta^{a_{1,2}} \notin B_3^{+*}$, $\beta^{a_{2,3}} = a_{2,3}a_{1,2}a_{2,3} > \beta$ et $\beta^{a_{1,3}} \notin B_3^{+*}$, tandis qu'on a la relation $\beta^{a_{2,3}a_{1,2}} = a_{2,3}a_{1,2}^2 < \beta$.

Le contre-exemple que l'on vient de voir, montre qu'il peut être nécessaire de conjuguer par une tresse de longueur 2 pour décroître vis-à-vis de l'ordre $<$.

Question 3.5. A-t-on une borne sur la longueur du conjugant γ de β pour que la tresse β^γ soit dans B_3^{+*} et satisfasse $\beta^\gamma < \beta$?

La réponse est certainement non. Expérimentalement la tresse $a_{2,3}^{3k}a_{1,2}^{3k-1}$ doit être conjuguée par $a_{1,3}a_{1,2}^{3k+2}$ afin d'obtenir un élément de B_3^{+*} plus petit.

Question 3.6. A-t-on une borne sur la 3-largeur du conjugant γ de β pour que la tresse β^γ soit dans B_3^{+*} et satisfasse $\beta^\gamma < \beta$?

La réponse est certainement non. En effet, expérimentalement, la tresse $a_{2,3}^{3k+1}a_{1,2}^{3k-2}$ doit être conjuguée par $\phi_3^{3k-2}(a_{1,2}) \cdot \dots \cdot a_{1,2}$ afin d'obtenir un élément de B_3^{+*} plus petit.

3.3 Un début de résultat pour 3 brins

N'ayant pas réussi à déterminer $\mu^*(\beta)$ pour β de B_3^{+*} par un algorithme simple, on cherche à reconnaître si une tresse β donnée vérifie $\mu^*(\beta) = \beta$.

Définition 3.7. Pour β une tresse de B_3^{+*}, on appelle *code de* β la suite $(e_b, \dots, e_1)$ où

$$\phi_3^{b-1}(a_{1,2}^{e_b}) \dots \phi_3^2(a_{1,2}^{e_2})\, a_{1,2}^{e_1}$$

est la forme normale tournante de β.

Tout d'abord nous avons le résultat suivant qui donne une condition nécessaire sur la 3-largeur de $\mu^*(\beta)$.

Lemme 3.8. *Pour β une tresse de B_3^{+*}, alors si la 3-largeur de $\mu(\beta)$ est différente de 1 elle n'est pas congrue à 1 modulo 3.*

Démonstration. Supposons que β soit une tresse de 3-largeur différente de 1 et congrue à 1 modulo 3. Notons $(e_b, \dots, e_1)$ le code de β. Alors la tresse $\beta' = \phi_3^{b-1}(a_{1,2}^{-e_b})\, \beta\, \phi_3^{b-1}(a_{1,2}^{e_b})$ est égale à

$$\phi_3^{b-2}(a_{1,2}^{e_{b-1}}) \cdot \dots \cdot \phi_3(a_{1,2}^{e_2}) \cdot a_{1,2}^{e_1+e_b}.$$

On vérifie immédiatement que $(e_{b-1}, \dots, e_1)$ est le code d'une tresse de B_3^{+*}. Ainsi la tresse β' appartient à B_3^{+*} et est de 3-largeur $b-1$. Il s'ensuit que la 3-largeur de $\mu^*(\beta)$ ne peut pas être b. □

D'après les expérimentations faites sur ordinateur il nous semble que la largeur de $\mu^*(\beta)$ ne peut pas être très inférieure à celle de β.

Lemme 3.9. *Pour β une tresse de B_3^{+*} de n-largeur $b \geqslant 2$ alors la n-largeur de la tresse $\beta\delta_3^6$ est égale à $b+6$.*

Démonstration. Le code de δ_3^6 est la suite $(1,1,1,1,1,1,0,6)$, qui est de longueur 8 et correspond au mot tournant $a_{2,3}a_{1,2}a_{1,3}a_{2,3}a_{1,2}a_{1,3}a_{1,2}^6$. Notons $(e_b, \dots, e_1)$ le code de β. On rappelle que $a_{[k]}$ désigne $a_{1,2}$ si k est congru à 1 modulo 3, $a_{2,3}$ s'il est congru à 2 modulo 3 et $a_{1,3}$ sinon. Comme δ_3^6 est dans le centre de B_3^{+*}, on a

$$\begin{aligned}
\beta\delta_3^6 &= a_{[b]}^{e_b} \dots a_{1,3}^{e_3} a_{2,3}^{e_2} a_{1,2}^{e_1} \cdot a_{2,3}a_{1,2}a_{1,3}a_{2,3}a_{1,2}a_{1,3}a_{1,2}^6 \\
&= a_{[b]}^{e_b} \dots a_{1,3}^{e_3} a_{2,3}^{e_2} a_{2,3}a_{1,2}a_{1,3}a_{2,3}a_{1,2}a_{1,3}a_{1,2}^6 a_{1,2}^{e_1} \\
&= a_{[b]}^{e_b} \dots a_{1,3}^{e_3} a_{2,3}^{e_2+1} a_{1,2}a_{1,3}a_{2,3}a_{1,2}a_{1,3}a_{1,2}^{e_1+6}.
\end{aligned}$$

La suite $(e_b, \dots, e_3, e_2+1, 1, 1, 1, 1, 1, 0, e_1+6)$ étant un code de longueur $b+6$, on déduit que la 3-largeur de $\beta\delta_3^6$ est $b+6$. □

Corollaire 3.10 ([DDRW08],chapitre II)**.** *Si deux tresses β, β' de B_n^+ sont conjuguées alors on a toujours $\beta' < \beta\delta_n^{2n}$.*

Proposition 3.11. *Pour toute tresse β de B_3^{+*} de 3-largeur b, la 3-largeur de $\mu(\beta)$ appartient à l'ensemble $\{b-5, \dots, b\}$.*

Démonstration. Si la n-largeur de $\mu(\beta)$ vaut 1 alors $\mu(\beta)$ est une puissance de $a_{1,2}$ et β est une puissance d'une A_3^+-lettre, ce qui implique $b \leqslant 3$.

Supposons que la n-largeur c de $\mu(\beta)$ soit supérieure ou égale à 2. Par le corollaire 3.10, on a $\beta < \mu(\beta)\delta_3^6$. Le théorème 1.10 assure alors que b est inférieur à la n-largeur de $\mu(\beta)\delta_3^6$. Le lemme 3.9 implique $b < c + 6$, c'est-à-dire, $b - 6 < c$. On conclut à l'aide de la relation évidente $\mu^*(\beta) \leqslant \beta$. □

Ce résultat est loin d'être une description complète de μ^*, mais il restreint sévèrement l'intervalle où $\mu^*(\beta)$ peut exister.

La prochaine étape devrait établir un lien entre les valeurs de μ^* pour des tresses suffisamment proches—ce qui pourrait donner un procédé de calcul par induction. Aucun résultat méritant d'être mentionné n'a été démontré pour le moment, mais, comme conclusion, nous mentionnons la conjecture suivante soutenue par l'expérimentation sur ordinateur :

Conjecture 3.12. *Pour toute tresse β de B_3^{+*}, on a $\mu(\delta_3^3\,\beta) = \delta_3^3\,a_{1,2}^{-3}\,\mu(\beta)\,a_{1,2}^3$.*

Nous rappelons que δ_3^3 est égale à Δ_3^2, un générateur du centre de B_3. Nous conjecturons aussi une formule similaire, $\mu(\Delta_3^2) = \Delta_3^2\sigma_1^{-2}\,\mu(\beta)\sigma_1^2$, où μ est une adaptation de μ^* à B_n^+.

Annexe A

Dans cette annexe nous décrivons la conjugaison d'une tresse de B_3^{+*} par une A_3^+-lettre. Nous rappelons la définition de code d'une tresse de B_3^{+*} :

Définition 3.13. Pour β une tresse de B_3^{+*}, on appelle *code de* β la suite $(e_b, \dots, e_1)$ où

$$\phi_3^{b-1}(a_{1,2}^{e_b}) \dots \phi_3^2(a_{1,2}^{e_2})\, a_{1,2}^{e_1}$$

est la forme normale tournante de β.

Par la proposition III.4.11 une suite d'entiers non nuls $(e_b, \dots, e_1)$ est le code d'une tresse de B_3^{+*} si et seulement si e_k est non nul pour $k \geqslant 3$. Pour un code de tresse s, on note $\beta(s)$ la tresse représentée par s.

Dans la liste ci-dessus, on note $s \rightsquigarrow \otimes$ si la tresse $\phi_3^{b-k}(a_{1,2}^{-1})\beta(s)\phi_3^{b-k}(a_{1,2})$ n'appartient pas à B_3^{+*} (k étant $-1, 0$ ou 1 en fonction du cas considéré). De même pour k valant $-1, 0$ ou 1 en fonction du cas considéré, on note $s \rightsquigarrow s'$ si la tresse $\phi_3^{b-k}(a_{1,2}^{-1})\beta(s)\phi_3^{b-k}(a_{1,2})$ appartient à B_3^{+*} et admet s' pour code—il se peut que l'on doive d'abord retirer le 0 le plus à gauche de s'.

Cette liste a été obtenue à l'aide du retournement et du corollaire II.3.27.

Cas 1 – Conjugaison par $\phi_3^{b-1}(a)$.

Si b est congru à 1 modulo 3 :
- $(e_1) \rightsquigarrow (e_1)$
- $(e_b, e_{b-1}, \dots, e_1) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_1{+}1)$

Si b est congru à 2 modulo 3 :
- $(e_2, 0) \rightsquigarrow (e_2, 0)$
- $(e_2, 1) \rightsquigarrow (1, 0, e_2)$
- $(e_2, e_{1\geqslant 2}) \rightsquigarrow (e_2{-}1, e_1{-}1, 1, 0, 1)$
- $(e_b, e_{b-1}, \dots, e_3, e_2, 0) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_3, e_2{+}1, 0)$
- $(e_b, e_{b-1}, \dots, e_3, e_2, 1) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_4, e_3{+}1, 0, e_2{+}1)$
- $(e_b, e_{b-1}, \dots, e_3, e_2, e_{1\geqslant 2}) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_2, e_1{-}1, 1, 0, 1)$

Si b est congru à 3 modulo 3 :
- $(e_3, e_2, 0) \rightsquigarrow (e_3, 0, e_2)$
- $(e_3, 0, 1) \rightsquigarrow (1, 1, 0, e_3{-}1)$
- $(e_b, \dots, e_3, e_2, 0) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_4, e_3{+}1, 0, e_2)$
- $(e_b, \dots, e_3, 0, 1) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_5, e_4{+}1, 1, 0, e_3)$
- $(\underbrace{1, \dots, 1}_{b-2}, 0, b{-}2) \rightsquigarrow (\underbrace{1, \dots, 1}_{b-1}, 0, b{-}3)$
- $(e_b, \dots, e_{k+2}, \underbrace{1, \dots, 1}_{k-1}, 0, k) \rightsquigarrow (e_b{-}1, e_{b-1} \dots, e_{k+4}, e_{k+3}{+}1, \underbrace{1, \dots, 1}_{k}, 0, e_{k+2}{+}k{-}1)$
- $(\underbrace{1, \dots, 1}_{b-2}, 0, e_{1\geqslant b-1}) \rightsquigarrow (e_1{-}b{+}3, \underbrace{1, \dots, 1}_{b-2}, 0, b{-}3)$

– $(2, \underbrace{1, \dots, 1}_{b-3}, 0, e_{1\geqslant b-1}) \rightsquigarrow (e_1{-}b{+}2, \underbrace{1, \dots, 1}_{b-1}, 0, b-2)$
– $(e_{b\geqslant}3, \underbrace{1, \dots, 1}_{b-3}, 0, e_{1\geqslant b-1}) \rightsquigarrow (e_b{-}2, e_1{-}b{+}2, \underbrace{1, \dots, 1}_{b-1}, 0, b-2)$
– $(e_b, \dots, e_{k+3}, e_{k+2\geqslant 2}, \underbrace{1, \dots, 1}_{k-1}, 0, e_{1\geqslant k+1}) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_{k+2}{-}1, e_1{-}k, \underbrace{1, \dots, 1}_{k+1}, 0, k)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, e_{1\geqslant 1}) \rightsquigarrow (e_b{-}1, e_{b-1}, \dots, e_1, 1, 0, 0)$

Cas 2 – Conjugaison par $\phi_3^b(a)$.

Si b est congru à 1 modulo 3 :
– $(e_1) \rightsquigarrow (e_1, 0, 0)$
– $(e_b, \dots, e_2, 0) \rightsquigarrow \otimes$
– $(e_b, \underbrace{1, \dots, 1}_{b-3}, 0, b{-}1) \rightsquigarrow (\underbrace{1, \dots, 1}_{b-2}, 0, e_b{+}b{-}2)$
– $(e_b, \dots, e_{k+2}, \underbrace{1, \dots, 1}_{k-1}, 0, k{+}1) \rightsquigarrow (e_b{+}1, e_{b-1}, \dots, e_{k+4}, e_{k+3}{+}1, \underbrace{1, \dots, 1}_{k-1}, 0, e_{k+2}{+}k{-}1)$
– $(e_b, \underbrace{1, \dots, 1}_{b-3}, 0, e_{1\geqslant b}) \rightsquigarrow (e_b, e_1{-}b{+}1, \underbrace{1, \dots, 1}_{b-2}, 0, b{-}2)$
– $(e_b, \dots, e_{k+3}, e_{k+2\geqslant 2}, \underbrace{1, \dots, 1}_{k-1}, 0, e_{1\geqslant k+2}) \rightsquigarrow$
$(e_b{+}1, e_{b-1}, \dots, e_{k+3}, e_{k+2}{-}1, e_1{-}k{-}1, \underbrace{1, \dots, 1}_{k}, 0, k)$
– $(e_b, \dots, e_2, 1) \rightsquigarrow (e_b{+}1, e_{b-1}, \dots, e_2)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, e_{1\geqslant 2}) \rightsquigarrow (e_b{+}1, e_{b-1}, \dots, e_2, e_1{-}1, 0, 0)$

Si b est congru à 2 modulo 3 :
– $(e_2, 0) \rightsquigarrow (e_2)$
– $(e_2, e_{1\geqslant 1}) \rightsquigarrow \otimes$
– $(e_b, \dots, e_3, 0, 0) \rightsquigarrow \otimes$
– $(e_b, \underbrace{1, \dots, 1}_{b-3}, 0, b{-}2) \rightsquigarrow (\underbrace{1, \dots, 1}_{b-2}, 0, e_b{+}b{-}3)$
– $(e_b, \dots, e_{k+2}, \underbrace{1, \dots, 1}_{k-1}, 0, k) \rightsquigarrow (e_b{+}1, \dots, e_{k+4}, e_{k+3}{+}1, \underbrace{1, \dots, 1}_{k-1}, 0, e_{k+2}{+}k{-}2)$
– $(e_b, \underbrace{1, \dots, 1}_{b-3}, 0, e_{1\geqslant b-1}) \rightsquigarrow (e_b, e_1{-}b{+}2, \underbrace{1, \dots, 1}_{b-2}, 0, b{-}3)$
– $(e_b, \dots, e_{k+3}, e_{k+2\geqslant 2}, \underbrace{1, \dots, 1}_{k-1}, 0, e_{1\geqslant k+1}) \rightsquigarrow$
$(e_b{+}1, e_{b-1}, \dots, e_{k+3}, e_{k+2}{-}1, e_1{-}k, \underbrace{1, \dots, 1}_{k}, 0, k{-}1)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, 0) \rightsquigarrow (e_b{+}1, e_{b-1}, \dots, e_3, e_2{-}1)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, e_{1\geqslant 1}) \rightsquigarrow \otimes$

Si b est congru à 3 modulo 3 :
– $(e_3, 0, e_1) \rightsquigarrow (e_3, e_1)$
– $(e_3, e_{2\geqslant 1}, e_1) \rightsquigarrow \otimes$
– $(e_b, \dots, e_3, 0, e_1) \rightsquigarrow (e_b{+}1, e_{b-1}, \dots, e_4, e_3{-}1, e_1)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, e_1) \rightsquigarrow \otimes$

Cas 3 – Conjugaison par $\phi_3^{b+1}(a)$.

Si b est congru à 1 modulo 3 :

– $(e_1) \rightsquigarrow \otimes$
– $(e_b, \dots, e_3, 0, 0) \rightsquigarrow \otimes$
– $(e_b, \underbrace{1, \dots, 1}_{b-3}, 0, b{-}2) \rightsquigarrow (2, \underbrace{1, \dots, 1}_{b-3}, 0, e_b{+}b{-}4)$
– $(e_b, \dots, e_{k+2}, \underbrace{1, \dots, 1}_{k-1}, 0, k) \rightsquigarrow (1, e_b, \dots, e_{k+4}, e_{k+3}{+}1, \underbrace{1, \dots, 1}_{k-1}, 0, e_{k+2}{+}k{-}2)$
– $(e_b, \dots, e_{k+3}, e_{k+2\geqslant 2}, \underbrace{1, \dots, 1}_{k-1}, 0, e_{1\geqslant k+1}) \rightsquigarrow (1, e_b, \dots, e_{k+3}, e_{k+2}{-}1, e_1{-}k, \underbrace{1, \dots, 1}_{k}, 0, k{-}1)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, 0) \rightsquigarrow (1, e_b, e_{b-1}, \dots, e_3, e_2{-}1)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, e_{1\geqslant 1}) \rightsquigarrow \otimes$

Si b est congru à 2 modulo 3 :
– $(e_b, \dots, e_3, 0, e_1) \rightsquigarrow (1, e_b, e_{b-1}, \dots, e_4, e_3{-}1, e_1)$
– $(e_b, \dots, e_3, e_{2\geqslant 1}, e_1) \rightsquigarrow \otimes$

Si b est congru à 3 modulo 3 :
– $(e_b, \dots, e_2, 0) \rightsquigarrow \otimes$
– $(e_b, \underbrace{1, \dots, 1}_{b-3}, 0, b{-}1) \rightsquigarrow (2, \underbrace{1, \dots, 1}_{b-3}, 0, e_b{+}b{-}3)$
– $(e_b, \dots, e_{k+2}, \underbrace{1, \dots, 1}_{k-1}, 0, k{+}1) \rightsquigarrow (1, e_b, \dots, e_{k+4}, e_{k+3}{+}1, \underbrace{1, \dots, 1}_{k-1}, 0, e_{k+2}{+}k{-}1)$
– $(e_b, \dots, e_{k+2\geqslant 2}, \underbrace{1, \dots, 1}_{k-1}, 0, e_{1\geqslant k+2}) \rightsquigarrow (1, e_b, \dots, e_{k+2}{-}1, e_1{-}k{-}1, \underbrace{1, \dots, 1}_{k}, 0, k)$
– $(e_b, \dots, e_2, 1) \rightsquigarrow (1, e_b, e_{b-1}, \dots, e_2)$
– $(e_b, \dots, e_{2\geqslant 1}, e_{1\geqslant 2}) \rightsquigarrow (1, e_b, e_{b-1}, \dots, e_2, e_1{-}1, 0)$

Références bibliographiques

[AD09] M Autord and P. Dehornoy. On the distance between the expressions of a permutation. Preprint, 2009.

[Art25] E. Artin. Theorie der Zöpfe. *Abh. Math. Sem. Univ. Hanburg*, 4:47–72, 1925.

[Art47] E. Artin. Theory of braids. *Ann. of Math. (2)*, 48:101–126, 1947.

[BDM02] D. Bessis, F. Digne, and J. Michel. Springer theory in braid groups and the Birman-Ko-Lee monoid. *Pacific J. Math.*, 205(2):287–309, 2002.

[Bes03] D. Bessis. The dual braid monoid. *Ann. Sci. École Norm. Sup. (4)*, 36(5):647–683, 2003.

[Big01] S. J. Bigelow. Braid groups are linear. *J. Amer. Math. Soc.*, 14(2):471–486 (electronic), 2001.

[Bir74] J. S. Birman. *Braids, links, and mapping class groups*. Princeton University Press, Princeton, N.J., 1974. Annals of Mathematics Studies, No. 82.

[BKL98] J. S. Birman, K. H. Ko, and S. J. Lee. A new approach to the word and conjugacy problems in the braid groups. *Adv. Math.*, 139(2):322–353, 1998.

[BMR98] M. Broué, G. Malle, and R. Rouquier. Complex reflection groups, braid groups, Hecke algebras. *J. Reine Angew. Math.*, 500:127–190, 1998.

[Bra01] T. Brady. A partial order on the symmetric group and new $K(\pi, 1)$'s for the braid groups. *Adv. Math.*, 161(1):20–40, 2001.

[Bre08] X. Bressaud. A normal form for braids. *J. Knot Theory Ramifications*, 17(6):697–732, 2008.

[BRS07] N. Brady, T. Riley, and H. Short. *The geometry of the word problem for finitely generated groups*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2007. Papers from the Advanced Course held in Barcelona, July 5–15, 2005.

[BS72] E. Brieskorn and K. Saito. Artin-Gruppen und Coxeter-Gruppen. *Invent. Math.*, 17:245–271, 1972.

[Bur94] S. Burckel. *L'ordre total sur les tresses positives*. PhD thesis, Université de Caen, 1994.

[Bur97] S. Burckel. The wellordering on positive braids. *J. Pure Appl. Algebra*, 120(1):1–17, 1997.

[CDW08] L. Carlucci, P. Dehornoy, and A. Weiermann. Unprovability results involving braids. preprint, 2008.

[Cha07] J. Chamboredon. Tresses, relaxation de lacet et forme normale de Bressaud. Mémoire de M2, Université de Caen, 2007.

[DDRW02] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest. *Why are braids orderable?*, volume 14 of *Panoramas et Synthèses [Panoramas and Syntheses]*. Société Mathématique de France, Paris, 2002.

[DDRW08] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest. *Ordering braids*, volume 148 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.

[Deh92] P. Dehornoy. Deux propriétés des groupes de tresses. *C. R. Acad. Sci. Paris Sér. I Math.*, 315(6):633–638, 1992.

[Deh94] P. Dehornoy. Braid groups and left distributive operations. *Trans. Amer. Math. Soc.*, 345(1):115–150, 1994.

[Deh97a] P. Dehornoy. A fast method for comparing braids. *Adv. Math.*, 125(2):200–235, 1997.

[Deh97b] P. Dehornoy. Groups with a complemented presentation. *J. Pure Appl. Algebra*, 116:115–137, 1997. Special volume on the occasion of the 60th birthday of Professor Peter J. Freyd.

[Deh00a] P. Dehornoy. *Braids and self-distributivity*, volume 192 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2000.

[Deh00b] P. Dehornoy. On completeness of word reversing. *Discrete Math.*, 225:93–119, 2000. Formal power series and algebraic combinatorics (Toronto, ON, 1998).

[Deh02] P. Dehornoy. Groupes de Garside. *Ann. Sci. École Norm. Sup. (4)*, 35(2):267–306, 2002.

[Deh03] P. Dehornoy. Complete positive group presentations. *J. Algebra*, 268(1):156–197, 2003.

[Deh08] P. Dehornoy. Alternating normal forms for braids and locally Garside monoids. *J. Pure Appl. Algebra*, 212(11):2413–2439, 2008.

[Del72] P. Deligne. Les immeubles des groupes de tresses généralisés. *Invent. Math.*, 17:273–302, 1972.

[DP99] P. Dehornoy and L. Paris. Gaussian groups and Garside groups, two generalisations of Artin groups. *Proc. London Math. Soc. (3)*, 79(3):569–604, 1999.

[DW06] P. Dehornoy and B. Wiest. On word reversing in braid groups. *Internat. J. Algebra Comput.*, 16(5):941–957, 2006.

[DW07] I. Dynnikov and B. Wiest. On the complexity of braids. *J. Eur. Math. Soc. (JEMS)*, 9(4):801–840, 2007.

[ECH+92] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992.

[ERM94] E. A. El-Rifai and H. R. Morton. Algorithms for positive braids. *Quart. J. Math. Oxford Ser. (2)*, 45(180):479–497, 1994.

[FGM03] N. Franco and J. González-Meneses. Conjugacy problem for braid groups and Garside groups. *J. Algebra*, 266(1):112–132, 2003.

[FGR+99] R. Fenn, M. T. Greene, D. Rolfsen, C. Rourke, and B. Wiest. Ordering the braid groups. *Pacific J. Math.*, 191(1):49–74, 1999.

[Gar69] F. A. Garside. The braid group and other groups. *Quart. J. Math. Oxford Ser. (2)*, 20:235–254, 1969.

[Gau] C. F. Gauß. Handbuch 7. Univ. Göttingen collection.

[Gd90] É. Ghys and P. de la Harpe, editors. *Sur les groupes hyperboliques d'après Mikhael Gromov*, volume 83 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1990. Papers from the Swiss Seminar on Hyperbolic Groups held in Bern, 1988.

[GMG08] J. González-Meneses and V. Gebhardt. On the cycling operation in braid groups. *Discrete Appl. Math.*, 156(16):3072–3090, 2008.

[Gro87] M. Gromov. Hyperbolic groups. In *Essays in group theory*, volume 8 of *Math. Sci. Res. Inst. Publ.*, pages 75–263. Springer, New York, 1987.

[Hig52] G. Higman. Ordering by divisibility in abstract algebras. *Proc. London Math. Soc. (3)*, 2:326–336, 1952.

[Höl01] O. Hölder. Die Axiome der Quantität und die Lehre vom Mass. *Math.Phys.Kl*, 53:1–64, 1901.

[Ito08] T. Ito. On finite thurston type orderings of braid groups, 2008. arXiv:0810.4074.

[Ito09] T. Ito. Finite thurston type orderings on dual braid monoids, 2009. arXiv:0902.0833.

[Jon87] V. F. R. Jones. Hecke algebra representations of braid groups and link polynomials. *Ann. of Math. (2)*, 126(2):335–388, 1987.

[Kra00] D. Krammer. The braid group B_4 is linear. *Invent. Math.*, 142(3):451–486, 2000.

[Kra02] D. Krammer. Braid groups are linear. *Ann. of Math. (2)*, 155(1):131–156, 2002.

[Kre72] G. Kreweras. Sur les partitions non croisées d'un cycle. *Discrete Math.*, 1(4):333–350, 1972.

[Lar94] D.M. Larue. *Left distributive and left-distributive idempotent algebras*. PhD thesis, University of Colorado, Boulder, 1994.

[Lav96] R. Laver. Braid group actions on left distributive structures, and well orderings in the braid groups. *J. Pure Appl. Algebra*, 108(1):81–98, 1996.

[Lév79] A. Lévy. *Basic set theory*. Springer-Verlag, Berlin, 1979.

[Mar47] A. Markoff. On the impossibility of certain algorithms in the theory of associative systems. *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, 55:583–586, 1947.

[Nav07] A. Navas. On the dynamics of (left) orderable groups, 2007. arXiv:0710.2466.

[Nie27] J. Nielsen. Untersuchungen zur topologie der geschlossenen zweiseitigen flächen. *Acta Math*, 50:189–358, 1927.

[Ore31] O. Ore. Linear equations in non-commutative fields. *Ann. of Math. (2)*, 32(3):463–477, 1931.

[Pos47] E. L. Post. Recursive unsolvability of a problem of Thue. *J. Symbolic Logic*, 12:1–11, 1947.

[Sib03] H. Sibert. *Algorithmique des tresses*. PhD thesis, Université de Caen, 2003.

[SW00] H. Short and B. Wiest. Orderings of mapping class groups after Thurston. *Enseign. Math. (2)*, 46:279–312, 2000.

[Tit66] J. Tits. Normalisateurs de tores. I. Groupes de Coxeter étendus. *J. Algebra*, 4:96–116, 1966.

Index des notions

Index des notations

Résumé de la thèse

Une tresse est une classe d'équivalence de mots de tresse. Diverses formes normales sur les tresses ont été décrites dans la littérature, c'est-à-dire, divers moyens de sélection, pour toute tresse, d'un mot de tresse distingué la représentant. Définie de façon naturelle sur les monoïdes de tresses de Birman–Ko–Lee (ou duaux), la forme normale tournante peut être étendue au groupe de tresses tout entier. Ici, nous donnons des contraintes de nature combinatoire satisfaites par cette nouvelle forme normale. Nous en obtenons ainsi une caractérisation et montrons que l'ensemble des formes normales tournantes des tresses duales constitue un langage régulier.

Un résultat de P. Dehornoy (1992) affirme que toute tresse non triviale admet un représentant sigma-défini. Ce résultat est à la base de la construction de l'ordre des tresses. À l'aide de la forme normale tournante et de ses propriétés, nous montrons que toute tresse admet un représentant sigma-défini de longueur quasi-géodésique, ce qui résout une question ouverte depuis une quinzaine d'années.

Un résultat de R. Laver montre que les monoïdes de Birman–Ko–Lee munis de l'ordre des tresses sont bien ordonnés mais laisse ouvert la détermination de leurs longueurs. À l'aide de la forme normale tournante, nous obtenons une caractérisation de l'ordre des tresses sur le monoïde de Birman–Ko–Lee à n brins à partir de sa restriction sur celui à $(n-1)$ brins. Une conséquence de ce résultat est une nouvelle démonstration du résultat de R. Laver ainsi que la détermination de la longueur des monoïdes de tresses duaux munis de l'ordre des tresses.

The rotating normal form of braids

Thesis summary

By definition, a braid is an equivalence class of braid words. Various normal forms have been described in the litterature, *i.e.*, various ways of selecting for each braid, a distinguished word that represents it. Naturally defined on the Birman–Ko–Lee monoids (or dual braid monoids), it can be extended to the whole braid group. Here, we give combinatoric constraints satified by this new normal form. From these, we obtain a characterization of the rotating normal form and show that the set of the rotating normal forms of dual braids is a regular language.

A result by P. Dehornoy (1992) states that each nontrivial braid admits a sigma-definite representative. This is the ground result for ordering braids. Thanks to the rotating normal form and its properties, we show that each braid admits a quasi-geodesic sigma-definite representative, which resolves a question opened for fifteen years.

A result by R. Laver states that the Birman–Ko–Lee monoids equipped with the braid ordering are well-ordered, but it leaves the determination of the lengths unsolved. Thanks to the rotating normal form, we obtain a characterization of the braid ordering on the n-strands Birman–Ko–Lee monoid from its restriction on the $(n-1)$-strands Birman–Ko-Lee monoid. A consequence of this result is a new proof of Laver's result and a determination of the length of the dual braid monoids equipped with the braid ordering.

Mots-clefs :

- **indexation Rameau :** Formes normales, théorie des tresses, algorithmes, monoïdes, ensembles ordonnés.
- **indexation libre :** Ordre des tresses, langage régulier, monoïdes de Birmna–Ko–Lee, structure de Garside.

Discipline : mathématiques et leurs interactions

Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139,
Université de Caen/Basse-Normandie BP 5186
14032 CAEN Cedex, FRANCE