



HAL
open science

Problèmes algorithmiques dans les groupes de tresses

Matthieu Calvez

► **To cite this version:**

Matthieu Calvez. Problèmes algorithmiques dans les groupes de tresses. Théorie des groupes [math.GR]. Université Rennes 1, 2012. Français. NNT: . tel-00718633

HAL Id: tel-00718633

<https://theses.hal.science/tel-00718633>

Submitted on 17 Jul 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de
DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et applications

Ecole doctorale Matisse

présentée par

Matthieu Calvez

préparée à l'unité de recherche 6625 du CNRS : IRMAR
Institut de Recherche Mathématique de Rennes
UFR de Mathématiques

**Problèmes
algorithmiques
dans les groupes
de tresses**

**Thèse soutenue à Rennes
le 12 juillet 2012**

devant le jury composé de :

Michel BOILEAU

Professeur, Univ. Toulouse 3 / *examineur*

Françoise DAL'BO

Professeur, Univ. Rennes 1 / *examineur*

Eddy GODELLE

MCF, Univ. Caen / *rapporteur*

Luis PARIS

Professeur, Univ. Dijon / *examineur*

José Luis VICENTE CÓRDOBA

Prof. Catedrático, Univ. Sevilla / *examineur*

Juan GONZÁLEZ-MENESES LÓPEZ

Prof. Titular, Univ. Sevilla / *directeur de thèse*

Bert WIEST

MCF, Univ. Rennes 1 / *directeur de thèse*

**PROBLÈMES ALGORITHMIQUES
DANS LES GROUPES DE TRESSES**

**PROBLEMAS ALGORÍTMICOS EN
LOS GRUPOS DE TRENZAS**

À Marie-Claude et Pierre-Yves

Remerciements

Bert Wiest et Juan González-Meneses m'ont fait l'honneur d'encadrer cette thèse. C'est tout naturel d'adresser à tous deux ma plus vive reconnaissance. Tantôt inspirateurs, tantôt correcteurs stricts et vigilants, ils auront contribué, avec une patience inépuisable et une disponibilité sans faille, à l'aboutissement de ce travail. Leur soutien administratif pour gérer le surplus de formalités lié à l'organisation de la cotutelle a été précieux.

Mes remerciements s'adressent aussi à Eddy Godelle et à Daan Krammer, qui ont accepté de relire ce travail ; leurs commentaires précis et détaillés ont permis d'en améliorer la qualité. A Françoise Dal'Bo, Michel Boileau, Luis Paris et José Luis Vicente Córdoba, je suis profondément reconnaissant d'avoir accepté l'invitation à faire partie du jury de cette thèse.

Pour leur soutien administratif et documentaire, je tiens à remercier ici Claude Boschet, Maryse Collin, Marie-Annick Guillemer, Emmanuelle Guiot, Chantal Halet, Dominique Hervé, Marie-Annick Paulmier, Patrick Pérez, Lola Pérez García, Hélène Rousseaux et Marie-Aude Verger.

Ces trois ans m'ont apporté une première confrontation avec le métier d'enseignant. Je remercie particulièrement Lionel Fourquaux et Christophe Mourougane ; le TD de Théorie des Nombres a été une expérience extrêmement enrichissante. Je remercie aussi vivement tous ceux qui par le passé ont contribué à me donner goût à leur discipline ; je pense spécialement à M. Bernard Petit.

Un grand merci à tous les collègues rennais, en particulier aux thésards et notamment à Gaël, mon cobureau depuis le Master. Merci aussi à tous les membres du Département d'Algèbre de l'Université de Seville. Mille mercis à Marta pour ses apports innombrables en de multiples domaines.

Je dis ma reconnaissance, pour leur accueil toujours chaleureux, à Max et Solenn, à Alan, Anne-Lise, Sabrina, Dongli et à Jelena. Merci aussi à tous ceux –mathématiciens ou non– avec qui, ici ou là, j'ai passé de bons moments et qui ont contribué à me rendre la vie plus agréable.

Enfin, ma plus grande gratitude va à ma famille, les proches et les moins proches. Je remercie tout particulièrement ma petite soeur Maÿliss et mes parents ; leur confiance et leur soutien toujours renouvelés m'ont porté jusqu'ici.

Agradecimientos

Bert Wiest y Juan González-Meneses me han hecho el honor de dirigir esta tesis. Es muy natural enviar a ambos mi reconocimiento más vivo. Unas veces inspiradores y otras correctores estrictos y vigilantes, habrán contribuido, con una paciencia inagotable y una disponibilidad total, al resultado de este trabajo. Su apoyo administrativo para afrontar el exceso de formalidades vinculado a la organización de la cotutela fue precioso.

Mis agradecimientos se dirigen también a Eddy Godelle y a Daan Krammer, que aceptaron releer este trabajo. Sus comentarios precisos y detallados permitieron mejorar la calidad de esta tesis. A Françoise Dal'Bo, Michel Boileau, Luis Paris y José Luis Vicente Córdoba, les estoy profundamente agradecido por haber aceptado la invitación para formar parte del jurado de esta tesis.

Por su apoyo administrativo y documental, quiero agradecer aquí a Claude Boschet, Maryse Collin, Marie-Annick Guillemer, Emmanuelle Guiot, Chantal Halet, Dominique Hervé, Marie-Annick Paulmier, Patrick Pérez, Lola Pérez García, Hélène Rousseaux y Marie-Aude Verger.

Estos tres años me aportaron una primera confrontación con el oficio de profesor. Particularmente agradezco a Lionel Fourquaux y Christophe Mourougane: las prácticas de Teoría de Números fueron una experiencia extremadamente enriquecedora. Agradezco tan vivamente a todos los que en el pasado contribuyeron dándome gusto por su disciplina; pienso especialmente en el señor D. Bernard Petit.

Un gran agradecimiento a todos los colegas de Rennes, en particular a los doctorantes entre los cuales está Gaël, mi compañero de despacho desde el Máster. Gracias también a todos los miembros del Departamento de Álgebra de la Universidad de Sevilla. Mil gracias a Marta por sus aportaciones innumerables en múltiples campos.

Doy mi reconocimiento, por su acogida siempre calurosa, a Max y Solenn, a Alan, Anne-Lise, Sabrina, Dongli y a Jelena. Gracias también a todos –matemáticos o no– con quien, aquí o allí, he pasado buenos momentos y que han contribuido a hacerme la vida más agradable.

Por último, mi gratitud va a mi familia, los allegados y los menos próximos. Agradezco muy particularmente a mi hermanita Maÿliss y a mis padres; su confianza y apoyo siempre renovados me llevaron hasta aquí.

Table des matières

Introduction	13
Introducción en español	17
Chapitre 1. Groupes modulaires et la classification de Nielsen-Thurston	1
1.1. Le groupe modulaire	1
1.2. Le groupe des tresses comme groupe modulaire	3
1.3. La classification de Nielsen-Thurston et la borne linéaire	6
Chapitre 2. Groupes de Garside, le problème de conjugaison	9
2.1. Groupes de Garside	9
2.2. Le groupe de tresses et ses deux structures de Garside	11
2.3. Le problème de conjugaison dans les groupes de Garside	14
Chapitre 3. Le problème de réductibilité : travaux antérieurs	21
3.1. Réductible ou pseudo-Anosov	21
3.2. Courbes rondes et standardisation	22
3.3. Le théorème de Benardete, Gutierrez et Nitecki	23
3.4. L'algorithme de González-Meneses et Wiest	25
Chapitre 4. Le problème de réductibilité : courbes rondes et la structure classique	27
4.1. Esquisse de la preuve	27
4.2. Des mots pour décrire les courbes	28
4.3. L'action des tresses positives	28
4.4. Preuve du théorème principal	31
Chapitre 5. Le problème de réductibilité : courbes standard et la structure duale	35
5.1. Enoncé du théorème principal, esquisse de la démonstration	35
5.2. Des mots pour décrire les courbes de \mathbb{D}_n	36
5.3. L'action des tresses duales positives	37
5.4. Preuve du théorème principal	40
5.5. Reconnaissance algorithmique de courbes de réduction standard	42
Chapitre 6. Le problème de réductibilité : le cas des tresses à 4 brins	45
6.1. Enoncé des principaux résultats	45
6.2. Description de l'algorithme	45
6.3. La réductibilité est aisée à détecter dans le Super Summit Set	49
Chapitre 7. Le problème de réductibilité et la propriété de borne linéaire	59
7.1. La borne linéaire sur les éléments conjugués	59
7.2. Un nouvel algorithme pour le problème de réductibilité	61
Chapitre 8. Le problème de conjugaison des tresses à 4 brins	63
8.1. Enoncé des principaux résultats	63
8.2. Etude des éléments pseudo-Anosov rigides de BKL_4	64
8.3. Validité des algorithmes	71
Bibliographie	73

Introduction

Les groupes de tresses sont à l'intersection de deux familles de groupes : d'une part celle des groupes modulaires de surfaces et d'autre part celle des groupes de Garside.

Le groupe modulaire d'une surface orientable S (noté $Mod(S)$) est le groupe des classes d'isotopie d'homéomorphismes de S qui préservent l'orientation. Lorsque $S = \mathbb{D}_n$ est le disque fermé percé de n trous ($n \in \mathbb{N}$), le groupe modulaire correspondant est un quotient du groupe de tresses usuel. Plus précisément, le groupe de tresses B_n est isomorphe au groupe des classes d'isotopie d'homéomorphismes de \mathbb{D}_n préservant l'orientation et induisant l'identité sur $\partial\mathbb{D}_n$, voir [5]. Dans ce contexte, le groupe modulaire de \mathbb{D}_n est isomorphe au quotient de B_n par le sous-groupe engendré par l'élément qui correspond à la rotation d'angle 2π de l'intérieur du disque.

Les groupes de Garside possèdent une structure de treillis ainsi qu'un élément spécial Δ qui jouissent de certaines propriétés initialement découvertes par Garside dans le cadre des groupes de tresses. Tout élément admet une unique *forme normale*, c'est à dire une unique décomposition de la forme $\Delta^p x_1 \dots x_r$ où les facteurs appartiennent à l'ensemble des éléments dits *simples*. Sont des groupes de Garside les groupes d'Artin de type sphérique (dont le groupe des tresses est un spécimen), les groupes de noeud torique $\langle x, y | x^p = y^q \rangle$ (p et q premiers entre eux), les groupes abéliens libres, et d'autres exemples de groupes (voir [22], [20], [46]).

Les problèmes du mot et de la conjugaison sont deux célèbres problèmes décisionnels posés par Max Dehn au début du vingtième siècle. On considère un groupe avec une présentation finie $G = \langle S | R \rangle$ fixée. Le problème du mot requiert un algorithme pour décider si un mot sur $S \cup S^{-1}$ représente l'élément neutre de G ou non. Le problème de conjugaison demande un algorithme pour décider si deux tels mots représentent ou non la même classe de conjugaison.

Tant dans les groupes modulaires de surfaces que dans les groupes de Garside, ces deux problèmes sont résolubles. Dans les deux classes, les groupes sont automatiques (et même biautomatiques pour les groupes de Garside), voir [45] pour $Mod(S)$ et [20] pour les groupes de Garside. Cela implique une solution en temps quadratique par rapport à la longueur des entrées pour le problème du mot (voir par exemple [49]).

Le problème de conjugaison est résoluble pour les groupes modulaires, en combinant l'automaticité et la propriété de borne linéaire sur la longueur des éléments conjugués établie par Masur-Minsky et Jing Tao [44, 48]; notons que l'algorithme obtenu est de complexité exponentielle.

Pour les groupes de Garside, la première solution au problème de conjugaison fut donnée par Garside en 1969 dans le cadre des groupes de tresses [30] en se basant sur les propriétés combinatoires sus-mentionnées. Nonobstant de nombreuses améliorations techniques, l'esprit de la démonstration de Garside persiste dans les algorithmes connus à ce jour. Malgré la rapidité en pratique des algorithmes développés récemment, la complexité connue actuellement est exponentielle ici aussi.

Un des résultats de cette thèse est l'obtention d'un algorithme de complexité polynômiale dans le cas du groupe des tresses à 4 brins (voir chapitre 8) :

THÉORÈME. [14] (Voir théorème 8.1.1). *Il existe un algorithme qui décide si deux éléments x et y de B_4 sont conjugués dans B_4 et qui fournit le cas échéant un élément conjugué. Sa complexité est cubique par rapport à la longueur des entrées.*

L'argument s'appuie sur le programme de Birman, Gebhardt et González-Meneses en vue d'une solution polynômiale au problème de conjugaison dans les groupes de tresses [6]. L'idée est d'utiliser le théorème de classification de Nielsen-Thurston des éléments du groupe modulaire d'une surface [16, 27]. Tout homéomorphisme f d'une surface S satisfait à isotopie près exactement l'une des propriétés suivantes :

- f est *périodique* si f est d'ordre fini,
- f est *réductible* s'il existe une famille non vide \mathcal{F} (appelée système de réduction) de classes d'isotopie de courbes fermées simples disjointes dans S telle que
 - l'action de f laisse \mathcal{F} invariant.
 - \mathcal{F} n'intersecte aucune autre classe d'isotopie de courbes fermées simples de S préservée par une puissance de f ,
- f est *pseudo-Anosov* (pA) sinon.

Cette classification subsiste pour les tresses : une tresse est périodique, réductible ou pseudo-Anosov si telle est sa projection dans le groupe modulaire de \mathbb{D}_n . L'idée dans [6] est de résoudre le problème de conjugaison séparément pour chacun des types de la classification ci-dessus. Afin de pouvoir procéder à cette résolution spécifique, il faut d'abord résoudre le nouveau problème algorithmique suivant : décider le type de Nielsen-Thurston d'un élément donné de $Mod(S)$, pour une surface S , et en particulier déterminer le type de Nielsen-Thurston d'une tresse. Une première réponse est donnée via la théorie des réseaux ferroviaires [3], mais l'algorithme subséquent est de complexité inconnue.

Une autre approche, dans le cas spécifique des groupes de tresses, est l'utilisation des techniques de Garside. Le résultat principal reliant le problème de décision du type de Nielsen-Thurston d'une tresse et la structure de groupe de Garside est le théorème suivant, dû à Benardete, Gutierrez et Nitecki :

THÉORÈME. [13] (Voir théorèmes 3.3.1 et 5.1.3). *Soit \mathcal{C} une courbe standard. Soit $x = \Delta^p x_1 \dots x_r$ une tresse en forme normale, classique ou duale. Si \mathcal{C}^x est standard, alors pour tout $m = 1, \dots, r$, $\mathcal{C}^{\Delta^p x_1 \dots x_m}$ est standard.*

Nous présentons au chapitre 4 une nouvelle preuve de ce résultat, plus élémentaire que l'originale, et dont le mérite supplémentaire est de s'étendre (voir chapitre 5) au cadre de la structure de Garside duale [4]. Le théorème précédent implique que si $x \in B_n$ est une tresse réductible, il existe un élément du Super Summit Set de x qui admet un système de réduction constitué de classes d'isotopies de cercles (des courbes *rondes* ou *standard*); de plus, cette dernière propriété peut être décidée aisément [2].

Le *Super Summit Set* de $x \in B_n$ ($SSS(x)$) est un sous-ensemble fini invariant de la classe de conjugaison de x calculable à l'aide des techniques de Garside [24]. L'algorithme résultant du paragraphe précédent pour détecter la réductibilité de $x \in B_n$ exige de calculer l'intégralité de $SSS(x)$ et cela est très lent, puisque en général la taille du Super Summit Set croît exponentiellement avec la longueur. En revanche il existe un algorithme quadratique pour calculer, à partir de $x \in B_n$, un élément de $SSS(x)$ [9].

Dans le cas particulier du groupe des tresses à 4 brins, nous démontrons que *tout* élément du Super Summit Set d'une tresse réductible admet une courbe de réduction (presque)-standard. Cela fournit un algorithme quadratique pour décider le type de Nielsen-Thurston d'une tresse à 4 brins donnée. Ce résultat est une étape clé dans la justification de notre algorithme pour résoudre le problème de conjugaison dans le groupe des tresses à 4 brins. Nous démontrons au chapitre 6 le :

THÉORÈME. [15] (Voir théorème 6.1.1). *Il existe un algorithme qui décide le type de Nielsen-Thurston d'une tresse x à 4 brins avec une complexité quadratique par rapport à la longueur de x .*

Dans le cas général d'un nombre arbitraire de brins, González-Meneses et Wiest ont produit un algorithme qui décide le type de Nielsen-Thurston d'une tresse donnée, de complexité polynômiale

par rapport au nombre de brins et à la longueur, modulo une conjecture sur la rapidité de convergence d'une opération de théorie de Garside appelée *cyclic sliding* [33], voir Conjecture 2.3.9. Nous donnons une preuve partielle de cette conjecture, basée sur la propriété sus-mentionnée de borne linéaire sur les éléments conjuguants (voir chapitre 7). Cela permet une modification de l'algorithme de González-Meneses et Wiest, qui conduit à un algorithme de complexité polynômiale par rapport à la longueur, pour tout nombre de brins fixé :

THÉORÈME. [12] (Voir théorème 7.2.1). *Soit n un entier naturel. Il existe un algorithme qui décide le type de Nielsen-Thurston d'une tresse x à n brins et dont la complexité est quadratique par rapport à la longueur de x .*

Malheureusement la constante dans la borne linéaire n'est à présent pas explicitement connue, de sorte que l'algorithme en question ne peut être explicitement programmé. L'importance de ladite constante se manifeste à nouveau au chapitre 8, où est utilisée une deuxième fois la borne linéaire sur les éléments conjuguants. Cela intervient dans la preuve du résultat suivant, une des clés pour notre solution au problème de conjugaison dans B_4 :

THÉORÈME. [14] (Voir théorème 8.1.2). *Pour tout $x \in B_4$ pseudo-Anosov rigide par rapport à la structure duale, le cardinal de $SC(x)$ pour la structure duale est borné supérieurement par $O(\ell(x)^2)$.*

Les notions de rigidité, d'ensembles de circuits glissants (SC) ainsi que tous les prérequis nécessaires de la théorie de Garside sont regroupés au chapitre 2. Là encore, on remarque que la méconnaissance d'une valeur explicite pour la constante intervenant dans la borne linéaire (même dans le cas du groupe des tresses à 4 brins) ne permet d'obtenir qu'un ordre de grandeur et pas une borne explicite sur la valeur du cardinal de l'ensemble des circuits glissants.

Introducción en español

Los grupos de trenzas pertenecen a dos familias importantes de grupos: la de los grupos de difeotopía de superficies (ó Mapping Class Groups) y la de los grupos de Garside.

El grupo de difeotopía de una superficie orientable S (que denotamos por $\mathcal{MCG}(S)$) es el grupo de clases de isotopía de homeomorfismos de S que preservan la orientación. Cuando $S = \mathbb{D}_n$ es el disco cerrado menos n puntos interiores, este grupo es un cociente del grupo de trenzas usual. Más precisamente, el grupo de trenzas B_n es isomorfo al grupo de las clases de isotopía de homeomorfismos de \mathbb{D}_n que preservan la orientación e inducen la identidad al restringirlos al borde $\partial\mathbb{D}_n$, ver [5]. En ese contexto, el grupo de difeotopía de \mathbb{D}_n es isomorfo al cociente de B_n por el subgrupo generado por el elemento que corresponde a la rotación del interior del disco por un ángulo de 2π .

Los grupos de Garside poseen una estructura de retículo y un elemento especial Δ que satisfacen ciertas propiedades inicialmente descubiertas por Garside en el contexto de los grupos de trenzas. Todo elemento admite una única *forma normal*, es decir una única descomposición de la forma $\Delta^p x_1 \dots x_r$ donde los factores pertenecen al conjunto de los elementos llamados *simples*. Los grupos de Artin de tipo esférico (por ejemplo el grupo de trenzas), los grupos de nudos tóricos $\langle x, y | x^p = y^q \rangle$ (p y q primos entre sí), los grupos abelianos libres, y muchos otros son ejemplos de grupos de Garside (ver [22], [20], [46]).

Los problemas de la palabra y de la conjugación son dos problemas famosos planteados por Max Dehn a principios del siglo XX. Se considera un grupo dado por una presentación finita $G = \langle S \mid R \rangle$. El problema de la palabra requiere un algoritmo para decidir si una palabra sobre $S \cup S^{-1}$ representa el elemento trivial del grupo G o no. El problema de la conjugación requiere un algoritmo para decidir si dos tales palabras representan o no la misma clase de conjugación.

Tanto en los grupos de difeotopía de superficies como en los grupos de Garside, estos dos problemas son resolubles. En ambas clases, los grupos son automáticos (e incluso los grupos de Garside son biautomáticos), ver [45] en el caso de $Mod(S)$ y [20] para los grupos de Garside. Esto implica una solución de complejidad cuadrática con respecto a la longitud de las entradas para el problema de la palabra (ver por ejemplo [49]).

El problema de la conjugación es resoluble para los grupos de difeotopía de superficies, al combinar la automaticidad y la propiedad de cota lineal sobre la longitud de los elementos conjugadores establecida por Masur-Minsky y Jing Tao [44, 48]; notamos que el algoritmo resultante es de complejidad exponencial.

Para los grupos de Garside, la primera solución al problema de la conjugación fue encontrada por Garside en 1969 en el contexto de los grupos de trenzas [30], basándose en las propiedades combinatorias mencionadas anteriormente. A pesar de numerosas mejoras técnicas, el espíritu de la demostración de Garside persiste en los algoritmos conocidos hoy en día. Los más recientes de estos algoritmos son en práctica muy rápidos. Sin embargo, su mejor complejidad teórica sigue siendo de orden exponencial.

Un resultado de esta tesis es la obtención de un algoritmo de complejidad cúbica en el caso del grupo de trenzas con cuatro cuerdas (Capítulo 8):

TEOREMA. [14] (Ver Teorema 8.1.1). *Existe un algoritmo que decide si dos elementos x e y de B_4 son conjugados o no y que produce si se da el caso un conjugador entre x e y . Su complejidad es cúbica con respecto a la longitud de las entradas.*

El argumento se apoya en el proyecto de Birman, Gebhardt y González-Meneses para obtener una solución polinomial al problema de la conjugación en los grupos de trenzas [6]. La idea es utilizar el teorema de clasificación de Nielsen-Thurston de los elementos del grupo de difeotopía de una superficie [16,27]. Todo homeomorfismo de una superficie S satisface modulo isotopía exactamente una de las siguientes propiedades:

- f es *periódico* si f tiene orden finito,
- f es *reducible* si existe una familia non vacía \mathcal{F} (llamada sistema de reducción) de clases de isotopía de curvas simples cerradas disjuntas en S tal que
 - la acción de f deja \mathcal{F} invariante,
 - \mathcal{F} no intersecta ninguna otra clase de isotopía de curvas simples cerradas de S preservada por una potencia de f ,
- f es *pseudo-Anosov* (pA) en otro caso.

Esta clasificación persiste para las trenzas: una trenza es periódica, reducible o pseudo-Anosov si lo es su proyección en el grupo de difeotopía de \mathbb{D}_n . La idea en [6] es resolver el problema de la conjugación separadamente en cada uno de los tipos de esta clasificación. Para poder hacerlo, es necesario resolver primero el nuevo problema algorítmico que aparece: decidir el tipo de Nielsen-Thurston de un elemento de $Mod(S)$, para una superficie S , y en particular, determinar el tipo de Nielsen-Thurston de una trenza. Una primera respuesta fue dada vía la teoría de los train-tracks [3], pero el algoritmo resultante tiene complejidad desconocida.

Otra posibilidad, en el caso específico de los grupos de trenzas, es usar las técnicas de Garside. El resultado principal vinculando el problema de decisión del tipo de Nielsen-Thurston de una trenza con la estructura de grupo de Garside es el teorema siguiente, debido a Benardete, Gutiérrez y Nitecki:

TEOREMA. [13] (Ver Teoremas 3.3.1 et 5.1.3). *Sea \mathcal{C} una curva estándar. Sea $x = \Delta^p x_1 \dots x_r$ la forma normal de una trenza $x \in B_n$ (clásica o dual). Si \mathcal{C}^x es estándar, entonces para todo $m = 1, \dots, r$, $\mathcal{C}^{\Delta^p x_1 \dots x_m}$ es estándar.*

Presentamos en el Capítulo 4 una nueva prueba de este resultado, más sencilla que la prueba original y que además se extiende (ver Capítulo 5) al caso de la estructura de Garside dual [4]. El teorema precedente implica que si $x \in B_n$ es una trenza reducible, entonces existe un elemento de su Super Summit Set que admite un sistema de reducción hecho de clases de isotopía de círculos (curvas *redondas* o *estándar*); además esta última propiedad puede detectarse fácilmente [2].

El *Super Summit Set* de $x \in B_n$ ($SSS(x)$) es un subconjunto finito de la clase de conjugación de x que se puede computar con la ayuda de las técnicas de Garside [24]. El algoritmo que resulta del párrafo anterior para detectar la reducibilidad de $x \in B_n$ exige calcular la totalidad del conjunto $SSS(x)$ y esto cuesta mucho tiempo porque en general el tamaño del Super Summit Set crece de manera exponencial con respecto a la longitud. En cambio, existe un algoritmo cuadrático para calcular, a partir de $x \in B_n$, un elemento de $SSS(x)$ [9].

En el caso particular del grupo de trenzas con cuatro cuerdas, demostramos que *todo* elemento del Super Summit Set de una trenza reducible admite una curva de reducción (casi-)estándar. Esto proporciona un algoritmo cuadrático para decidir el tipo de Nielsen-Thurston de una trenza con cuatro cuerdas. Este resultado es un paso importante hacia nuestra solución al problema de la conjugación en B_4 . Demostramos en el Capítulo 6 el:

TEOREMA. [15] (Ver Teorema 6.1.1). *Existe un algoritmo que decide el tipo de Nielsen-Thurston de una trenza x con 4 cuerdas y cuya complejidad es cuadrática con respecto a la longitud de x .*

En el caso general de un número de cuerdas arbitrario, González-Meneses y Wiest han producido un algoritmo que decide el tipo de Nielsen-Thurston de una trenza cualquiera, de complejidad polinomial con respecto al número de cuerdas y a la longitud, módulo una conjetura sobre la velocidad de convergencia de una operación de teoría de Garside llamada *cyclic sliding* [33], ver Conjetura 2.3.9. Daremos una prueba parcial de esta conjetura, basada en la propiedad mencionada anteriormente de la cota lineal sobre los elementos conjugadores (ver Capítulo 7). Esto permite una modificación del algoritmo de González-Meneses y Wiest, conduciendo a un algoritmo de complejidad polinomial con respecto a la longitud, para todo número de cuerdas fijado:

TEOREMA. [12] (*Ver Teorema 7.2.1*). *Sea n un entero positivo. Existe un algoritmo que decide el tipo de Nielsen-Thurston de una trenza x con n cuerdas y cuya complejidad es cuadrática con respecto a la longitud de x .*

Desgraciadamente la constante en la cota lineal aún no es conocida explícitamente, así que el algoritmo mencionado no puede ser explícitamente programado. La importancia de esta constante se manifiesta otra vez en el Capítulo 8, donde se usa una segunda vez la cota lineal sobre los elementos conjugadores. Esto interviene en la prueba del siguiente resultado, uno de los pasos clave en nuestra solución al problema de la conjugación en B_4 :

TEOREMA. [14] (*Ver Teorema 8.1.2*). *Para toda trenza $x \in B_4$, pseudo-Anosov rígida con respecto a la estructura dual, el cardinal de $SC(x)$ para la estructura dual está acotado superiormente por $O(\ell(x)^2)$.*

Las nociones de rigidez, de conjuntos de circuitos deslizantes (SC) así como todos los requisitos previos necesarios de la teoría de Garside se pueden encontrar en el Capítulo 2. Hacemos notar de nuevo que el desconocimiento de un valor explícito para la constante interviniendo en la cota lineal (incluso en el caso del grupo de trenzas con cuatro cuerdas) sólo permite obtener un orden de estimación y no un valor explícito sobre el valor del cardinal del conjunto de circuitos deslizantes.

Groupes modulaires et la classification de Nielsen-Thurston

Dans ce chapitre, nous rappelons la définition et quelques propriétés du groupe modulaire d'une surface S . Nous donnons une interprétation du groupe des tresses comme groupe modulaire d'un disque finement perforé. Enfin, nous énonçons deux résultats cruciaux pour la suite, à savoir le théorème de classification de Nielsen-Thurston et la borne linéaire sur la longueur des éléments conjugués (dû à Masur-Minsky et Jing Tao [44], [48]). Une référence pour ce chapitre est le livre de Farb et Margalit [26].

1.1. Le groupe modulaire

Soit Σ une surface connexe, compacte, orientable, de genre $g \geq 0$, avec $b \geq 0$ composantes de bord. Soit n un entier naturel et \mathcal{P} un sous-ensemble fini de l'intérieur de Σ de cardinal n . Nous considérons la surface perforée $\Sigma_n = \Sigma \setminus \mathcal{P}$ (Σ_n n'est plus compacte dès lors que $n > 0$). Nous aurons parfois besoin d'utiliser simultanément Σ et Σ_n ; toutefois le plus souvent nous considérerons le cas général d'une surface Σ_n comme ci-dessus ($n \geq 0$) : nous l'appellerons S . Les éléments de \mathcal{P} seront appelés *trous*.

L'ensemble des homéomorphismes de S qui préservent l'orientation forme un groupe $\text{Homeo}^+(S)$ par rapport à la composition des homéomorphismes. Muni de la topologie compacte-ouverte, $\text{Homeo}^+(S)$ est un groupe topologique. On dit que deux homéomorphismes f et g dans $\text{Homeo}^+(S)$ sont *isotopes* et on note $f \sim g$ s'il existe une famille continue $(f_t)_{t \in [0,1]}$ d'éléments de $\text{Homeo}^+(S)$ telle que $f_0 = f$ et $f_1 = g$. L'isotopie est une relation d'équivalence compatible avec la composition, de sorte que le quotient de $\text{Homeo}^+(S)$ par cette relation est un groupe :

DÉFINITION 1.1.1. *On appelle groupe modulaire de S et on note $\text{Mod}(S)$ le groupe quotient :*

$$\text{Mod}(S) = \text{Homeo}^+(S) / \sim .$$

Nous adoptons la convention suivante pour le produit dans $\text{Mod}(S)$: si f et g sont des éléments de $\text{Mod}(S)$ le produit fg est l'élément de $\text{Mod}(S)$ obtenu en appliquant d'abord f puis g . Cette convention n'est pas standard dans le contexte général du groupe modulaire mais le deviendra dès la section 1.2, dès lors qu'il s'agira de tresses. Nous étudions le groupe $\text{Mod}(S)$ à travers l'action de ses éléments sur la surface S ; dans cette étude, les notions de courbe fermée simple et d'arc dans S jouent un rôle central :

DÉFINITION 1.1.2. *Une courbe fermée dans S est l'image d'une application continue γ du cercle \mathbb{S}^1 dans S . Une courbe fermée \mathcal{C} est dite simple s'il existe une application continue injective $\mathbb{S}^1 \rightarrow S$ dont l'image est \mathcal{C} . Enfin, on dit que \mathcal{C} est non dégénérée si \mathcal{C} n'est homotope ni à un point, ni à un trou, ni à une composante de bord de S .*

On dit que deux courbes fermées simples sont *isotopes* si elles sont homotopes via des courbes fermées *simples*. De plus, deux courbes fermées simples non dégénérées sont isotopes si et seulement si elles sont homotopes (voir [26], proposition 1.10). Si \mathcal{C} est une courbe fermée simple, on note $[\mathcal{C}]$ sa classe d'isotopie. Enfin, on dit que deux classes d'isotopie de courbes fermées simples sont *disjointes* si on peut en trouver des représentants respectifs qui ne s'intersectent pas.

DÉFINITION 1.1.3. *Supposons que \mathcal{P} a au moins deux éléments. Un arc dans S est l'intersection de S avec l'image d'une application continue injective α de l'intervalle $[0, 1]$ dans $S \cup \mathcal{P}$ satisfaisant $\alpha^{-1}(\mathcal{P}) = \{0, 1\}$ et $\alpha^{-1}(\partial S) = \emptyset$.*

Si \mathcal{A} est un arc dans S défini par une application α comme ci-dessus, on appelle *extrémités* de \mathcal{A} les trous $\alpha(0)$ et $\alpha(1)$. Nous devons, comme pour les courbes fermées simples, considérer des homotopies d'arcs. Les seules homotopies permises ici se font à l'intérieur de la classe des arcs précédemment définis (ainsi les extrémités restent fixées au cours du temps). Nous appellerons désormais arc la classe d'homotopie d'un arc.

Outre leur rôle de témoin de l'action des éléments du groupe modulaire sur la surface (voir paragraphe 1.3.1), les courbes fermées simples permettent de définir une famille importante d'éléments de $Mod(S)$.

Soit \mathcal{C} une courbe fermée simple dans S . Il existe alors un homéomorphisme ϕ préservant l'orientation entre un sous-ensemble \mathcal{V} de S et l'anneau $A = \{re^{i\theta} \in \mathbb{C} \mid 1 \leq r \leq 2\}$ tel que la courbe fermée simple $\phi^{-1}(\frac{3}{2}e^{i\theta})$, $\theta \in [0, 2\pi]$ est isotope à \mathcal{C} . Soit τ l'homéomorphisme de A donné par

$$\tau(re^{i\theta}) = re^{i(\theta - 2\pi r)}.$$

Notons que τ induit l'identité sur le bord de l'anneau. Voir figure 1 (a).

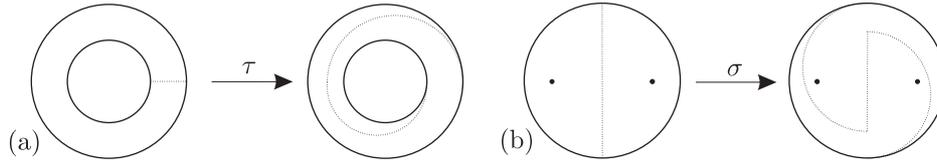


FIGURE 1. (a) L'action de l'homéomorphisme τ de l'anneau A sur un arc dans A . (b) L'action de l'homéomorphisme σ sur un arc dans le disque privé de deux points.

DÉFINITION 1.1.4. *On appelle twist de Dehn autour de \mathcal{C} et on note $\tau_{\mathcal{C}}$ la classe d'isotopie dans $Mod(S)$ de l'homéomorphisme de S défini par*

$$x \mapsto \begin{cases} x & \text{si } x \in S \setminus \mathcal{V}, \\ \phi^{-1}\tau\phi(x) & \text{si } x \in \mathcal{V} \end{cases}$$

Remarquons que la classe d'isotopie de $\tau_{\mathcal{C}}$ ne dépend que de la classe d'isotopie de la courbe \mathcal{C} ; on note parfois $\tau_{[\mathcal{C}]}$.

On peut définir de manière analogue, en relation avec les arcs, la notion de *demi-twist de Dehn*. Supposons que \mathcal{P} a au moins deux éléments et considérons un arc \mathcal{A} dans S . Soient $p_1, p_2 \in \mathcal{P}$ les extrémités de \mathcal{A} . Il existe un homéomorphisme ϕ préservant l'orientation entre un voisinage fermé \mathcal{V} de l'arc \mathcal{A} dans S et le disque $\{re^{i\theta} \in \mathbb{C} \mid r \leq 1\} \setminus \{-\frac{1}{2}, \frac{1}{2}\}$ de sorte que l'image de \mathcal{A} est le segment $]-\frac{1}{2}, \frac{1}{2}[$. Soit σ l'homéomorphisme du disque (voir figure 1 (b)) donné par

$$\sigma(re^{i\theta}) = \begin{cases} re^{i(\theta - \pi)} & \text{si } r \leq \frac{1}{2}, \\ re^{i(\theta - 2\pi r)} & \text{si } \frac{1}{2} < r \leq 1. \end{cases}$$

DÉFINITION 1.1.5. *On appelle demi-twist de Dehn le long de l'arc \mathcal{A} et on note $\sigma_{\mathcal{A}}$ la classe d'isotopie dans $Mod(S)$ de l'homéomorphisme de S défini par*

$$x \mapsto \begin{cases} x & \text{si } x \in S \setminus \mathcal{V}, \\ \phi^{-1}\sigma\phi(x) & \text{si } x \in \mathcal{V} \end{cases}$$

Remarquons que si \mathcal{A} est un arc, et \mathcal{V} est un voisinage de \mathcal{A} homéomorphe à un disque fermé moins deux points, le bord de \mathcal{V} est une courbe fermée simple non dégénérée dans S , disons \mathcal{C} . Alors on a $\tau_{\mathcal{C}} = \sigma_{\mathcal{A}}^2$.

La notion de demi-twist de Dehn joue un rôle très important dans ce texte. Notons que $Mod(S)$ est engendré par un nombre fini de twists de Dehn et de demi-twists de Dehn (voir [26], paragraphe 4.4.4).

Enfin, $Mod(S)$ agit sur les classes d'isotopie de courbes fermées simples (respectivement sur les arcs); nous notons cette action à droite : l'action de $f \in Mod(S)$ sur la classe $[\mathcal{C}]$ (respectivement l'arc \mathcal{A}) est notée $[\mathcal{C}]^f$ (respectivement \mathcal{A}^f). Il est intéressant de noter la relation de conjugaison suivante. Si \mathcal{C} (respectivement \mathcal{A}) est une courbe fermée simple (respectivement un arc) dans S , et $f \in Mod(S)$, on a $\tau_{[\mathcal{C}]^f} = f^{-1}\tau_{\mathcal{C}}f$ et $\sigma_{(\mathcal{A}^f)} = f^{-1}\sigma_{\mathcal{A}}f$.

1.2. Le groupe des tresses comme groupe modulaire

Nous commençons par une définition des groupes de tresses. Cette définition a été formalisée pour la première fois par Emil Artin [1]. Soit n un entier naturel strictement positif. Soient p_1, \dots, p_n n points distingués du plan complexe \mathbb{C} . Il est commode (mais pas nécessaire) de supposer ces points alignés (comme dans la figure 2). On appelle *tresse géométrique à n brins* la donnée de n applications continues b_i , $i = 1, \dots, n$ de l'intervalle $[0, 1]$ dans $\mathbb{C} \times [0, 1]$, dont les images sont appelées *brins*, satisfaisant :

- les brins $b_i([0, 1])$ sont disjoints,
- $b_i(0) = (p_i, 0)$,
- $b_i(1) \in \{p_1, \dots, p_n\} \times \{1\}$,
- $b_i(t) \in \mathbb{C} \times \{t\}$, pour tout $t \in [0, 1]$.

Notons que puisque les chemins b_i sont disjoints, une tresse géométrique induit une permutation π : pour tout $i = 1, \dots, n$, $\pi(i)$ est l'unique élément de $\{1, \dots, n\}$ tel que $b_i(1) = (p_{\pi(i)}, 1)$. On dit qu'une tresse géométrique est *pure* si la permutation qui lui est associée de cette manière est triviale.

On appelle *tresse à n brins* la classe d'homotopie d'une tresse géométrique à n brins (les homotopies permises ont lieu relativement aux points p_i et via des tresses géométriques). À une tresse à n brins on peut associer un diagramme planaire, dit *diagramme de tresse*, obtenu par projection parallèlement à l'axe y , comme sur la figure 2. Modulo homotopie, on peut supposer que la projection n'a que des points doubles transverses, que nous appelons *croisements*. Le dessin de la partie droite de la figure 2 retient alors toutes les propriétés de la tresse de la partie gauche si l'on indique quel brin passe "devant" ou "derrière" pour chaque croisement. L'ensemble des tresses à n

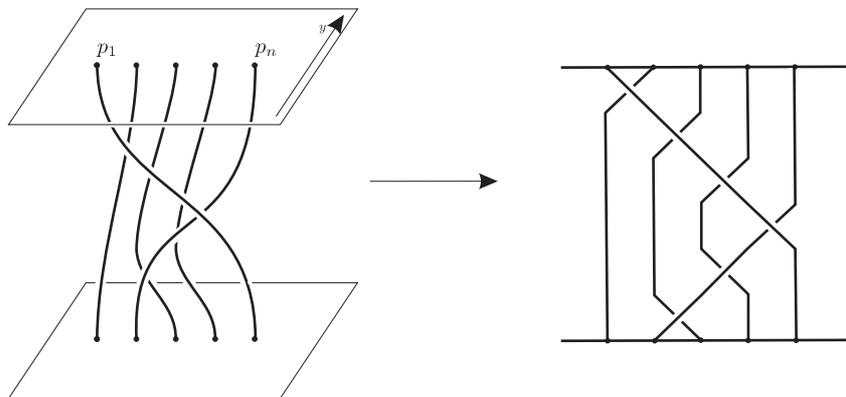


FIGURE 2. À gauche, une tresse géométrique, à droite le diagramme de tresse correspondant à sa classe d'isotopie, obtenu par projection dans la direction y .

brins est muni d'une multiplication donnée par concaténation et rééchelonnement ; cette opération induit une structure de groupe : la *groupe des tresses à n brins* est noté B_n .

Nous pouvons maintenant décrire comment les groupes de tresses s'inscrivent dans le contexte des groupes modulaires. Nous reprenons, pour une surface S avec un bord non vide, la définition du groupe modulaire donnée à la section 1.1, avec une modification des conditions au bord. Nous restreignons la classe des homéomorphismes permis, en demandant que ces derniers induisent l'identité en restriction au bord de S . Le groupe des tels homéomorphismes de S préservant l'orientation est noté $Homeo^+(S, \partial S)$. De manière similaire à la section 1.1, nous considérons ces homéomorphismes modulo isotopie, les isotopies devant se faire à l'intérieur de $(Homeo^+(S), \partial S)$; le groupe quotient obtenu est le groupe modulaire de S *relativement au bord* : $Mod(S, \partial S)$.

Soit \mathbb{D} le disque fermé dans \mathbb{C} orienté dans le sens horaire ; conformément aux notations de la section 1.1, nous notons \mathbb{D}_n le même disque de l'intérieur duquel ont été retirés n points ($n > 0$). Il s'avère que le groupe des tresses B_n et le groupe modulaire de \mathbb{D}_n relativement au bord sont isomorphes. La définition du groupe des tresses à n brins comme groupe modulaire d'un disque privé de n points relativement au bord est contemporaine de celle d'Artin [43]. Nous donnons ici une brève description de cet isomorphisme ; voir [5] pour les détails.

Notons p_1, \dots, p_n les n points ôtés de l'intérieur de \mathbb{D} . Soit $f \in Mod(\mathbb{D}_n, \partial \mathbb{D}_n)$. On peut voir f comme un élément de $Mod(\mathbb{D}, \partial \mathbb{D})$; ainsi, par l'astuce d'Alexander (voir [26], lemme 2.1), il existe une isotopie $(f_t)_{t \in [0,1]}$ entre $Id_{\mathbb{D}}$ et un représentant de f via des homéomorphismes de \mathbb{D} induisant l'identité sur $\partial \mathbb{D}$. La tresse associée à f est alors donnée, et bien définie, comme la classe d'homotopie des chemins dans $\mathbb{D} \times [0,1] : (f_t(p_1), t), \dots, (f_t(p_n), t)$. Réciproquement, soit b une tresse donnée par le n -uplet de brins $((b_1(t), t), \dots, (b_n(t), t))$. Ces brins définissent un mouvement des points p_1, \dots, p_n qui peut être étendu en une famille continue d'homéomorphismes de $(\mathbb{D}, \partial(\mathbb{D}))$ (par exemple comme composition de demi-twists de Dehn), joignant $Id_{\mathbb{D}}$ à un homéomorphisme de \mathbb{D} relativement à $\partial \mathbb{D}$. Ce dernier est aussi un élément de $Homeo^+(\mathbb{D}_n, \partial \mathbb{D}_n)$; sa classe d'isotopie est l'image de la tresse b .

Remarquons que dans \mathbb{D}_n ($n > 2$), la notion de non dégénérescence d'une courbe fermée simple peut se traduire de la façon suivante : une courbe fermée simple dans \mathbb{D}_n est non dégénérée si et seulement si elle entoure au moins 2 trous et au plus $(n - 1)$ trous.

Nous décrivons maintenant deux familles importantes de demi-twists de Dehn dans $Mod(\mathbb{D}_n)$. Supposons que $n \geq 2$. Supposons pour fixer les idées que les trous p_1, \dots, p_n sont alignés le long du diamètre horizontal de \mathbb{D}_n , de la gauche vers la droite (figure 3(a)). Pour $1 \leq i < j \leq n$, considérons l'arc $\mathcal{A}_{i,j}$ décrit par le demi-cercle dans le demi-plan inférieur d'extrémités p_i et p_j (figure 3(a)). Notons $a_{i,j}$ la tresse correspondant au demi-twist de Dehn $\sigma_{\mathcal{A}_{i,j}}$. Pour $1 \leq i \leq n - 1$, on note aussi $\sigma_i := a_{i,i+1}$. La tresse σ_i est représentée sur la figure 3(b).

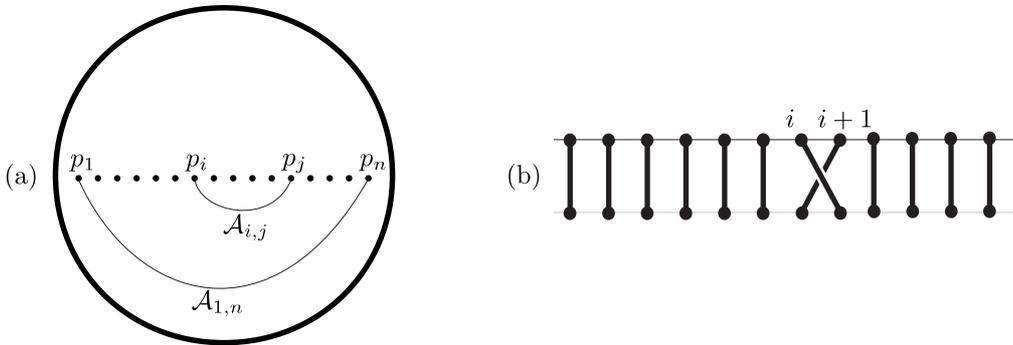


FIGURE 3. (a) Les arcs $\mathcal{A}_{i,j}$, (b) La tresse σ_i .

L'ensemble $\{\sigma_1, \dots, \sigma_{n-1}\}$ est un système générateur de B_n , ses éléments sont appelés *générateurs d'Artin* (voir théorème 2.2.1).

On remarque que pour tous $1 \leq i < j \leq n$,

$$\mathcal{A}_{i,j} = \mathcal{A}_{i,i+1}^{\sigma_{i+1} \dots \sigma_{j-1}}$$

(avec $\sigma_{i+1} \dots \sigma_{j-1} = 1$ si $j = i + 1$); ainsi en vertu de la remarque à la fin de la section 1.1, on obtient la relation suivante dans le groupe B_n (illustrée par la figure 4(b)) :

$$(1) \quad a_{i,j} = (\sigma_{j-1}^{-1} \dots \sigma_{i+1}^{-1}) \sigma_i (\sigma_{i+1} \dots \sigma_{j-1}),$$

avec $\sigma_{i+1} \dots \sigma_{j-1} = 1$ si $j = i + 1$. La famille $\{a_{i,j}, 1 \leq i < j \leq n\}$ admet certaines symétries plus aisément remarquables si l'on représente les trous p_i le long d'un cercle Γ concentrique au bord de \mathbb{D}_n , voir figure 4(a). La famille des tresses $a_{i,j}$ ($1 \leq i < j \leq n$) est aussi un système générateur de B_n (elle contient $\{\sigma_1, \dots, \sigma_{n-1}\}$); on appelle ses éléments les *générateurs de Birman-Ko-Lee*. Nous reviendrons sur ces deux familles génératrices à la section 2.2.

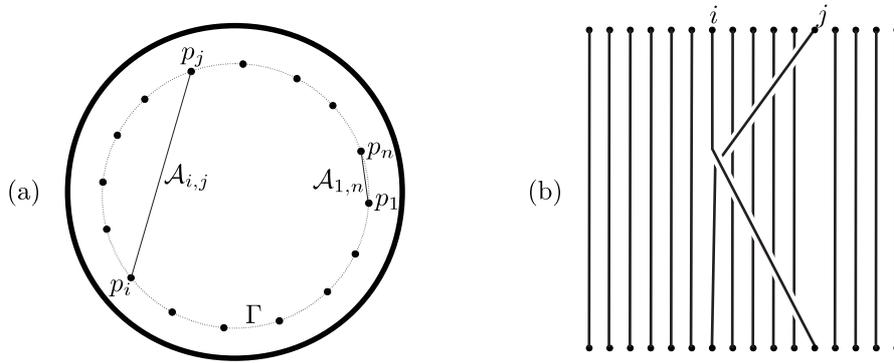


FIGURE 4. (a) Un diagramme de la tresse $a_{i,j}$, (b) la représentation circulaire, avec le cercle Γ en pointillés.

Enfin, considérons le twist de Dehn autour d'une courbe fermée simple parallèle à $\partial\mathbb{D}_n$. Cet élément est trivial dans $Mod(\mathbb{D}_n)$, mais pas dans $Mod(\mathbb{D}_n, \partial\mathbb{D}_n)$; de même dans B_n , la tresse correspondante est l'élément usuellement dénoté Δ_n^2 (ou simplement Δ^2 s'il n'y a pas d'ambiguïté sur le nombre de brins) : voir figure 5. C'est la raison qui nous oblige à considérer des homéomorphismes du disque fixant point par point plutôt que globalement le bord de \mathbb{D}_n .



FIGURE 5. La tresse correspondant au twist de Dehn autour d'une courbe parallèle au bord de \mathbb{D}_n (ici, $n = 5$).

En fait, en quotientant \mathbb{D}_n par son bord, la surface obtenue est une sphère avec $(n + 1)$ trous \mathbb{S}_{n+1} . Le groupe $Mod(\mathbb{D}_n)$ est un sous-groupe d'indice $n + 1$ de $Mod(\mathbb{S}_{n+1})$, précisément le sous-groupe des éléments de $Mod(\mathbb{S}_{n+1})$ fixant ce $(n + 1)$ -ième trou. On a un morphisme $Mod(\mathbb{D}_n, \partial\mathbb{D}_n) \rightarrow Mod(\mathbb{S}_{n+1})$, qui consiste à étendre un homéomorphisme de \mathbb{D}_n en un homéomorphisme de la sphère fixant le $n + 1$ -ième trou. Son noyau est exactement le sous-groupe de B_n engendré par l'élément Δ^2 ([26], proposition 3.19). Ainsi, $Mod(\mathbb{D}_n) \simeq B_n / \langle \Delta^2 \rangle$.

1.3. La classification de Nielsen-Thurston et la borne linéaire

Nous revenons au cas général d'une surface S pour énoncer deux théorèmes d'une grande importance.

1.3.1. La classification de Nielsen-Thurston. Le premier résultat fournit une classification des éléments de $Mod(S)$ via leur action sur les classes d'isotopie de courbes fermées simples non dégénérées de S . Pour une étude détaillée des travaux de Thurston (classification des homéomorphismes, théorie pseudo-Anosov, théorie de Teichmüller) on peut consulter les deux traités [27], [16].

DÉFINITION 1.3.1. *Un élément f de $Mod(S)$ est dit périodique s'il existe un entier strictement positif k tel que $f^k = 1$. Cela signifie qu'il existe un représentant de f dont une puissance est isotope à l'identité.*

Définissons maintenant la notion d'élément réductible de $Mod(S)$. Soit $f \in Mod(S)$. Un *système de réduction* de f est une famille de classes d'isotopie de courbes fermées simples non dégénérées disjointes dans S préservée par l'action de f . Les éléments d'un système de réduction de f sont appelés *courbes de réduction* de f . Notons qu'un système de réduction est nécessairement fini. Ainsi, une classe d'isotopie de courbes fermées simples non dégénérées $[C]$ dans S est une courbe de réduction de f s'il existe une puissance non nulle m de f qui fixe $[C]$ et si les classes d'isotopie des courbes $[C]^{f^i}$, $i = 0, \dots, m-1$ sont disjointes. Dans la littérature, un élément f de $Mod(S)$ est dit *réductible* s'il existe un système de réduction de f qui est non vide, autrement dit si f admet au moins une courbe de réduction.

On observe que selon cette définition, des éléments périodiques peuvent être réductibles. La figure 6 montre un élément g de $Mod(\mathbb{D}_4)$ avec un système de réduction formé de deux classes d'isotopie de courbes fermées simples non dégénérées disjointes $[C_1]$ et $[C_2]$ (et donc g est réductible, selon la définition ci-dessus). Néanmoins le carré de g est l'identité dans $Mod(\mathbb{D}_4)$: c'est le twist de Dehn autour de $\partial\mathbb{D}_4$; donc g est périodique.

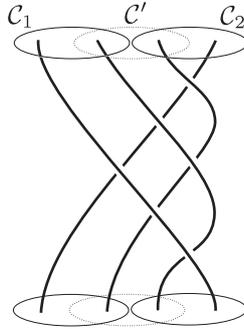


FIGURE 6. Un élément de $Mod(\mathbb{D}_4)$ réductible au sens précédent mais qui n'est pas réductible selon la définition 1.3.2.

En vue d'une classification et pour éviter le recouvrement des subdivisions de cette classification, nous définissons une notion plus restrictive de réductibilité. Soit f un élément de $Mod(S)$. Un *système de réduction essentiel* de f est un système de réduction de f dont tous les éléments sont disjoints de toute courbe de réduction de f . Un élément d'un système de réduction essentiel de f s'appelle une *courbe de réduction essentielle* de f . Nous pouvons maintenant définir la notion de réductibilité souhaitée :

DÉFINITION 1.3.2. *Un élément f de $Mod(S)$ est dit réductible (non périodique) s'il admet un système de réduction essentiel non vide.*

Cette définition exclut l'exemple de la figure 6, à cause de la courbe \mathcal{C}' en pointillés. D'après Birman, Lubotzky et McCarthy [10], le *système de réduction canonique* de $f \in \text{Mod}(S)$, noté $\text{CRS}(f)$, est l'ensemble des courbes de réduction essentielles de f . Ainsi, un élément f de $\text{Mod}(S)$ est réductible si et seulement si $\text{CRS}(f)$ est non vide. De plus, pour un élément réductible, le système de réduction canonique découpe la surface S en sous-surfaces sur lesquelles la restriction de f (ou plus précisément d'une puissance convenable de f) est irréductible, c'est à dire soit périodique, soit pseudo-Anosov (voir définition 1.3.3) [10]. Observons encore que par définition, $\text{CRS}(f) = \text{CRS}(f^m)$ pour tout $f \in \text{Mod}(S)$ et tout entier m non nul.

DÉFINITION 1.3.3. *Un élément f de $\text{Mod}(S)$ est dit pseudo-Anosov, noté pA , s'il existe un représentant f_0 de f et une paire de feuilletages mesurés transverses (\mathcal{F}_u, μ_u) et (\mathcal{F}_s, μ_s) sur S , appelés respectivement feuilletages instable et stable, ainsi qu'un nombre réel $\lambda > 1$, appelé coefficient de dilatation, tels que*

$$(\mathcal{F}_u, \mu_u)^{f_0} = (\mathcal{F}_u, \lambda\mu_u) \quad \text{et} \quad (\mathcal{F}_s, \mu_s)^{f_0} = (\mathcal{F}_s, \frac{1}{\lambda}\mu_s).$$

Le très célèbre théorème de classification des homéomorphismes de surface dit de Nielsen-Thurston affirme alors :

THÉORÈME 1.3.4. [49] *Soit $f \in \text{Mod}(S)$. On a la trichotomie suivante :*

- f est périodique,
- f est réductible,
- f est pseudo-Anosov.

Le *type de Nielsen-Thurston* de $f \in \text{Mod}(s)$ est la subdivision de la classification ci-dessus à laquelle f appartient. Nous formulons d'ores et déjà la remarque, simple mais importante, que le type de Nielsen-Thurston est invariant par conjugaison.

Dans le cas des groupes de tresses, la classification donnée par le théorème 1.3.4 persiste, en définissant une tresse comme réductible, périodique ou pseudo-Anosov si sa projection dans $\text{Mod}(\mathbb{D}_n)$ est réductible, périodique ou pseudo-Anosov. Notons qu'une tresse est périodique si et seulement si c'est une racine d'un élément du sous-groupe cyclique de B_n engendré par Δ^2 .

Le théorème 1.3.4 soulève un problème important, qui est une des principales motivations du présent texte : étant donné un système de générateurs de $\text{Mod}(S)$, peut-on trouver un algorithme qui décide si un élément de $\text{Mod}(S)$ exprimé comme un mot de longueur l en terme de ces générateurs est périodique, réductible ou pseudo-Anosov? Est-il possible de surcroît de trouver les éléments invariants, i.e. un système de courbes de réduction pour un élément réductible ou une paire de feuilletages transverses mesurés et un coefficient de dilatation pour un élément pseudo-Anosov? Enfin, peut-on trouver un tel algorithme de sorte que sa complexité soit polynômiale par rapport à l ?

Une réponse positive aux deux premières questions (ainsi qu'une nouvelle preuve du Théorème 1.3.4), est apportée par Bestvina et Handel dans [3] via les techniques des réseaux ferroviaires. L'algorithme qui y est proposé est implémenté et disponible librement [41]. Cet algorithme donne en pratique d'excellents résultats; toutefois, sa complexité théorique n'est pas connue. Un des principaux buts de ce texte est de présenter des algorithmes pour résoudre le problème ci-dessus dans les groupes de tresses. Comme ci-dessus, nous souhaitons une complexité polynômiale en fonction de la longueur; de plus nous considérons le nombre de brins n comme un paramètre et nous désirons que la complexité des algorithmes dépende de n de manière polynômiale. Nous suivons une approche radicalement différente de celle de Bestvina et Handel, basée sur les propriétés algébriques du groupe de tresses exposées dans le chapitre 2 (voir chapitre 3).

1.3.2. La borne linéaire sur la longueur des éléments conjugués. Avant de clore ce chapitre, nous abordons un résultat d'une grande importance lié au problème de conjugaison dans les groupes modulaires. Historiquement, la preuve repose sur le théorème 1.3.4 puisque le résultat

en question a été démontré d'abord pour des éléments pseudo-Anosov [44] puis pour des éléments réductibles et périodiques [48].

THÉORÈME 1.3.5. *Soit \mathcal{G} un système de générateurs de $Mod(S)$. Pour $f \in Mod(S)$, soit $|f|$ la longueur de f relativement à \mathcal{G} , c'est à dire la longueur du mot le plus court sur $\mathcal{G} \cup \mathcal{G}^{-1}$ représentant f . Alors il existe une constante $C_{\mathcal{G}}$ telle que pour tous $g_1, g_2 \in Mod(S)$ conjugués dans $Mod(S)$, il existe $u \in Mod(S)$ tel que $g_1^u = g_2$ et $|u| \leq C_{\mathcal{G}}(|g_1| + |g_2|)$.*

Nous reviendrons sur la spécialisation de ce résultat au groupe des tresses dans les chapitres 7 et 8 où il jouera un rôle majeur ; mais avant de pouvoir en faire un usage intéressant, nous devons nous pencher en détail sur la structure algébrique du groupe des tresses.

Groupes de Garside, le problème de conjugaison

Les groupes de Garside sont, sommairement, les groupes satisfaisant les propriétés initialement découvertes par Garside [30] dans le cadre des groupes de tresses. Nous adoptons un point de vue a posteriori en donnant d'abord la définition et quelques propriétés élémentaires des groupes de Garside (pour une exposition plus complète on peut consulter [22], [20]). Les structures de Garside classique et duale des groupes de tresses sont exposées dans un deuxième temps. Enfin, dans une troisième partie, nous mettons l'accent sur les techniques de résolution du problème de conjugaison dans les groupes de Garside. Mentionnons aussi que la théorie dite de Garside est l'objet de développements récents, avec notamment l'introduction des *catégories de Garside* qui généralisent les groupes de Garside [21].

2.1. Groupes de Garside

DÉFINITION 2.1.1. [33]

Soit G un groupe. On appelle structure de Garside sur G la donnée d'une paire (P, Δ) , où P est un sous-monoïde de G et Δ est un élément distingué de P , satisfaisant les propriétés suivantes :

- (G1) La relation \preceq définie sur G par $x \preceq y \Leftrightarrow x^{-1}y \in P$ induit une structure de treillis sur G , c'est à dire, pour tous $x, y \in G$, il existe un unique $d \in G$ et un unique $m \in G$ tels que
 - $d \preceq x$, $d \preceq y$ et pour tout $d' \in G$ tel que $d' \preceq x$ et $d' \preceq y$, on a $d' \preceq d$,
 - $x \preceq m$, $y \preceq m$ et pour tout $m' \in G$ tel que $x \preceq m'$ et $y \preceq m'$, on a $m \preceq m'$.
- (G2) La conjugaison par Δ préserve le monoïde P .
- (G3) L'ensemble $\mathcal{S} = \{x \in G \mid 1 \preceq x \preceq \Delta\}$ est fini et engendre G comme groupe.
- (G4) Pour tout $x \in P \setminus \{1\}$,

$$\|x\| = \sup\{k \mid \exists a_1, \dots, a_k \in P \setminus \{1\} \mid x = a_1 \dots a_k\} < \infty,$$

en particulier le monoïde P est noethérien.

On dit que G est un groupe de Garside si G admet au moins une structure de Garside.

La relation \preceq est naturellement appelée relation d'ordre des *préfixes* : si $x \preceq y$, on dit que x est un *préfixe* de y . Il découle de la définition que la relation \preceq est invariante par multiplication à gauche : pour tous $x, y, z \in G$, $x \preceq y \Leftrightarrow zx \preceq zy$.

De manière équivalente, une structure de Garside peut être définie par la donnée d'une relation d'ordre \preceq invariante par multiplication à gauche et satisfaisant les propriétés de treillis. On demande alors que le cône positif de cette relation, i.e. $P := \{x \in G \mid 1 \preceq x\}$ (qui est un monoïde) satisfasse (G4) et contienne un élément spécial Δ avec les propriétés (G2) et (G3).

On appelle *positifs* les éléments de P . L'élément Δ s'appelle *élément de Garside*. La longueur maximale $\|\Delta\|$ d'un mot $a_1 \dots a_k$ représentant Δ avec $a_1, \dots, a_k \in P \setminus \{1\}$ est une importante caractéristique numérique attachée à la structure de Garside (P, Δ) . Pour tous $x, y \in G$, les éléments d et m de G dont l'existence est garantie par la condition (G1) sont respectivement les *plus grand diviseur* et *plus petit multiple communs* de x et y ; on note $d = x \wedge y$ et $m = x \vee y$. Une conséquence immédiate de la définition 2.1.1 est l'absence de torsion dans un groupe de Garside. Supposons en effet que $x \in G$ est d'ordre fini m , alors l'élément $d = 1 \wedge x \wedge \dots \wedge x^{m-1}$ vérifie $xd = x \wedge x^2 \wedge \dots \wedge x^m = d$, ce qui implique $x = 1$.

Notons qu'à une structure de Garside (P, Δ) est aussi associée une relation d'ordre \succ invariante par multiplication à droite et satisfaisant (G1), définie par la formule $x \succ y$ si et seulement si $xy^{-1} \in P$; si $x \succ y$, on dit que y est un *suffixe* de x . En vertu de (G2), la conjugaison par Δ préserve les deux relations \preceq et \succ , autrement dit si on note τ l'automorphisme intérieur de G associé à Δ , on a pour tous $x, y \in G$, $x \preceq y \Leftrightarrow \tau(x) \preceq \tau(y)$ et $x \succ y \Leftrightarrow \tau(x) \succ \tau(y)$.

La condition (G2) implique aussi que $\mathcal{S} = \{x \in G \mid \Delta \succ x \succ 1\}$. On appelle *éléments simples* les éléments de \mathcal{S} . A tout $s \in \mathcal{S}$, on associe son *complément à droite* $\partial(s) = s^{-1}\Delta$ et son *complément à gauche* $\partial^{-1}(s) = \Delta s^{-1}$. Les deux fonctions ∂ et ∂^{-1} , de \mathcal{S} dans lui-même, sont des bijections inverses l'une de l'autre. On remarque aussi que ∂^2 est la restriction de τ à \mathcal{S} . Puisque \mathcal{S} est fini et engendre G , le centre de G doit contenir une puissance de Δ . La condition (G3) implique que Δ n'est pas l'élément neutre (dès lors que G n'est pas trivial); or G est sans torsion : le centre d'un groupe de Garside non trivial est non trivial.

La condition (G4) implique l'existence d'éléments spéciaux de P , appelés *atomes*. Supposons que x est un élément de P et écrivons $x = a_1 \dots a_k$, avec $k = \|x\|$ et $a_i \in P \setminus \{1\}$. Alors pour tout $i = 1, \dots, k$, si $a_i = uv$ avec $u, v \in P$ on doit avoir $u = 1$ ou $v = 1$ sans quoi la définition de $\|x\|$ serait contredite. Un élément $a \in P \setminus \{1\}$ est un *atome* si pour tout produit $a = uv$, avec $u, v \in P$, on a $u = 1$ ou $v = 1$. Remarquons que tout système générateur de P doit contenir tous les atomes; en particulier, les atomes sont en nombre fini. On note λ le nombre d'atomes. Ce nombre est une caractéristique de la structure de Garside (P, Δ) .

Nous rappelons maintenant une propriété fondamentale des groupes de Garside. Sommairement il s'agit d'associer, à tout élément x de G , un unique mot sur l'alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$, représentant distingué de x : sa *forme normale*.

DÉFINITION 2.1.2. Soient s_1 et s_2 deux éléments simples de G . On dit que la paire (s_1, s_2) est *pondérée (à gauche)* si $\partial(s_1) \wedge s_2 = 1$, autrement dit si s_1 est le plus grand diviseur simple de $s_1 s_2$. Si (s_1, s_2) n'est pas pondérée à gauche, soit $t = \partial(s_1) \wedge s_2$; on appelle *glissement local de la paire* (s_1, s_2) la transformation de s_1 en $s'_1 = s_1 t$ et de s_2 en $s'_2 = t^{-1} s_2$, qui fournit une paire (s'_1, s'_2) pondérée à gauche.

PROPOSITION 2.1.3. Soit $x \in G$. Il existe une unique décomposition $x = \Delta^p x_1 \dots x_r$ où r est un entier naturel, p est le plus grand entier relatif satisfaisant $\Delta^p \preceq x$, les x_i sont des éléments simples avec $x_r \neq 1$ et (pour $r \geq 2$) la paire (x_i, x_{i+1}) est pondérée à gauche pour tout $i = 1, \dots, r-1$.

Dans la proposition précédente, l'écriture $x = \Delta^p x_1 \dots x_r$ s'appelle *forme normale (à gauche)* de x ; les entiers p et r sont appelés respectivement *infimum* et *longueur canonique* de x , on les note respectivement $\inf(x)$ et $\ell(x)$. On appelle *supremum* de x et on note $\sup(x)$ la quantité $p+r$. Pour tout $x \in G$, $\sup(x) = \min\{k \in \mathbb{Z}, x \preceq \Delta^k\}$. Notons que les éléments de longueur canonique 0 sont les puissances de Δ . Enfin, pour $x \in G$ avec $\ell(x) \geq 1$ et forme normale $x = \Delta^p x_1 \dots x_r$, on attache à x deux éléments simples importants, à savoir le *facteur initial* de x noté $\iota(x)$ défini par $\iota(x) = \tau^{-p}(x_1)$ et le *facteur final* de x noté $\varphi(x)$ et défini par $\varphi(x) = x_r$.

De manière symétrique on peut définir aussi les notions de pondération à droite et de forme normale à droite. Cela conduit à des notions de supremum, infimum et longueur canonique associés aux formes normales à droite : ces quantités coïncident avec les supremum, infimum et longueur canonique associés aux formes normales à gauche. Dans le reste du manuscrit, nous considérons seulement la forme normale à gauche, par conséquent nous l'appellerons désormais simplement *forme normale* et nous dirons qu'une paire d'éléments simples est *pondérée* si elle est pondérée à gauche.

Le langage des formes normales définit une structure biautomatique sur G ([20], proposition 3.12). En particulier, les formes normales résolvent le problème du mot en temps quadratique (voir par exemple [25], théorème 2.3.10). Cela signifie qu'il existe un algorithme qui calcule la forme normale de l'élément de G représenté par un mot w sur $\mathcal{S} \cup \mathcal{S}^{-1}$ de longueur l en temps $O(l^2)$, et de là peut décider si w représente l'élément neutre ou pas. De manière plus précise, le coût algorithmique du

calcul de la forme normale d'un élément x de G donné comme un mot sur $\mathcal{S} \cup \mathcal{S}^{-1}$ de longueur au plus l est $O(\lambda^2 \|\Delta\|)$ ([32], théorème 4.4).

L'ensemble des éléments simples de G induit naturellement une longueur sur G . La longueur $|x|$ d'un élément x de G est définie comme la plus petite longueur possible pour un mot représentant x exprimé dans l'alphabet formé par les diviseurs de Δ et leurs inverses. Nous remarquons que pour tout $x \in G$, $\ell(x) \leq |x|$. Rappelons aussi que tout $x \in G$ admet une unique écriture de la forme $x = a^{-1}b$, où a et b sont des éléments de P satisfaisant $a \wedge b = 1$ ([25], chapitre 9). On appelle cela la *forme canonique mixte*. Soient alors $a = a_1 \dots a_k$ et $b = b_1 \dots b_l$ les formes normales respectives de a et b . Une conséquence du lemme 3.11 de [20] (voir [17] lemme 3.1) est que le mot $a_k^{-1} \dots a_1^{-1} b_1 \dots b_l$ est une géodésique dans le graphe de Cayley de G associé aux éléments simples. Par conséquent, la longueur d'un élément de G définie ci-dessus est la longueur (en tant que mot sur \mathcal{S}) de sa forme canonique mixte. Si $x \in G$ satisfait $\text{inf}(x) = p$ et $\ell(x) = r$, on a les relations suivantes :

$$|x| = \begin{cases} p + r & \text{si } p \geq 0, \\ r & \text{si } p < 0 \text{ et } |p| \leq r, \\ |p| & \text{si } p < 0 \text{ et } |p| > r. \end{cases}$$

Les groupes de tresses constituent les premiers et les plus célèbres exemples de groupes de Garside. Cela est décrit en détail dans la section 2.2. En outre, il est important de mentionner que la classe des groupes de Garside contient plusieurs exemples importants de groupes, parmi lesquels les groupes abéliens libres de type fini, les groupes d'Artin de type fini (qui sont une généralisation des groupes de tresses), les groupes de noeud torique et d'autres [6], [46].

2.2. Le groupe de tresses et ses deux structures de Garside

Les groupes de tresses admettent deux structures de Garside (i.e. deux couples (\preceq, Δ)) bien connues, que nous allons décrire maintenant.

2.2.1. La structure classique. Nous commençons par rappeler un résultat important dû à Artin :

THÉORÈME 2.2.1. [1] *Le groupe des tresses à n brins B_n admet la présentation suivante :*

$$B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{si } |i - j| \geq 2, \\ \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} & \text{si } 1 \leq i \leq n - 2 \end{array} \right\rangle.$$

Les générateurs et les relations apparaissant dans cette présentation sont comme sur la figure 1.

Considérons le monoïde B_n^+ défini par la présentation donnée au théorème 2.2.1. Les éléments de B_n^+ s'écrivent comme des mots où les lettres σ_i ne peuvent apparaître qu'avec un exposant positif; on les appelle *tresses positives*.

Dans le remarquable article [30], Garside a montré, bien que les axiomes (G1) à (G4) de la définition 2.1.1 n'apparaissent pas explicitement dans son travail, que la paire (B_n^+, Δ) (où

$$\Delta = (\sigma_1 \dots \sigma_{n-1})(\sigma_1 \dots \sigma_{n-2}) \dots (\sigma_1 \sigma_2) \sigma_1,$$

est une structure de Garside pour le groupe des tresses B_n (on peut voir aussi [11]). Géométriquement, la tresse Δ correspond à un demi-tour de tous les brins (voir figure 5 au chapitre 1, où est représenté le tour complet Δ^2). On appelle structure de Garside *classique* ou *structure d'Artin-Garside* de B_n la paire (B_n^+, Δ) . On remarque que cette structure contient $\lambda = n - 1$ atomes, à savoir les éléments $\sigma_1, \dots, \sigma_{n-1}$. De plus, comme les relations de la présentation du théorème 2.2.1 sont équilibrées (c'est à dire qu'il y a le même nombre d'atomes de part et d'autre des égalités), pour tout $x \in B_n^+$, $\|x\|$ est la longueur (en termes des atomes) de tout mot positif représentant x . Notons la valeur $\|\Delta\| = \frac{n(n-1)}{2}$. Enfin on peut vérifier, à partir des relations de la présentation du théorème 2.2.1, les égalités $\Delta \sigma_i = \sigma_{n-i} \Delta$ pour tout $i = 1, \dots, n - 1$; ainsi la conjugaison par Δ

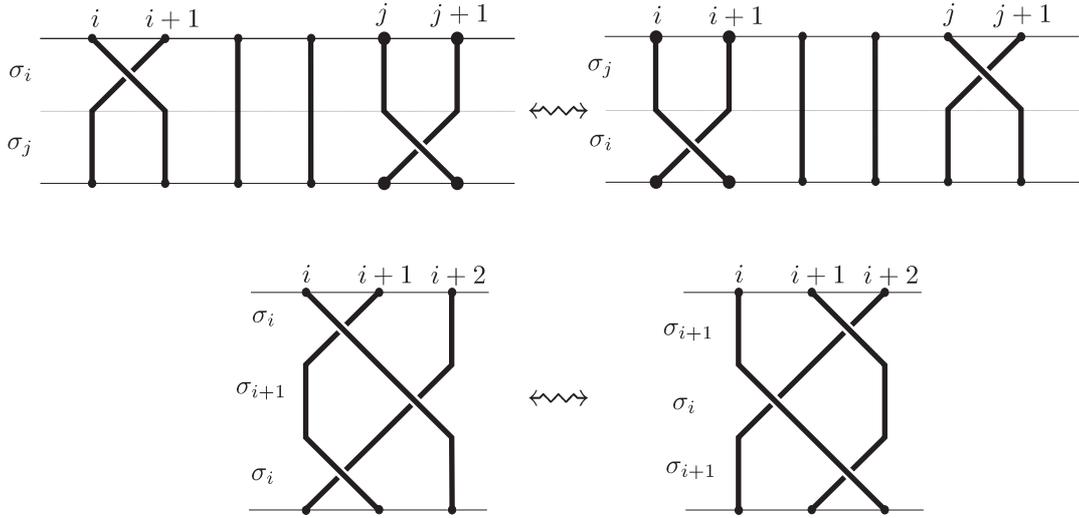


FIGURE 1. Les générateurs d'Artin et les relations dans les groupes de tresses.

est une involution. En fait, il est connu que le centre de B_n ($n \geq 3$) est précisément le sous-groupe engendré par Δ^2 (voir par exemple [30], théorème 7).

ElRifai et Morton [24] et Thurston ([25], chapitre 9) ont donné une description géométrique des éléments simples de la structure d'Artin-Garside de B_n , en termes de croisements de brins. Cela conduit à une caractérisation de la pondération (et partant, des formes normales). Remarquons que Δ est l'unique tresse positive dans laquelle chaque paire de brins se croise exactement une fois. Les éléments simples sont alors les tresses positives dans lesquelles chaque paire de brins se croise *au plus* une fois. Cette description fournit une bijection entre l'ensemble des éléments simples et le groupe symétrique (il existe exactement une tresse simple induisant une permutation donnée) : il y a exactement $n!$ éléments simples.

Le lemme suivant joue un rôle important dans la suite (voir section 4.4) :

LEMME 2.2.2. [24] *Soit s un élément simple. Soit $i = 1, \dots, n-1$. Alors*

- $\sigma_i \preceq s$ si et seulement si les brins numérotés i et $i+1$ au début de s se croisent dans s .
- $\sigma_i \preceq \partial(s)$ si et seulement si les brins qui sont en position i et $i+1$ à la fin de s ne se croisent pas dans s .

COROLLAIRE 2.2.3. [24] *Soient s_1 et s_2 deux tresses simples. Alors la paire (s_1, s_2) est pondérée si et seulement si pour tout $i = 1, \dots, n-1$, dès que les brins portant les numéros i et $i+1$ se croisent dans s_2 , alors les brins en position i et $i+1$ à la fin de s_1 se croisent dans s_1 .*

Notons que l'estimation du coût algorithmique du calcul de la forme normale donnée à la section 2.1 n'est pas optimale dans le cas de la structure classique de B_n . En effet, l'étude des propriétés du groupe symétrique permet d'estimer cette complexité en $O(\ell^2 n \log n)$ au lieu de $O(\ell^2 n^3)$ comme annoncé (voir [25], corollaire 9.5.3).

2.2.2. La structure duale. Dans les années 1990, Birman, Ko et Lee ont découvert une autre structure de Garside pour le groupe B_n :

THÉORÈME 2.2.4. [4] *Le groupe des tresses à n brins B_n admet la présentation de groupe avec générateurs*

$$a_{i,j}, 1 \leq i < j \leq n,$$

et relations

$$a_{i,j}a_{k,l} = a_{k,l}a_{i,j} \text{ si les intervalles entiers } [i, j] \text{ et } [k, l] \text{ sont disjoints}$$

$$\text{ou satisfont } [i, j] \subset [k, l] \text{ ou } [k, l] \subset [i, j], \text{ avec } k \neq i \text{ et } l \neq j,$$

et

$$a_{i,j}a_{j,k} = a_{j,k}a_{i,k} = a_{i,k}a_{i,j} \text{ si } 1 \leq i < j < k \leq n.$$

De plus, la paire constituée du monoïde donné par la même présentation et de l'élément distingué $\delta = a_{1,2} \dots, a_{n-1,n}$ est une structure de Garside pour B_n .

Cette structure est appelée structure *duale* ou *structure de Birman-Ko-Lee* (BKL). On note $BKL_n := B_n$ lorsque l'on considère le groupe des tresses B_n muni de cette structure; le monoïde donné par la présentation du théorème 2.2.4 est noté BKL_n^+ et ses éléments sont appelés *tresses duales positives* (ou simplement tresses positives s'il n'y a pas d'ambiguïté). Les tresses $a_{i,j}$ ont été décrites à la section 1.2; ce sont les atomes de la structure duale et on a donc $\lambda = \frac{n(n-1)}{2}$. A nouveau, les relations dans la présentation du théorème 2.2.4 sont équilibrées; et pour $x \in BKL_n^+$, la quantité $\|x\|$ est la longueur (en terme des atomes) de tout mot positif représentant x . On a $\|\delta\| = n - 1$. Ainsi, on remarque que les valeurs λ et $\|\Delta\|$ sont interchangées entre les deux structures de Garside de B_n . Remarquons aussi que les valeurs de $\|\Delta\|$ et de λ dépendent polynômialement de n dans les deux cas. Enfin, notons l'égalité $\delta^n = \Delta^2$; ainsi l'automorphisme τ associé à la structure duale est d'ordre n .

Nous terminons cette section par une description des éléments simples de la structure duale ainsi qu'une condition de pondération. Rappelons la description de B_n comme groupe modulaire d'un disque perforé de n trous p_1, \dots, p_n (voir section 1.2). On envisage la représentation circulaire de la figure 4 (a) du chapitre 1, où Γ est un cercle concentrique à $\partial\mathbb{D}_n$ à l'intérieur du disque \mathbb{D}_n sur lequel sont placés les trous p_1, \dots, p_n (voir figure 3 (b), chapitre 1).

Les relations dans la présentation du théorème 2.2.4 impliquent le fait suivant. Soit r un entier avec $2 \leq r \leq n$. Considérons r entiers distincts $1 \leq i_1 < \dots < i_r \leq n$ de sorte que les r trous p_{i_1}, \dots, p_{i_r} de \mathbb{D}_n sont disposés dans cet ordre le long du cercle Γ en le parcourant dans le sens horaire depuis p_{i_1} jusqu'à p_{i_r} . Considérons la suite d'atomes $(a_{i_1, i_2}, \dots, a_{i_{r-1}, i_r}, a_{i_1, i_r})$, modulo permutation cyclique des termes. Alors tous les mots obtenus comme la concaténation de $r - 1$ termes consécutifs de cette suite représentent la même tresse P . De plus, pour chaque paire $1 \leq d < e \leq r$, la lettre a_{i_d, i_e} est un préfixe (et un suffixe de P). On peut alors représenter cette tresse P par un polygone de sommets p_{i_1}, \dots, p_{i_r} ; pour cette raison nous appelons *polygone* une telle tresse (si $r = 2$, le polygone est réduit au segment $[p_{i_1}, p_{i_2}]$). Remarquons que P induit une permutation circulaire des trous p_{i_1}, \dots, p_{i_r} dans le sens antihoraire laissant les autres trous fixés. Les relations dans la présentation du théorème 2.2.4 impliquent également que deux tels polygones *disjoints*, c'est à dire dont les enveloppes convexes sont disjointes, commutent. La tresse δ est un polygone : celui dont tous les trous sont des sommets. Cela suggère la caractérisation des éléments simples de la structure duale.

De fait, tout élément simple dual s'écrit de manière unique comme produit (commutatif) de polygones disjoints [4]. Il est connu que le nombre d'éléments simples duaux est le nombre de Catalan $C_n = \frac{(2n)!}{(n+1)!n!}$ [4]. Notons que ce nombre est strictement inférieur à celui des éléments simples de la structure classique (mais dépend toujours exponentiellement de n).

Enfin, la représentation géométrique que nous venons d'évoquer permet aussi de caractériser la pondération. Pour tout $i = 1, \dots, n$, notons p'_i le milieu du segment $[p_i, p_{i+1}]$ dans \mathbb{D} (avec $i+1 = 1$ si $i = n$). La figure 2 illustre le lemme suivant.

LEMME 2.2.5. [4] *Soit s une tresse simple duale. Soit $s = P_1 \dots P_m$ la décomposition de s en termes de polygones. Soient i, j des entiers avec $1 \leq i < j \leq n$. Alors*

- $a_{i,j} \preceq s$ si et seulement si $s \succeq a_{i,j}$ si et seulement si l'un des polygones P_1, \dots, P_m a pour sommets p_i et p_j simultanément.

- $a_{i,j} \preceq \partial(s)$ si et seulement si le segment $[p'_i, p'_j]$ est disjoint de l'enveloppe convexe de chaque polygone P_1, \dots, P_m .

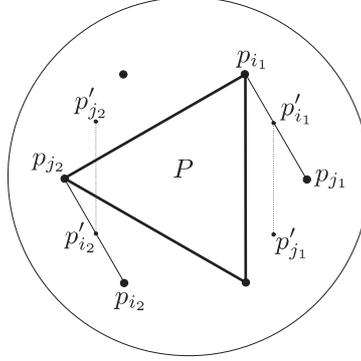


FIGURE 2. Ici, $n = 6$. L'élément simple représenté (en gras) est un seul polygone P . On a représenté deux atomes a_{i_1, j_1} et a_{i_2, j_2} ainsi que les segments correspondants $[p'_{i_1}, p'_{j_1}]$ et $[p'_{i_2}, p'_{j_2}]$ en pointillés. La tresse Pa_{i_2, j_2} n'est pas simple, i.e. a_{i_2, j_2} n'est pas un préfixe de $\partial(P)$. A contrario, $a_{i_1, j_1} \preceq \partial(P)$.

Remarquons que dans le cas de la structure duale de B_n , on peut aussi améliorer l'estimation du coût algorithmique du calcul des formes normales donnée dans la section 2.1 puisqu'un produit d'éléments simples et de leurs inverses avec l facteurs peut être mis en forme normale en temps $O(l^2n)$ (voir [4], théorème 4.4).

2.3. Le problème de conjugaison dans les groupes de Garside

Le problème de conjugaison dans un groupe G de type fini est l'un des trois célèbres problèmes énoncés par Max Dehn au début du vingtième siècle. Il s'agit de décider si deux éléments x et y exprimés comme produits des générateurs et de leurs inverses appartiennent à la même classe de conjugaison ou pas. Ce problème de décision (que nous noterons DC) soulève immédiatement le problème de recherche d'un élément conjugué (que nous noterons RC) : si les deux éléments x et y sont conjugués, peut-on trouver un élément conjugué, i.e. un élément z de G tel que $x = z^{-1}yz$, ou en notation plus compacte que nous adopterons désormais, $x = y^z$? Garside [30] a démontré que les deux problèmes sont résolubles dans les groupes de tresses. Les généralisations ultérieures qui conduisent à la définition 2.1.1 retiennent entre autres propriétés la résolubilité des problèmes DC et RC pour tout groupe de Garside.

2.3.1. L'algorithme général. Soit G un groupe de Garside avec structure de Garside (P, Δ) . Rappelons les valeurs numériques λ (le nombre d'atomes) et $||\Delta||$ introduites précédemment. Ces deux paramètres permettent de mesurer la complexité d'un algorithme dans G . Dans le cas spécifique des groupes de tresses, pour la structure classique comme pour la structure duale, λ et $||\Delta||$ ne dépendent en fait que d'un seul paramètre, à savoir le nombre de brins n (et ce de manière au plus quadratique).

Les algorithmes connus pour résoudre le problème de conjugaison dans G reposent sur la définition, pour tout élément x de G , d'un sous-ensemble *fini non vide* E_x de la classe de conjugaison de x satisfaisant $E_x = E_y$ si et seulement si x et y sont conjugués. Nous appelons un tel ensemble un *invariant de conjugaison*. Depuis 1969 et le travail de Garside, plusieurs ensembles E_x avec ces propriétés ont été définis ; nous examinons dans un premier temps les propriétés générales de l'algorithme, avant de dresser l'historique des cas particuliers.

On observe que les propriétés caractéristiques des ensembles E_x permettent de résoudre le problème DC dans G dès lors que l'on est capable de calculer effectivement E_x , pour tout $x \in G$. Comme

nous allons le voir, les techniques de calcul de E_x mises en oeuvre fournissent aussi une solution au problème RC. L'algorithme pour calculer E_x repose sur trois propriétés cruciales. La première d'entre elles est l'existence d'un procédé effectif pour calculer, pour tout $x \in G$, des éléments $x_0 \in E_x$ et $z \in G$, tels que $x_0 = x^z$. Les deux autres propriétés sont basées sur les idées de Franco et González-Meneses [29]. D'abord l'ensemble des éléments de G qui conjuguent un élément x de G vers un élément de E_x doit être stable sous les opérations de plus grand diviseur commun et de plus petit multiple commun : pour tous $x, a, b \in G$, si $x^a \in E_x$ et $x^b \in E_x$, alors $x^{a \wedge b} \in E_x$ et $x^{a \vee b} \in E_x$.

La dernière propriété cruciale exprime une notion de connexité pour l'invariant de conjugaison E_x . Avant de l'énoncer nous introduisons deux définitions :

DÉFINITION 2.3.1. [29] *Soit $x \in G$. Soit $y \in E_x$. On dit qu'un élément non trivial s de P est un élément conjugant minimal pour y si $y^s \in E_x$ et si pour tout $t \in P$ tel que $t \preceq s$ et $y^t \in E_x$, on a $t = 1$ ou $t = s$.*

Grâce à cette définition, on peut associer à tout élément de G un graphe orienté qui décrit l'ensemble E_x .

DÉFINITION 2.3.2. *A tout élément $x \in G$, on associe un graphe orienté GE_x défini de la façon suivante:*

- chaque sommet correspond à un élément de E_x ,
- pour tout élément $y \in E_x$ et toute élément conjugant minimal s pour y , le graphe GE_x contient une arête orientée du sommet y vers le sommet y^s et étiquetée s .

Les conjugaisons par des éléments conjugants minimaux sont représentées dans le graphe GE_x par des flèches ; pour cette raison on parle habituellement de *flèches minimales* plutôt que d'éléments conjugants minimaux pour $y \in E_x$. La propriété de connexité attendue est la suivante :

PROPRIÉTÉ 2.3.3. [29] *Soit $x \in G$. Pour tous $y \neq y' \in E_x$, il existe un entier $m \geq 1$, des éléments s_1, \dots, s_m de $P \setminus \{1\}$, et des éléments $y = y_1, \dots, y_{m+1} = y'$ dans E_x tels que pour $i = 1, \dots, m$, s_i est une flèche minimale pour y_i , avec $y_{i+1} = y_i^{s_i}$.*

De plus, l'ensemble E_x est invariant par τ et pour $y \in E_x$, les flèches minimales pour y sont des éléments simples en nombre borné par le nombre d'atomes λ [29]. L'algorithme pour calculer E_x procède comme suit :

ALGORITHME 2.3.4. En entrée $x \in G$, en sortie E_x .

1°) Calculer $x_0 \in E_x$, poser $E := \{x_0\}$ et $E' := \emptyset$.

2°) Tant que E n'est pas vide,

- (a) choisir un élément y de E ,
- (b) calculer $A_y = \{y^s \mid s \text{ est une flèche minimale pour } y\}$,
- (c) changer $E' := E' \cup \{y\}$ et $E := (E \cup A_y) \setminus E'$.

3°) Répondre E' .

En vertu de la propriété 2.3.3, l'ensemble fini E_x est entièrement calculé par ce procédé. De plus, en gardant trace des éléments conjugants à chaque étape, on peut mémoriser, pour tout $y \in E_x$, un élément de G qui conjugue x à y : cela fournit une solution au problème RC.

L'évaluation de la complexité de l'étape 1°) est un point clé dans l'estimation de la complexité de l'algorithme 2.3.4. Parallèlement, il est essentiel de développer des techniques efficaces afin de calculer l'ensemble des flèches minimales pour $y \in E_x$. Enfin, le cardinal de E_x est bien sûr un élément important dont dépend la complexité de l'algorithme 2.3.4. Notons qu'il dépend lui même, ainsi que la complexité de l'étape 1°), de la longueur canonique de x . Nous présentons maintenant les différents candidats E_x proposés dans la littérature, ainsi que quelques remarques concernant la complexité des algorithmes qui leur sont associés.

Dans le travail de Garside [30], le rôle de E_x est joué par le *Summit Set* de x . Seule la notion d'infimum est utilisée, permettant de décomposer tout $x \in G$ comme $x = \Delta^p x^+$ avec $p \in \mathbb{Z}$ maximal et $x^+ \in P$. Le Summit Set de x (noté $SS(x)$) est l'ensemble des conjugués de x dont l'infimum est maximal. C'est un ensemble fini, qui contient tous les invariants E_x définis ultérieurement. Notons aussi que pour des éléments de longueur canonique 0 (c'est à dire de la forme Δ^p , $p \in \mathbb{Z}$) on a $SS(\Delta^p) = \{\Delta^p\}$.

Le concept de Summit Set a été amélioré par ElRifai et Morton grâce aux formes normales [24]. L'ensemble E_x est cette fois un sous-ensemble du Summit Set de x , appelé *Super Summit Set* (et noté $SSS(x)$), qui consiste en l'ensemble des conjugués de x dont la longueur canonique est minimale, ou de manière équivalente, ayant *simultanément* leur infimum maximal et leur supremum minimal. La longueur canonique d'un élément de $SSS(x)$, autrement dit la longueur canonique minimale d'un conjugué de x est notée $\ell_s(x)$.

On remarque que les algorithmes proposés par Garside d'une part et ElRifai et Morton d'autre part ne s'appuient pas sur la notion d'élément conjuguant minimal mais sur une propriété de connexité plus faible : pour $y, y' \in SS(x)$ (respectivement $SSS(x)$), il existe un entier $m \geq 1$, des éléments $y = y_1, \dots, y_{m+1} = y'$ de $SS(x)$ (respectivement $SSS(x)$) et des éléments *simples* s_1, \dots, s_m tels que pour $i = 1, \dots, m$, $y_{i+1} = y_i^{s_i}$. L'étape correspondant à l'étape 2°(b) de l'algorithme 2.3.4 nécessite de calculer les conjugués de y par *tous* les éléments simples puis de retenir ceux qui ont la propriété convenable. De plus, dans l'algorithme de Garside, l'étape 1° n'a pas lieu. L'algorithme commence avec $x \in G$, $E = \{x\}$, $E' = \emptyset$ puis procède à l'étape 2° de l'algorithme 2.3.4 (avec

$$A_y = \{y^s | s \text{ simple}\} \cap \{y \in G | \inf(y) \geq \inf(x)\}.$$

Si un conjugué y de x avec $\inf(y) > \inf(x)$ est obtenu ainsi, alors l'algorithme doit recommencer au début avec $E = \{y\}$ et $E' = \emptyset$. Enfin, notons que les deux algorithmes de Garside et de ElRifai et Morton ont été initialement conçus dans le cadre des groupes de tresses (de même que le Théorème 2.3.7 ci-dessous).

Dans le travail d'ElRifai et Morton, la technique de calcul d'un premier élément x_0 du Super Summit Set est basée sur les opérations suivantes :

DÉFINITION 2.3.5. [24] *Soit $x \in G$. Soit $x = \Delta^p x_1 \dots x_r$ la forme normale de x . Supposons $r \geq 1$. On définit :*

- le *cyclage* $\mathbf{c}(x) = x^{\iota(x)} = \Delta^p x_2 \dots x_r \tau^{-p}(x_1)$,
- le *décyclage* $\mathbf{d}(x) = x^{\varphi(x)^{-1}} = \Delta^p \tau^p(x_r) x_1 \dots x_{r-1}$.

Si $\ell(x) = 0$, on définit aussi $\mathbf{c}(x) = \mathbf{d}(x) = x$.

Notons que cyclage et décyclage n'augmentent pas le supremum, ni ne diminuent l'infimum. En particulier, pour tout $x \in G$, $\ell(\mathbf{c}(x)) \leq \ell(x)$ et $\ell(\mathbf{d}(x)) \leq \ell(x)$. Ainsi, cyclage et décyclage préservent les Super Summit Sets. Cette observation permet à Gebhardt [31] de considérer un nouvel invariant de conjugaison : pour $x \in G$, le *Ultra Summit Set* de x (noté $USS(x)$) est l'ensemble des points périodiques de \mathbf{c} dans $SSS(x)$. Notons qu'une définition analogue est possible, en utilisant le décyclage au lieu du cyclage. C'est cette asymétrie qui conduit Gebhardt et González-Meneses à introduire un nouveau type de conjugaison, appelé *glissement cyclique*, qui unifie cyclage et décyclage en un seul concept théorique plus simple [33] :

DÉFINITION 2.3.6. [33] *Soit $x \in G$. Soit $x = \Delta^p x_1 \dots x_r$ la forme normale de x . Supposons $r \geq 1$. On définit le préfixe préféré de x par la formule*

$$\mathbf{p}(x) = \iota(x) \wedge \partial(\varphi(x)).$$

Le glissement cyclique est défini comme la conjugaison par le préfixe préféré :

$$\mathbf{s}(x) = x^{\mathbf{p}(x)}.$$

Si $\ell(x) = 0$ on définit $\mathbf{s}(x) = x$.

Notons que cette nouvelle opération préserve aussi les Super Summit Sets : pour tout $x \in G$, $\ell(\mathfrak{s}(x)) \leq \ell(x)$. Nous avons mentionné que le calcul d'un premier élément x_0 du Super Summit Set d'un élément x de G était basé sur les opérations **c** et **d**. Le résultat suivant obtenu par Birman, Ko et Lee [9] dans le cadre des groupes de tresses et énoncé originalement en termes de cyclage et décyclage, est avantageusement simplifié grâce à la notion de glissement cyclique.

THÉORÈME 2.3.7. [9, 33] *Soit $x \in G$. Si $\ell(x)$ n'est pas minimal dans la classe de conjugaison de x , alors il existe un entier $k_0 \in \mathbb{N}$ majoré par $(\|\Delta\| - 1)$ tel que $\ell(\mathfrak{s}^{k_0}(x)) < \ell(x)$.*

Ce résultat fournit une procédure pour calculer un premier élément du Super Summit Set de x , pour $x \in G$ (étape 1°) de l'algorithme 2.3.4). Il suffit d'appliquer itérativement à x l'opération \mathfrak{s} jusqu'à ce que la longueur canonique reste constante durant $(\|\Delta\| - 1)$ itérations. Si x est exprimé comme un mot sur $\mathcal{S} \cup \mathcal{S}^{-1}$ de longueur au plus l , cela a une complexité $O(\lambda^2 \|\Delta\|^2)$. En effet, la mise en forme normale de x a un coût $O(\lambda^2 \|\Delta\|)$ puis chaque itération de \mathfrak{s} a un coût $O(\lambda \|\Delta\|)$, voir ([32], section 4). Simultanément, on obtient un test avec la même complexité algorithmique pour déterminer si un élément donné de G est membre de son propre Super Summit Set ou non.

L'opération \mathfrak{s} est ultimement périodique ; cela permet de définir un nouvel invariant de conjugaison (qui est un sous-ensemble du Super Summit Set). Bien que plus naturel, ce nouvel invariant semble toujours pâtir d'un déficit de notoriété par rapport à son ancêtre *USS*.

DÉFINITION 2.3.8. *Soit $x \in G$. On appelle ensemble des circuits glissants de x l'ensemble des conjugués de x qui sont des points périodiques du glissement cyclique. En formule, $SC(x) = \{y \in x^G \mid \exists k \in \mathbb{N} - \{0\}, \mathfrak{s}^k(y) = y\}$.*

La définition même de SC donne un moyen de calculer, pour $x \in G$, un élément de $SC(x)$: il suffit d'appliquer itérativement l'opération \mathfrak{s} jusqu'à obtenir une répétition. Malheureusement, le nombre d'itérations requises pour obtenir cette répétition demeure mystérieux. La conjecture suivante est l'une des plus importantes questions ouvertes concernant l'algorithmique des groupes de Garside :

CONJECTURE 2.3.9. ([40], Conjecture 3.5) *Il existe un polynôme T , dépendant seulement de G et de sa structure de Garside (i.e. de $\|\Delta\|$) tel que pour tout $x \in G$, $\mathfrak{s}^{T(\ell(x))}(x) \in SC(x)$.*

Au chapitre 7, nous prouverons cette conjecture pour certains éléments pseudo-Anosov des groupes de tresses (voir théorème 7.1.1).

Sans rentrer dans les détails, indiquons que depuis [29], plusieurs algorithmes pour calculer les flèches minimales ont été développés (voir [29] algorithme 6, [32] algorithme 2). Enfin, il est important de mentionner que, de manière générale, $SC(x)$ est beaucoup plus petit que $SSS(x)$, pour $x \in G$; voir à ce titre les expériences menées sur ordinateur dans le cas des groupes de tresses et détaillées dans [31]. Cependant, même dans le cas des groupes de tresses, il n'existe pas de borne générale moins qu'exponentielle (par rapport aux paramètres n et ℓ) sur le cardinal de $SC(x)$, $x \in B_n$. En effet, González-Meneses a exhibé une famille de tresses dont la taille de l'ensemble des circuits glissants pour la structure classique croît exponentiellement avec le nombre de brins et la longueur canonique ([39], proposition 5.5). Nous reviendrons largement sur cette question, voir notamment théorème 8.1.2.

2.3.2. Eléments rigides. Nous allons détailler dans ce paragraphe le cas des éléments *rigides* d'un groupe de Garside G . Avant d'en donner la définition, il convient de rappeler quelques faits utiles pour la suite. La première observation est que les ensembles de circuits glissants sont stables par conjugaison par Δ , par cyclage et décyclage. Par ailleurs pour $x \in G$ et $y \in SC(x)$, les flèches minimales pour y admettent une agréable description en termes de la forme normale de y :

PROPOSITION 2.3.10. ([8], corollaire 2.7) *Soit $x \in G$ avec $\ell_s(x) > 0$. Pour tout $y \in SC(x)$, les flèches minimales pour y sont des préfixes de $\iota(y)$ ou de $\partial(\varphi(y))$ (ou des deux à la fois).*

Remarquons que $SC(x)$ peut être remplacé dans cet énoncé par l'un quelconque des invariants E_x défini au paragraphe 2.3.1. Enfin, pour $x \in G$, nous notons $SCG(x)$ le graphe associé à l'invariant $SC(x)$ (définition 2.3.2).

Nous définissons maintenant la notion de rigidité. Les éléments rigides sont en quelque sorte les plus simples d'un point de vue algébrique; ce sont notamment des points fixes du glissement cyclique :

DÉFINITION 2.3.11. *Soit $x \in G$. Soit $x = \Delta^p x_1 \dots x_r$ la forme normale de x . Supposons $r \geq 1$. On dit que x est rigide si la paire $\varphi(x)\iota(x)$ est pondérée, ou de manière équivalente si $\mathbf{p}(x) = 1$.*

Par convention, un élément de longueur canonique 0 n'est pas rigide. On remarque qu'il existe une notion plus générale de rigidité ([6], définition 3.3) mais nous n'en ferons pas usage.

Nous souhaitons étudier la structure de l'ensemble des conjugués rigides d'un élément x de G . Il est possible que cet ensemble soit vide, par exemple l'élément $x = \sigma_1 \sigma_3 \sigma_2$ de B_4 avec la structure classique satisfait $\mathbf{p}(x) = x$ et est un point fixe non rigide de \mathfrak{s} ; de plus, $SC(x) = \{\sigma_1 \sigma_3 \sigma_2, \sigma_2 \sigma_1 \sigma_3\}$ et $\sigma_2 \sigma_1 \sigma_3$ est aussi un point fixe non rigide de \mathfrak{s} . Puisque les conjugués rigides de x sont nécessairement membres de $SC(x)$, x n'a aucun conjugué rigide.

Lorsque un élément x de G a un conjugué rigide, alors l'ensemble des conjugués rigides de x est exactement l'ensemble des circuits glissants de x ([33], théorème 1). Par conséquent, étudier l'ensemble des conjugués rigides de x revient dans ce cas à étudier l'ensemble $SC(x)$.

Nous supposons désormais que x est un élément rigide de G et nous décrivons la structure du graphe $SCG(x)$. Notons d'abord que les graphes $SCG(x)$ et $SCG(x^{-1})$ sont isomorphes, via $y \mapsto y^{-1}$ au niveau des sommets et $s \mapsto s$ au niveau des flèches ([8], corollaire 3.10).

Une notion cruciale dans notre étude est celle d'orbite d'un élément $y \in SC(x)$:

DÉFINITION 2.3.12. *Soit $x \in G$ un élément rigide. Soit $y \in SC(x)$. On appelle orbite de y l'ensemble $O_y = \{\tau^k \mathbf{c}^l(y), k, l \in \mathbb{N}\}$.*

L'orbite de $y \in SC(x)$ est un sous-ensemble de $SC(x)$. Le lemme suivant décrit de manière précise l'orbite de $y \in SC(x)$, x rigide. Même si ses conclusions sont bien connues, nous en donnons une preuve pour être aussi complet que possible.

LEMME 2.3.13. *Soit $x \in G$ un élément rigide. Soit $y \in SC(x)$. Notons $p = \text{inf}(x)$ et $r = \ell(x)$.*

- (i) *L'orbite O_y est stable par cyclage, décyclage, et τ ; en particulier, pour tout $z \in O_y$, $z^{\iota(z)}$ et $z^{\partial(\varphi(z))}$ sont des éléments de O_y .*
- (ii) *Pour tous $y_1, y_2 \in SC(x)$, $O_{y_1} \neq O_{y_2}$ si et seulement si $O_{y_1} \cap O_{y_2} = \emptyset$.*
- (iii) *Le cardinal de l'orbite O_y est borné supérieurement par $f \cdot \ell(y)$ (où f est l'ordre de τ).*

DÉMONSTRATION. (i) La stabilité de O_y par cyclage et conjugaison par Δ est contenue dans la définition (puisque \mathbf{c} et τ commutent). Montrons que $\mathbf{d}(z) \in O_y$ dès lors que $z \in O_y$. Soit $\Delta^p z_1 \dots z_r$ la forme normale de z . Alors

$$\mathbf{d}(z) = \Delta^p \tau^p(z_r) z_1 \dots z_{r-1}.$$

Cette dernière expression est une forme normale puisque z était rigide. Par ailleurs, on observe que (à cause de la rigidité), $\mathbf{d}(z) = \tau^p(\mathbf{c}^{r-1}(z))$, qui est un élément de O_y par définition. Pour la deuxième partie de l'affirmation, il suffit de se rappeler que $z^{\iota(z)} = \mathbf{c}(z)$ et que $z^{\partial(\varphi(z))} = \tau(\mathbf{d}(z))$.

Remarque. Soit f l'ordre de l'automorphisme τ . On observe que pour tout $m \in \mathbb{N}$ et pour tout $z \in SC(x)$, $\mathbf{c}^{rm}(z) = \tau^{-pm}(z)$; ainsi, pour tout $m \in \mathbb{N}$ et pour tout $z \in SC(x)$,

$$\mathbf{c}^{rfm}(z) = z.$$

- (ii) Il suffit de montrer que pour tout $y \in SC(x)$ et pour tout $z \in O_y$, $O_z = O_y$. L'inclusion $O_z \subset O_y$ est vraie par la partie (i). Réciproquement, soient $k, l \in \mathbb{N}$ tels que $z = \tau^k \mathbf{c}^l(y)$. Nous

montrons que $y \in O_z$. Soit j le plus petit entier positif tel que $rfj > l$. On a alors, en vertu de la remarque ci-dessus,

$$\mathbf{c}^{rfj-l}(\tau^{k(f-1)}(z)) = y$$

donc $y \in O_z$ et par (i), $O_y \subset O_z$, comme nous voulions montrer.

(iii) Considérons les r premiers cyclages successifs des f éléments

$$y, \tau(y), \dots, \tau^{f-1}(y).$$

Cela fournit au plus rf éléments de O_y . Nous affirmons que cela construit tous les éléments de O_y . En effet, soit $z = \tau^k(\mathbf{c}^l(y))$. Soit $m \in \mathbb{N}$ tel que $rm \leq l < r(m+1)$. Alors $l - rm \in [0, \dots, r-1]$ et

$$z = \tau^k(\mathbf{c}^{rm}(\mathbf{c}^{l-rm}(y))) = \tau^{k-rm}(\mathbf{c}^{l-rm}(y))$$

(la deuxième égalité en vertu de la remarque), donc z apparaît comme l'un des r premiers cyclages de l'un des $y, \tau(y), \dots, \tau^{f-1}(y)$. \square

La relation $x \sim y$ si et seulement si $O_x = O_y$ est une relation d'équivalence sur $SC(x)$ et $SC(x)$ est la réunion disjointe des différentes orbites O_y . Soit $\widetilde{SC}(x)$ l'ensemble quotient $SC(x)/\sim$. On commence par décrire un "graphe-quotient" correspondant à $\widetilde{SC}(x)$ de la même façon que $SCG(x)$ correspond à $SC(x)$. Pour cela, on introduit la définition suivante :

DÉFINITION 2.3.14. Soit $y \in SC(x)$. Soit s une flèche minimale pour y . On dit que s est une flèche minimale utile si $y^s \notin O_y$.

REMARQUE 2.3.15. D'après la proposition 2.3.10 et le lemme 2.3.13 (i), les flèches minimales utiles pour y sont des préfixes stricts de $\iota(y)$ ou de $\partial(\varphi(y))$.

Rappelons la notion de *transport sous cyclage* d'une flèche, due à Gebhardt [31] : si $y, s \in G$, on définit le transport de s sous cyclage en y par la formule $s_y^{(1)} = \iota(y)^{-1}s\iota(y^s)$. Il est connu ([31], corollaire 2.7) que le transport induit une bijection entre l'ensemble des flèches minimales pour $y \in SC(x)$ et l'ensemble des flèches minimales pour $\mathbf{c}(y)$. De plus, la conjugaison par Δ induit également une bijection entre les flèches minimales pour y et les flèches minimales pour $\tau(y)$. En particulier, si s est une flèche minimale utile entre y et y^s , alors $s_y^{(1)}$ est une flèche minimale utile entre $\mathbf{c}(y)$ et $\mathbf{c}(y^s)$ et $\tau(s)$ est une flèche minimale utile entre $\tau(y)$ et $\tau(y^s)$. On peut alors définir sans ambiguïté le graphe-quotient souhaité :

DÉFINITION 2.3.16. A tout élément rigide $x \in G$, on associe un graphe connexe orienté $\widetilde{SCG}(x)$ défini de la façon suivante :

- Chaque sommet correspond à un élément de $\widetilde{SC}(x)$,
- Pour tout élément $O_y \in \widetilde{SC}(x)$, on choisit un représentant y' de O_y . A chaque flèche minimale utile s pour y' , de $y' \in O_y$ vers $z' \in O_z$, on associe une arête orientée de O_y vers O_z .

L'étude des flèches minimales utiles s'avère très fructueuse ; à titre d'exemple nous donnons un algorithme cubique pour résoudre DC et RC dans le groupe des tresses à 3 brins, muni de sa structure de Garside classique. Cet exemple sert aussi d'introduction au chapitre 8 où nous verrons une application des mêmes techniques au cas des tresses à 4 brins (voir théorème 8.1.2).

Rappelons que la structure classique de B_3 contient seulement 4 éléments simples distincts de 1 et Δ , à savoir $\sigma_1, \sigma_2, \sigma_1\sigma_2$ and $\sigma_2\sigma_1$.

PROPOSITION 2.3.17. Soit x une tresse à 3 brins, $p = \inf(x)$ et $r = \ell(x)$. Soient $x_1, \dots, x_r \in B_3^+$ des éléments simples non triviaux. Si $x = \Delta^p x_1 \cdots x_r$, alors cette écriture est la forme normale de x .

DÉMONSTRATION. Si ce ne l'était pas, il existerait un indice $i = 1, \dots, r-1$ tel que la paire (x_i, x_{i+1}) n'est pas pondérée ; un glissement local créerait alors un facteur Δ , contredisant $\inf(x) = p$ ou diminuerait le nombre de facteurs, contredisant $\sup(x) = r$ ou encore les deux simultanément. \square

Rappelons que si $x \in G$, $\ell_s(x)$ désigne la longueur canonique des éléments du Super Summit Set de x .

PROPOSITION 2.3.18. *Soit x une tresse à 3 brins avec $\ell_s(x) > 1$. Alors x admet un conjugué rigide. De plus, $SSS(x)$ est l'ensemble des conjugués rigides de x .*

DÉMONSTRATION. Soit $y \in SSS(x)$, soit $y = \Delta^p y_1 \dots y_r$ sa forme normale. Alors $\mathbf{c}(y) = \Delta^p y_2 \dots y_r \tau^{-p}(y_1) \in SSS(x)$ satisfait $\inf(\mathbf{c}(y)) = p$ et $\ell(\mathbf{c}(y)) = r$. Par la proposition 2.3.17, la dernière expression pour $\mathbf{c}(y)$ est sa forme normale et par conséquent la paire $(x_r, \tau^{-p}(x_1))$ est pondérée; en d'autres termes y est rigide. \square

PROPOSITION 2.3.19. *Soit x une tresse à 3 brins avec $\ell_s(x) > 0$. Alors le cardinal de $SSS(x)$ est supérieurement borné par $2 \cdot \ell_s(x)$.*

DÉMONSTRATION. Les éléments de longueur canonique 0 ont un Super Summit Set réduit à un élément (une puissance de Δ). De plus, toute tresse de longueur canonique 1 est un élément de son Super Summit Set (puisque'elle n'est pas conjuguée à une puissance de Δ et donc sa longueur canonique est déjà minimale). Puisque l'infimum est constant à l'intérieur du super Summit set et comme σ_1 et σ_2 sont conjugués (par Δ), on a

$$\begin{aligned} SSS(\Delta^k \sigma_1) &= \{\Delta^k \sigma_1, \Delta^k \sigma_2\}, \\ SSS(\Delta^k \sigma_1 \sigma_2) &= \{\Delta^k \sigma_1 \sigma_2, \Delta^k \sigma_2 \sigma_1\}, \end{aligned}$$

pour tout $k \in \mathbb{Z}$. Cela prouve l'assertion lorsque $\ell_s(x) = 1$.

Supposons maintenant $\ell_s(x) > 1$. En vertu de la proposition 2.3.18, les ensembles $SSS(x)$ et $SC(x)$ sont les mêmes. En vertu du lemme 2.3.13 (iii), il suffit de montrer que le graphe $\widetilde{SCG}(x)$ a un seul sommet (rappelons que pour la structure classique, τ est une involution). Cela revient à montrer que $y \in SC(x)$ ne peut pas avoir de flèche minimale utile. Mais la conjugaison de $y \in SC(x)$ par un préfixe strict de $\iota(y)$ ou de $\partial(\varphi(y))$ augmenterait la longueur canonique, ce qui prouve notre affirmation. \square

Cela fournit un algorithme pour résoudre DC et RC en temps polynômial par rapport à la longueur des entrées dans le groupe B_3 .

COROLLAIRE 2.3.20. *Les problèmes DC et RC sont résolubles en temps $O(l^3)$ dans B_3 .*

DÉMONSTRATION. Supposons que $x, y \in B_3$ sont donnés comme des mots de longueur l , disons sur les générateurs d'Artin. Prenons $E_x = SSS(x)$; alors l'étape 1° de l'algorithme 2.3.4 est faisable en temps $O(l^2)$ en vertu du théorème 2.3.7 et l'étape 2° en temps $O(l^3)$, pour la structure classique comme pour la structure duale, en vertu de ([29], propositions 6.2 et 6.4). \square

Le problème de réductibilité : travaux antérieurs

Nous revenons maintenant au problème de décision du type de Nielsen-Thurston d'une tresse. Nous en cherchons une solution algorithmique de complexité polynômiale (en fonction du nombre de brins n et de la longueur l). L'objet de ce chapitre est de mettre en lumière le lien entre ce problème et les techniques algébriques développées au chapitre 2. Le principal résultat est dû à Benardete, Gutierrez et Nitecki (voir théorème 3.3.1). Avant de l'énoncer et d'en étudier quelques conséquences (section 3.3), nous expliquons pourquoi il est aisé de reconnaître une tresse périodique, ramenant notre problème à la dichotomie pseudo-Anosov/réductible (section 3.1). La section 3.2 récapitule les notions de courbe ronde et de standardisateur. Enfin, on trouvera dans la section 3.4 un résumé de l'article [40], dont l'algorithme sera adapté au chapitre 7.

3.1. Réductible ou pseudo-Anosov

Par définition, les tresses périodiques sont les éléments de B_n dont la projection dans $Mod(\mathbb{D}_n) \cong B_n / \langle \Delta^2 \rangle$ est d'ordre fini. Nous en donnons maintenant une nouvelle caractérisation.

Soit donc x une tresse périodique. Notons \hat{x} la projection de x dans le groupe $Mod(\mathbb{D}_n)$ et m l'ordre de \hat{x} . On peut voir \hat{x} comme un élément (d'ordre m) du sous-groupe $Mod(\mathbb{S}_{n+1, p_{n+1}})$ de $Mod(\mathbb{S}_{n+1})$ formé par les éléments qui fixent le $(n+1)$ -ième trou. Il existe alors un représentant $\hat{x}_0 \in Homeo^+(\mathbb{S}_{n+1, p_{n+1}})$ de \hat{x} tel que \hat{x}_0 est d'ordre m (théorème de réalisation de Nielsen [26], théorème 7.1). Maintenant, un théorème classique de Eilenberg [23] et Kerékjártó [18] affirme que \hat{x}_0 est conjugué dans $Homeo^+(\mathbb{S}_{n+1, p_{n+1}})$ à une rotation r de la sphère \mathbb{S}_{n+1} . Selon le nombre de trous (autre p_{n+1}) qui se trouvent sur l'axe de cette rotation, on voit que la tresse x doit être conjuguée soit à une puissance de $\delta = \sigma_1 \dots \sigma_{n-1}$ (s'il n'y a pas d'autre trou que p_{n+1} sur l'axe de r), soit à une puissance de $\varepsilon = \delta\sigma_1$ (si l'axe de rotation contient p_{n+1} et un autre trou). Les deux tresses δ et ε sont représentées par la figure 1(a) et (b) respectivement.

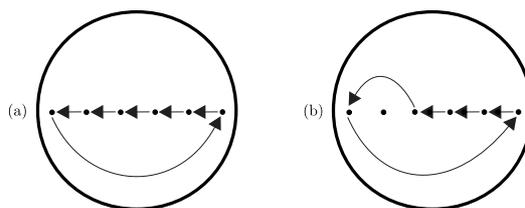


FIGURE 1. (a) La tresse δ , (b) la tresse ε .

On remarque que δ est l'élément de Garside de la structure duale de B_n . Mentionnons aussi que le choix de ε (c'est à dire de laisser le *deuxième* brin fixé) suit la convention de [7], Remarque 3. Les deux tresses δ et ε satisfont $\delta^n = \varepsilon^{n-1} = \Delta^2$. Il est dès lors facile de décider si une tresse est périodique : $x \in B_n$ est périodique si et seulement si x^n ou x^{n-1} est une puissance de Δ^2 ([7], corollaire 5). Il résulte alors des estimations de la complexité du calcul des formes normales données au chapitre 2 (pour la structure classique) un algorithme de complexité $O(l^2 n^3 \log n)$ pour décider si un produit des éléments simples et de leurs inverses avec au plus l facteurs représente une tresse périodique ou non (voir [7], algorithme A). Ainsi, les tresses périodiques peuvent être écartées et

notre problème revient à décider si une tresse non périodique est réductible ou pseudo-Anosov, i.e. réductible ou pas. C'est pourquoi nous parlons de *problème de réductibilité*.

Notons que si x est une tresse non périodique, alors l'existence d'un système de réduction de x , fût-il non essentiel, implique la réductibilité de x . Dans ce qui suit, les courbes considérées sont fermées, simples et non dégénérées et pour alléger la rédaction, nous sous-entendons ces trois qualificatifs. Un *système* de (classes d'isotopie de) courbes est une famille de classes d'isotopie de courbes dont les éléments sont disjoints. De plus, dans tout le chapitre on suppose que les trous de \mathbb{D}_n sont alignés sur le diamètre horizontal du disque, comme sur la figure 3(a) du chapitre 1. Sauf mention du contraire, chaque référence à une notion définie au chapitre 2 s'inscrit dans le cadre de la structure classique de B_n .

3.2. Courbes rondes et standardisation

Afin de décider algorithmiquement de la réductibilité d'une tresse x , on cherche à détecter des courbes de réduction de x . Dans cette optique, la notion de courbe ronde joue un rôle fondamental.

DÉFINITION 3.2.1. *On dit qu'une courbe est ronde si elle est isotope à un cercle géométrique dans \mathbb{D}_n (autrement dit si elle est isotope à une courbe qui intersecte le diamètre horizontal de \mathbb{D}_n exactement deux fois). On dit qu'une classe d'isotopie de courbes dans \mathbb{D}_n est ronde si un de ses représentants (ou de manière équivalente si tout représentant) est rond.*

Cette notion de rondeur nous permet, à l'aide de la théorie de Garside, de définir la complexité d'une (classe d'isotopie de) courbe(s) :

DÉFINITION 3.2.2. *Soit $[C]$ une classe d'isotopie de courbes dans \mathbb{D}_n . On appelle complexité de $[C]$ la longueur canonique minimale d'une tresse positive dont l'action transforme $[C]$ en une classe d'isotopie de courbes rondes. La complexité d'une courbe est alors définie comme la complexité de sa classe d'isotopie.*

Remarquons que si une tresse positive transforme $[C]$ en une classe ronde $[C_0]$, alors il existe une tresse positive de même longueur qui transforme $[C_0]$ en $[C]$. La complexité d'une courbe mesure le degré "d'enchevêtrement" de cette courbe. Intuitivement, plus la complexité d'une courbe est élevée, plus il est difficile d'étudier l'action d'une tresse sur sa classe d'isotopie, et donc de reconnaître si cette dernière est une courbe de réduction pour une tresse donnée.

Par définition, les courbes de complexité 0 sont les courbes rondes. Nous appelons *presque-rondes* les (classes d'isotopie de) courbes de complexité 1. La figure 2 représente 4 courbes de \mathbb{D}_4 . La première est ronde, la seconde est presque-ronde et sa classe d'isotopie est transformée en une classe d'isotopie ronde sous l'action de la tresse simple $\sigma_2\sigma_1\sigma_3$. La troisième (respectivement quatrième) courbe est de complexité 2 (respectivement 4). Sa classe d'isotopie résulte de l'action de la tresse σ_2^2 (respectivement σ_2^4) (de longueur canonique 2 (respectivement 4)) sur la classe d'isotopie de la première.

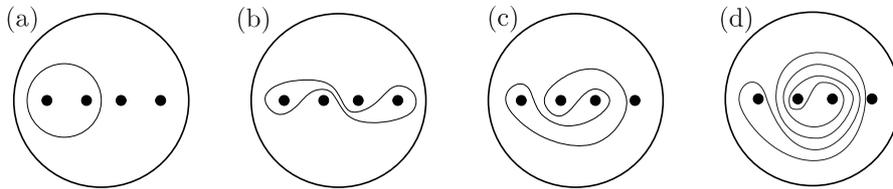


FIGURE 2

Remarquons que les classes d'isotopie de courbes rondes sont en nombre $\frac{n \cdot (n-1)}{2} - 1$. Par contraste, le nombre de classes d'isotopie de courbes de complexité k ($k \geq 1$) dépend exponentiellement de n . Avant de revenir sur le rôle des courbes rondes dans la solution du problème de réductibilité, il

est opportun de rappeler une importante définition, directement reliée aux notions de rondeur et de complexité des courbes.

THÉORÈME 3.2.3. ([42], théorème 4.2) *Soit \mathcal{F} une famille non vide de classes d'isotopies de courbes disjointes dans \mathbb{D}_n . Alors l'ensemble des tresses positives dont l'action transforme \mathcal{F} en une famille de classes d'isotopie de courbes rondes est un sous-treillis non vide de B_n^+ (i.e. stable par les opérations de plus grand diviseur commun et plus petit multiple commun). En particulier, il existe une unique tresse positive minimale par rapport à \preceq qui transforme \mathcal{F} en une famille de classes d'isotopie de courbes rondes.*

On appelle *standardisateur* de \mathcal{F} la tresse minimale dans l'énoncé du Théorème 3.2.3. On note cette tresse $\zeta(\mathcal{F})$. Lorsque \mathcal{F} consiste en une seule classe d'isotopie de courbes $[\mathcal{C}]$, on note $\zeta([\mathcal{C}])$ pour $\zeta(\{[\mathcal{C}]\})$, le *standardisateur* de $[\mathcal{C}]$. Par définition, la complexité d'une courbe \mathcal{C} est donc la longueur canonique du standardisateur $\zeta([\mathcal{C}])$. Les standardisateurs jouissent de très bonnes propriétés, liées à la structure de Garside de B_n . En particulier, le résultat suivant montre que la conjugaison d'une tresse x par le standardisateur d'un système de réduction de x ne peut pas augmenter la "complexité algébrique de x " :

THÉORÈME 3.2.4. ([42], théorème 4.9) *Soit $x \in B_n$ et \mathcal{F} un système de réduction non vide de x . Alors :*

- $\inf(x) \leq \inf(x^{\zeta(\mathcal{F})})$ et $\sup(x) \geq \sup(x^{\zeta(\mathcal{F})})$,
- Si $x \in SSS(x), USS(x)$ ou $SC(x)$, alors $x^{\zeta(\mathcal{F})}$ également.

La notion de standardisateur interviendra dans la preuve de la proposition 3.3.2. Enfin, nous rappelons [42] une importante propriété des tresses qui préservent une famille non vide de classes d'isotopie de courbes rondes disjointes. Si \mathcal{F} est une telle famille, quitte à considérer seulement les composantes les plus extérieures de \mathcal{F} , on peut supposer qu'aucun membre de \mathcal{F} n'en entoure un autre. On peut alors décomposer une tresse x préservant \mathcal{F} en une *tresse intérieure* et une *tresse extérieure*. Intuitivement, chaque élément $[\mathcal{C}]$ de \mathcal{F} entourant p trous donne lieu à une tresse à p brins $x_{[\mathcal{C}]}$ en oubliant tous les brins de x dont le point de départ n'est pas entouré par $[\mathcal{C}]$ (et le point d'arrivée n'est pas entouré par $[\mathcal{C}]^x$). La tresse intérieure est alors la collection des tresses $x_{[\mathcal{C}]}$, pour $[\mathcal{C}] \in \mathcal{F}$. La tresse extérieure est la tresse obtenue à partir de x en considérant comme un seul "gros" brin chaque ensemble de brins de x entouré par un élément de \mathcal{F} . Plus généralement, les tresses intérieure et extérieure associées à une tresse réductible arbitraire sont définies dans [42] à l'aide des notions de standardisateur et de système de réduction canonique.

3.3. Le théorème de Benardete, Gutierrez et Nitecki

Le théorème suivant est le principal résultat reliant les propriétés géométriques d'une tresse à sa forme normale de Garside.

THÉORÈME 3.3.1 ([2], théorème 5.7). *Soit \mathcal{C} une courbe ronde dans \mathbb{D}_n . Soit x une tresse dont la forme normale est $\Delta^p x_1 \cdots x_r$. Si $[\mathcal{C}]^x$ est ronde, alors $[\mathcal{C}]^{\Delta^p x_1 \cdots x_m}$ est ronde, pour tout $m = 1, \dots, r$.*

Nous examinons maintenant plusieurs conséquences du théorème 3.3.1 et en particulier un algorithme pour décider le type de Nielsen-Thurston d'une tresse donnée. D'abord, notons que l'énoncé du théorème 3.3.1 concerne des courbes de complexité 0 ; la notion de standardisateur permet d'en déduire un analogue en complexité quelconque, pour des courbes de réduction *invariantes*. La proposition suivante jouera un rôle essentiel au chapitre 6.

PROPOSITION 3.3.2. *Soit \mathcal{C} une courbe de complexité s dans \mathbb{D}_n . Soit x une tresse dont la forme normale est $\Delta^p x_1 \cdots x_r$ et telle que $[\mathcal{C}]^x = [\mathcal{C}]$. Alors la complexité de $[\mathcal{C}]^{\Delta^p x_1 \cdots x_m}$ est au plus s , pour tout $m = 1, \dots, r$.*

DÉMONSTRATION. Le cas $s = 0$ est une conséquence directe du théorème 3.3.1. Supposons $s \geq 1$. Soit $\zeta := \zeta([\mathcal{C}])$ le standardisateur de $[\mathcal{C}]$. En vertu du théorème 3.2.4 on a $\inf(x^\zeta) \geq \inf(x)$ et $\sup(x^\zeta) \leq \sup(x)$. Moyennant quelques changements mineurs, la proposition 2.1 et le corollaire 2.2 de [31] assurent l'existence de tresses positives $\zeta_0 = \tau^p(\zeta), \zeta_1, \dots, \zeta_r$ telles que la forme normale de x^ζ est

$$\Delta^p(\zeta_0^{-1}x_1\zeta_1) \dots (\zeta_{r-1}^{-1}x_r\zeta_r)$$

(avec éventuellement certains indices $0 \leq i' < i'' \leq r-1$ tels que $\zeta_i^{-1}x_{i+1}\zeta_{i+1} = \Delta$ pour $i \leq i'$ et $\zeta_i^{-1}x_{i+1}\zeta_{i+1} = 1$ pour $i \geq i''$) et

$$\inf(\zeta_i) \geq \inf(\zeta), \quad \sup(\zeta_i) \leq \sup(\zeta) \quad \text{pour } i = 0, \dots, r.$$

Le théorème 3.3.1 nous dit alors que les classes d'isotopie de courbes

$$([\mathcal{C}]^\zeta)^{(\Delta^p(\zeta_0^{-1}x_1\zeta_1) \dots (\zeta_{i-1}^{-1}x_i\zeta_i))}$$

sont rondes, pour tout $i = 1, \dots, r$. Mais cela peut être réécrit comme

$$([\mathcal{C}]^{\Delta^p x_1 \dots x_i})_{\zeta_i}.$$

La complexité de $[\mathcal{C}]^{\Delta^p x_1 \dots x_i}$ est donc au plus $\ell(\zeta_i) \leq \ell(\zeta) = s$. Cela démontre la Proposition 3.3.2. \square

Une autre conséquence du théorème 3.3.1 est l'invariance sous cyclage, décyclage et glissement cyclique, de la propriété de préserver un système de classes d'isotopie de courbes rondes :

PROPOSITION 3.3.3 ([39], proposition 4.2). *Soit $x \in B_n$. Soit \mathcal{F} un système de réduction non vide de x formé de classes d'isotopie de courbes rondes. Alors $\mathcal{F}^{\mathfrak{P}(x)}$ est un système de réduction de $\mathfrak{s}(x)$ formé de classes d'isotopie de courbes rondes.*

Soit x une tresse réductible. On peut trouver un conjugué y de x tel que y préserve un système de courbes de réduction rondes. La proposition 3.3.3 et le théorème 2.3.7 impliquent alors :

COROLLAIRE 3.3.4 ([2], théorème 5.8, [39], corollaire 4.3). *Soit x une tresse réductible. Alors il existe $y \in SSS(x)$ (respectivement $SC(x)$) tel que y préserve un système de courbes de réduction rondes.*

Le théorème 3.3.1 fournit un algorithme pour décider de la réductibilité d'une tresse. D'une part, il conduit à un test rapide (polynômial en n et ℓ) pour détecter l'existence d'un système de courbes de réduction rondes, comme expliqué dans la section 6 de [2]. D'autre part, le corollaire 3.3.4 nous dit qu'il suffit d'appliquer ce test à tout élément du Super Summit Set (respectivement de l'ensemble des circuits glissants) : la tresse initiale est pseudo-Anosov si et seulement si le test est négatif pour tout élément de son Super Summit Set (respectivement ensemble de circuits glissants). Comme le montre la proposition 5.5 de [39], cette partie de l'algorithme n'a pas une complexité polynômiale en général, ni en n ni en la longueur (remarquons que l'exemple donné dans [39] est une tresse réductible). Observons le cas exceptionnel des tresses à 3 brins, situation dans laquelle la proposition 2.3.19 implique une complexité polynômiale pour l'algorithme que nous venons de décrire :

PROPOSITION 3.3.5. *Le problème de réductibilité est résoluble en temps $O(l^3)$ dans le groupe B_3 .*

DÉMONSTRATION. Le calcul du Super Summit Set d'un élément x de B_3 est faisable en temps $O(l^3)$, et pour chacun des éléments de $SSS(x)$ (qui sont en nombre $O(l)$, proposition 2.3.19) le test précédent coûte $O(l)$. \square

Afin d'éviter le calcul d'un "gros" sous-ensemble de la classe de conjugaison d'une tresse donnée, plusieurs auteurs ont cherché à modifier l'énoncé du corollaire 3.3.4 en exhibant un invariant de conjugaison E_x (au sens de la section 2.3) tel que x est réductible si et seulement si on peut détecter

facilement des courbes de réduction pour *tout* élément de E_x (par exemple, si tout élément de E_x préserve un système de classes d'isotopie de courbes rondes).

A l'exception des tresses à 4 brins (voir proposition 6.2.1), notons déjà que le Super Summit Set ne peut jouer ce rôle, comme le montre l'exemple suivant ; c'est une tresse réductible dont les seules courbes de réduction sont de complexité 2 :

EXEMPLE 3.3.6. Considérons la tresse

$$z = \sigma_1 \sigma_2 \sigma_1 \sigma_3 \sigma_2 \sigma_1 \cdot \sigma_1 \sigma_3 \cdot \sigma_1 \sigma_3 \sigma_2 \sigma_4 \cdot \sigma_2 \sigma_1 \sigma_4 \sigma_3 \sigma_2 \sigma_1 \cdot \sigma_1 \sigma_2 \sigma_1 \cdot \sigma_1 \sigma_2 \sigma_1 \sigma_3 \sigma_2 \cdot \sigma_3 \in B_5.$$

Alors z est en forme normale comme écrite, $z \in SSS(z)$, et z n'a aucune courbe de réduction ronde (ni presque-ronde). En revanche, z préserve la classe d'isotopie de la courbe de complexité 2 de la figure 3. Remarquons que c'est une courbe de réduction essentielle puisque la tresse intérieure est pseudo-Anosov (la tresse intérieure est l'élément de B_3 dont les brins sont représentés en gras, à savoir $\sigma_1 \sigma_2 \sigma_1^3 \sigma_2^2 \sigma_1^3 \sigma_2 \sigma_1 \sigma_2$.)

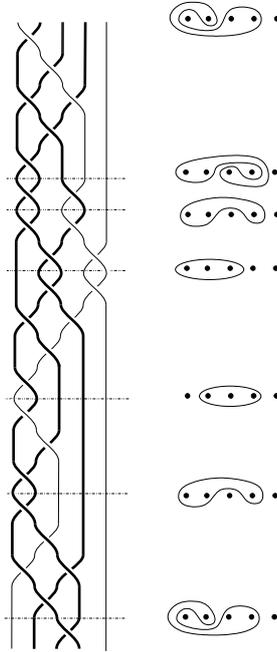


FIGURE 3. La tresse de l'Exemple 3.3.6, les traits pointillés indiquent les séparations entre les facteurs de Garside.

En s'appuyant sur les notions de tresses intérieure et extérieure associées à une tresse réductible, Lee et Lee ont montré (théorème 7.4 de [42]), modulo une hypothèse technique sur la longueur canonique de la tresse extérieure, que si x est une tresse réductible, alors *tout* élément de $USS(x)$ admet un système de courbes de réduction rondes.

3.4. L'algorithme de González-Meneses et Wiest

Nous présentons maintenant les résultats obtenus par González-Meneses et Wiest dans [40]. Leur démarche s'inscrit dans la continuité du résultat de Lee et Lee que nous venons de mentionner. Cette fois, l'invariant de conjugaison considéré est une légère restriction de l'ensemble des circuits glissants :

DÉFINITION 3.4.1. ([40], définition 3.3) *Soit $x \in B_n$, soit m un entier strictement positif. On appelle ensemble des circuits glissants m -stables de x l'ensemble*

$$SC^{[m]}(x) = \{y \in x^{B_n} \mid \forall i = 1, \dots, m, y^i \in SC(x^i)\}.$$

Pour tout entier naturel non nul m l'ensemble $SC^{[m]}(x)$ est un invariant de conjugaison fini et non vide ([40], proposition 4.4). On observe que cette définition s'étend naturellement au contexte d'un groupe de Garside quelconque. Le résultat principal de [40] est le suivant :

THÉORÈME 3.4.2. ([40], théorème 3.4) *Soit $x \in B_n$ une tresse réductible. Alors il existe un entier $m \leq \|\Delta\|^3 - \|\Delta\|^2$ tel que tout élément de $SC^{[m]}(x)$ admet une courbe de réduction essentielle ronde ou presque-ronde.*

La preuve de ce résultat repose sur l'étude des tresses réductibles rigides :

THÉORÈME 3.4.3. ([40], théorème 5.16) *Soit $x \in B_n$ une tresse réductible rigide. Alors il existe un entier $k \leq n$ tel que l'une des conditions suivantes est satisfaite :*

- (i) x^k préserve une courbe de réduction essentielle ronde,
- (ii) $\inf(x^k)$ et $\sup(x^k)$ sont pairs et soit $\Delta^{-\inf(x^k)}x^k$, soit $x^{-k}\Delta^{\sup(x^k)}$ est une tresse positive préservant une courbe de réduction essentielle presque-ronde dont les brins intérieurs ne se croisent pas.

Soit $N = \|\Delta\|^3 - \|\Delta\|^2$. Sommairement, la preuve du théorème 3.4.2 découle maintenant de l'existence, pour tout élément y de l'ensemble des circuits glissants N -stables d'une tresse réductible x , d'une puissance y^m rigide, pour $m \leq N$ ([40] lemme 5.15). Ainsi, tout élément $z \in SC^{[m]}(x)$ a sa m -ième puissance rigide et le théorème 3.4.2 en découle, en observant que les courbes de réduction (essentielles) de z^m sont aussi des courbes de réduction (essentielles) de z .

En sus des courbes rondes, il nous faut donc considérer aussi des courbes de réduction presque-rondes lesquelles sont en nombre exponentiel par rapport à n . Pour détecter une courbe de réduction presque-ronde en temps polynômial, il nous faut donc éviter un test texhaustif. C'est l'objet du résultat suivant :

THÉORÈME 3.4.4. ([40], théorème 2.9) *Il existe un algorithme qui décide si une tresse positive x donnée en forme normale et de longueur canonique au plus ℓ préserve une courbe de réduction presque-ronde dont les brins intérieurs ne se croisent pas. La complexité de cet algorithme est $O(\ell \cdot n^4)$.*

Pour obtenir une solution polynômiale au problème de réductibilité à partir du théorème 3.4.2, on doit enfin être capable de trouver, pour $x \in B_n$, un élément $z \in SC(x)$ et ce via un procédé de complexité polynômiale en n et ℓ . Un tel procédé n'est pas connu à ce jour, voir Conjecture 2.3.9. Comme nous l'avons déjà mentionné, nous donnerons dans ce texte une preuve partielle de la Conjecture 2.3.9, qui nous permet d'adapter l'algorithme de [40], voir chapitre 7.

Nous concluons ce chapitre par une introduction conjointe aux chapitres 4 et 5. Nous y décrivons l'ensemble des résultats de [13]. La nécessité d'utiliser non seulement des courbes rondes, mais aussi presque-rondes, remet en cause le choix de la structure de Garside classique pour la mise en oeuvre des techniques présentées dans le présent chapitre. Afin d'utiliser la structure de Garside duale au lieu de la structure classique, il est indispensable d'établir l'analogie du théorème fondamental (théorème 3.3.1). Cela est mené à bien au chapitre 5 (théorème 5.1.3). Nous observons que les preuves du théorème 3.3.1 données par Benardete-Gutierrez-Nitecki puis par Lee et Lee ne s'adaptent pas naturellement au cadre dual. Pour cette raison, nous développons de nouvelles techniques qui conduisent parallèlement à une nouvelle preuve du théorème 3.3.1, voir chapitre 4. On remarque enfin que les méthodes algébriques développées dans [36] et basées sur la théorie des catégories de Garside permettent une généralisation du théorème 3.3.1 à tous les groupes d'Artin de type fini, munis de leur structure de Garside classique [36]. Il semble en outre [34] que les mêmes techniques pourraient s'étendre au cas de la structure de Garside duale, pour tous les groupes d'Artin de type fini ; toutefois cela n'apparaît pas dans la littérature.

Le problème de réductibilité : courbes rondes et la structure classique

Ce chapitre est dédié à la preuve du théorème 3.3.1. Afin d'introduire la démonstration, nous en donnons d'abord une ébauche simplifiée, sans détails techniques (section 4.1). Le mot "courbe" seul désignera toujours une courbe fermée simple non dégénérée dans \mathbb{D}_n et tous les concepts de théorie de Garside convoqués dans ce chapitre s'inscrivent dans le cadre de la structure classique de B_n . L'argument repose sur une description rigoureuse des courbes dans \mathbb{D}_n à l'aide de mots dont les lettres sont des numéros (intersections des courbes avec le diamètre horizontal de \mathbb{D}_n) et des arcs semi-circulaires ayant pour diamètre un segment inclus dans le diamètre horizontal de \mathbb{D} . A chaque classe d'isotopie de courbes $[\mathcal{C}]$, nous associons un unique *mot réduit* $W([\mathcal{C}])$. Cela est détaillé dans la section 4.2. Le mot $W([\mathcal{C}])$ permet de décrire l'action de tresses positives sur la classe d'isotopie $[\mathcal{C}]$. Cela donne lieu à un ensemble de formules, expliquées dans la section 4.3. Enfin, les outils élaborés dans les sections 4.2 et 4.3 nous permettent de prouver le théorème 3.3.1 au cours de la section 4.4.

4.1. Esquisse de la preuve

Supposons que \mathcal{C} est une courbe ronde et x une tresse telle que $[\mathcal{C}]^x$ est ronde. Soit $\Delta^p x_1 \dots x_r$ la forme normale de x . Nous voulons montrer la rondeur de $[\mathcal{C}]^{\Delta^p x_1 \dots x_m}$, pour tout $m = 1, \dots, r$. Pour ce faire, il est suffisant (par induction sur la longueur canonique) de prouver la rondeur de $[\mathcal{C}]^{\Delta^p x_1}$. Nous donnons une preuve par contradiction en démontrant que si $[\mathcal{C}]^{\Delta^p x_1}$ n'est pas ronde, alors $[\mathcal{C}]^{\Delta^p x_1 \dots x_m}$ n'est ronde pour aucun $m = 1, \dots, r$. Cela implique que $[\mathcal{C}]^{\Delta^p x_1 \dots x_r} = [\mathcal{C}]^x$ n'est pas ronde, contredisant les hypothèses du théorème 3.3.1.

On identifie \mathbb{D}_n avec le disque euclidien dans \mathbb{C} dont le diamètre horizontal est le segment $[0, n+1]$ et les points $p_i = i$ ($i = 1, \dots, n$) ôtés. Pour $1 \leq i \leq n$, on note simplement i au lieu de p_i le i -ième trou de \mathbb{D}_n . Nous verrons que si $[\mathcal{C}]^{\Delta^p x_1}$ n'est pas ronde, alors une partie (d'un représentant convenable) de $[\mathcal{C}]^{\Delta^p x_1}$ intersecte la droite réelle comme le montre la figure 1, pour certains entiers $0 \leq i < j < k \leq n$. De plus, la tresse $x_1 \sigma_j$ est simple, autrement dit les brins dans x_1 numérotés j et $j+1$ à la fin de x_1 ne se sont pas croisés dans x_1 (lemme 2.2.2).

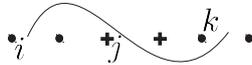


FIGURE 1. Les brins qui arrivent en position j et $j+1$ (représentés par des croix) ne se sont pas croisés dans x_1 .

Nous prouvons alors par récurrence que si $x_1 \dots x_r$ est en forme normale, les propriétés que nous venons d'évoquer doivent être vraies pour $[\mathcal{C}]^{\Delta^p x_1 \dots x_m}$, pour tout $m = 1, \dots, r$. En d'autres termes, une partie (d'un représentant convenable) de $[\mathcal{C}]^{\Delta^p x_1 \dots x_m}$ intersecte la droite réelle comme le montre la figure 1, pour certains entiers $0 \leq i_m < j_m < k_m \leq n$; de plus, $x_m \sigma_{j_m}$ est simple. En particulier, cela implique que $[\mathcal{C}]^{\Delta^p x_1 \dots x_r}$ n'est pas ronde et démontre le théorème 3.3.1. Les mots décrits dans la section 4.2 vont nous permettre de rendre rigoureuse l'idée exprimée par la figure 1 et ainsi, de mener à bien les détails de la preuve que nous venons d'évoquer.

4.2. Des mots pour décrire les courbes

Soit \mathcal{C} une courbe dans \mathbb{D}_n . On peut supposer que \mathcal{C} intersecte la droite réelle un nombre fini de fois, et que tous les croisements sont transverses. Nous allons maintenant associer à \mathcal{C} un mot $W(\mathcal{C})$ en nous inspirant de la stratégie développée dans l'appendice A de [28]. Soit $*$ un point de \mathcal{C} appartenant à la droite réelle (un tel point existe si \mathcal{C} est non dégénérée). Choisissons aussi une orientation pour \mathcal{C} . En parcourant \mathcal{C} selon l'orientation choisie, avec point de départ et d'arrivée $*$, nous construisons un mot sur l'alphabet $X = \{\smile, \frown, 0, \dots, n\}$ de la manière suivante : chaque arc qui traverse le demi-plan supérieur donne une lettre \frown , chaque arc dans le demi-plan inférieur une lettre \smile , et chaque intersection avec le segment $]i, i + 1[$ contribue une lettre i . La lettre correspondant au numéro associé à $*$ peut être placée indifféremment au début ou à la fin du mot. Nous notons $W(\mathcal{C})$ le mot sur X obtenu de cette manière et nous l'appelons le *mot associé* à \mathcal{C} .

Le choix d'un autre point de base $*$ ou le changement de place de la lettre associée à $*$ (au début ou à la fin) correspondent à une permutation cyclique des lettres de $W(\mathcal{C})$. De plus, en choisissant l'orientation inverse pour \mathcal{C} , on obtient le renversement du mot $W(\mathcal{C})$, c'est à dire le même mot, mais lu à l'envers. Ainsi, le mot associé à une courbe est défini modulo permutation cyclique des lettres et modulo renversement.

EXEMPLE 4.2.1. Soit \mathcal{C} la courbe représentée par la figure 2.

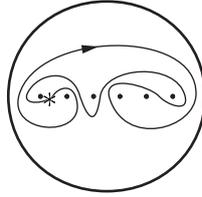


FIGURE 2. La courbe \mathcal{C} de l'Exemple 4.2.1.

Si on fixe le point $*$ dans l'intervalle $]1, 2[$ et l'orientation horaire, alors le mot associé à \mathcal{C} est

$$W(\mathcal{C}) = 1 \frown 2 \smile 0 \frown 6 \smile 3 \frown 5 \smile 6 \frown 3 \smile 2 \frown 0 \smile .$$

On remarque que si \mathcal{C} et \mathcal{C}' sont deux courbes isotopes via une isotopie de \mathbb{D}_n qui préserve globalement le diamètre horizontal, alors $W(\mathcal{C}) = W(\mathcal{C}')$. On dit que le mot associé à \mathcal{C} est *réduit* s'il ne contient aucun sous-mot de la forme $i \smile i$ ou $i \frown i$. On dit qu'une courbe \mathcal{C} est *réduite* si le mot associé $W(\mathcal{C})$ est réduit. On remarque que les courbes réduites sont exactement celles qui ne forment aucun *bigone* (voir [28] ou [26], paragraphe 1.2.4) avec la droite réelle. Selon [28], toute courbe \mathcal{C} est isotope à une courbe réduite \mathcal{C}^{red} . Cette courbe réduite est unique, modulo isotopie de \mathbb{D}_n préservant globalement le diamètre horizontal. On peut donc finalement définir, pour chaque classe d'isotopie de courbes $[\mathcal{C}]$ dans \mathbb{D}_n , le *mot réduit associé* à $[\mathcal{C}]$ par la formule $W([\mathcal{C}]) = W(\mathcal{C}^{red})$.

4.3. L'action des tresses positives

Au lieu des générateurs d'Artin habituels, il va être plus commode d'utiliser un système générateur de B_n^+ plus gros, à savoir

$$\{\Sigma_{p,k} = \sigma_{p-1} \dots \sigma_{p-k}, \quad 1 \leq k < p \leq n\}.$$

La tresse $\Sigma_{p,k}$ correspond au mouvement du p -ième trou à travers le demi-plan supérieur jusqu'à la position $p-k$, tandis que tous les trous $p-1, \dots, p-k$ sont décalés d'une position vers la droite.

Soient \mathcal{C} une courbe et x une tresse positive. Nous décrivons les transformations à effectuer sur le mot $W = W([\mathcal{C}])$ afin d'obtenir le mot $W([\mathcal{C}]^x)$. A cette fin, nous étudions d'abord le cas $x = \Sigma_{p,k}$.

Puisque les générateurs que nous considérons consistent principalement en des mouvements de trous à travers le demi-plan supérieur, nous supposons que l'action des tresses $\Sigma_{p,k}$ transforme principalement les arcs supérieurs \frown qui apparaissent dans W (à partir desquels de nouveaux arcs inférieurs peuvent être créés) tandis que les arcs inférieurs sont transformés seulement par translation de leurs extrémités. Tout cela est commodément décrit par les formules suivantes, qui sont aussi représentées par la figure 3.

Pour $i < j$, on définit :

$$(i \frown j)^{\Sigma_{p,k}} = \begin{cases} i \frown j & \text{si } [p-k, p[\cap \{i, j\} = \emptyset & (F1) \\ (i+1) \frown (j+1) & \text{si } [p-k, p[\cap \{i+1, j\} = \{i+1, j\} & (F2) \\ (i+1) \frown (p-k) \smile (p-k-1) \frown j & \text{si } [p-k, p[\cap \{i, j\} = \{i\} & (F3) \\ i \frown (p-k-1) \smile (p-k) \frown (j+1) & \text{si } [p-k, p[\cap \{i+1, j\} = \{j\} & (F4) \end{cases}$$

On peut définir de la même façon (toujours avec $i < j$) le mot $(j \frown i)^{\Sigma_{p,k}}$. Il suffit de prendre les renversements des formules ci-dessus (en utilisant la même dessin que celui de la figure 3).

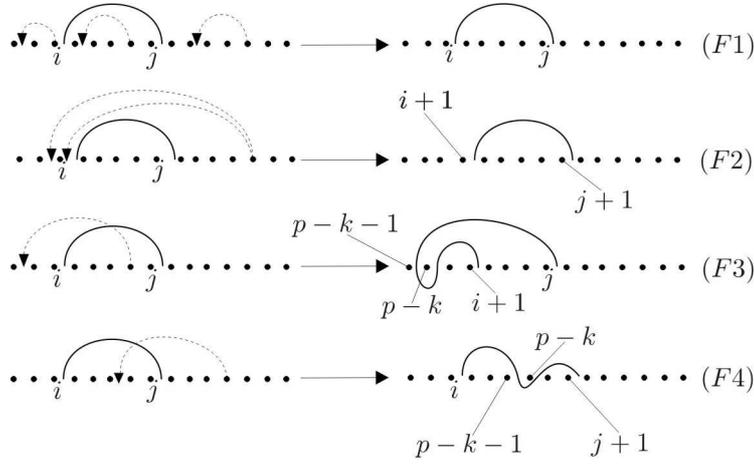


FIGURE 3. Comment l'action des tresses $\Sigma_{p,k}$ transforme-t-elle les arcs supérieurs? Les pointillés représentent la trace du mouvement du trou initialement numéroté p (jusqu'à la position $p-k$). Les traits pleins représentent l'arc $i \frown j$ à gauche et son image $(i \frown j)^{\Sigma_{p,k}}$ à droite.

Soit maintenant \widetilde{W} le mot obtenu en remplaçant chaque sous-mot de la forme $i \frown j$ dans W par le sous-mot $(i \frown j)^{\Sigma_{p,k}}$ correspondant. Cela transforme les arcs inférieurs $(i \smile j)$ seulement en translatant leurs extrémités.

Remarquons que \widetilde{W} n'est pas nécessairement un mot réduit, de sorte que $W([\mathcal{C}]^{\Sigma_{p,k}})$ et \widetilde{W} peuvent être différents. Le lemme suivant explique comment obtenir le mot réduit $W([\mathcal{C}]^{\Sigma_{p,k}})$ à partir du mot \widetilde{W} .

LEMME 4.3.1. *Soit $[\mathcal{C}]$ une classe d'isotopie de courbes et $W = W([\mathcal{C}])$. Soit $1 \leq k < p \leq n$. Soit \widetilde{W} comme précédemment et soit $W^{\Sigma_{p,k}}$ le mot obtenu à partir de \widetilde{W} en enlevant toutes les occurrences de sous-mots de la forme $p \smile p \frown$. Alors $W^{\Sigma_{p,k}} = W([\mathcal{C}]^{\Sigma_{p,k}})$, c'est à dire que $W^{\Sigma_{p,k}}$ est le mot réduit associé à $[\mathcal{C}]^{\Sigma_{p,k}}$.*

DÉMONSTRATION. Observons que les formules qui définissent $(i \frown j)^{\Sigma_{p,k}}$ ne contiennent aucun sous-mot de la forme $c \smile c$ ni $c \frown c$. La seule occurrence possible d'un tel sous-mot dans \widetilde{W} provient donc nécessairement de la transformation d'un arc inférieur. Or un arc inférieur $c \smile d$ ne peut être transformé qu'en un arc $k \smile l$, avec $k \in \{c, c+1\}$ et $l \in \{d, d+1\}$. Ainsi, cet arc $k \smile l$ borde un bigone avec l'axe horizontal si et seulement si $c+1 = d$, $k = c+1$ et $l = d$ (quitte à renverser le

mot on peut supposer que $c < d$). Dans ce cas, \widetilde{W} contient le sous-mot $d \smile d$. Selon les formules qui définissent $(i \frown j)^{\Sigma_{p,k}}$, cela a lieu si et seulement si $d = p$, c'est à dire $c \smile d = (p-1) \smile p$. En particulier, nous avons montré qu'aucun sous-mot de la forme $c \frown c$ ne peut apparaître dans \widetilde{W} .

Nous prouvons maintenant qu'en enlevant les sous-mots de la forme $p \smile p \frown$, nous obtenons à partir de \widetilde{W} un mot réduit; autrement dit tout sous-mot de la forme $p \smile p \frown$ dans \widetilde{W} est un sous-mot d'un sous-mot plus long de la forme $a \frown p \smile p \frown b$, avec $a \neq b$.

Soit $h \frown (p-1) \smile p \frown l$ un sous-mot de W . Comme \mathcal{C} est une courbe simple, les entiers h, l doivent se trouver dans l'un des 3 cas suivants (voir figure 4) :

- 1) $h < p-1 < p < l$,
- 2) $l \leq h < p-1 < p$,
- 3) $p-1 < p < l \leq h$.

Nous allons voir que dans chacun des 3 cas, le sous-mot $a \frown p \smile p \frown b$ de \widetilde{W} obtenu par l'action de $\Sigma_{p,k}$ satisfait

$$a \in \{p-k, \dots, p-1\}$$

et

$$b \in \{0, \dots, p-k-1\} \cup \{p+1, \dots, n\},$$

et donc $a \neq b$, comme nous voulions montrer.

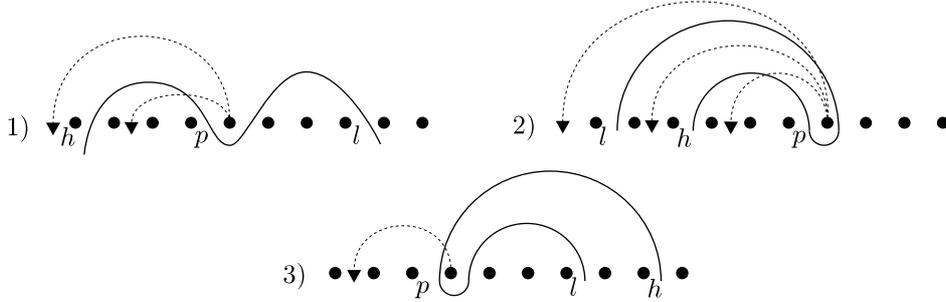


FIGURE 4. Les 3 cas possibles de sous-mots de $h \frown (p-1) \smile p \frown l$ qui apparaissent dans W , avec les différents mouvements possibles du trou p .

Dans les deux premiers cas, la transformation de l'arc $(h \frown p)$ induit les égalités $a = h+1$ ou $a = p-k$, et donc $a \in \{p-k, \dots, p-1\}$. Dans le troisième cas, nous obtenons aussi $a = p-k$. Par ailleurs, dans les premier et troisième cas, on a $b = l$ (donc $b > p$); dans le second cas, $b = l$ si $p-k \geq l+1$ ou $b = p-k-1$ sinon (et donc $b < p-k$).

Cela achève la preuve du lemme. □

A chaque classe d'isotopie de courbes $[\mathcal{C}]$ et chaque tresse $\Sigma_{p,k}$, on peut donc associer le mot $W([\mathcal{C}])^{\Sigma_{p,k}}$ défini grâce à la construction ci-dessus; ce mot vérifie l'identité

$$W([\mathcal{C}])^{\Sigma_{p,k}} = W([\mathcal{C}]^{\Sigma_{p,k}}).$$

Pour toute tresse positive x et toute courbe \mathcal{C} , on peut alors définir l'image W^x de $W = W([\mathcal{C}])$ sous l'action de x . En effet, si x est exprimée comme un produit de la forme $x = \prod_{m=1}^r \Sigma_{p_m, k_m}$, alors en vertu du lemme 4.3.1 la formule de récurrence

$$W^x = (W \prod_{m=1}^{r-1} \Sigma_{p_m, k_m})^{\Sigma_{p_r, k_r}}$$

définit un mot sur X qui est le mot réduit associé à $[\mathcal{C}]^x$. Ici et dans la suite, nous utiliserons la notation d'un produit malgré la non-commutativité; le produit est donc à considérer dans l'ordre croissant des indices. La définition donnée pour W^x ne dépend pas de la décomposition de x en fonction des tresses $\Sigma_{p,k}$. En d'autres termes, on a pour tout $x \in B_n^+$ et toute courbe \mathcal{C} , $W([\mathcal{C}]^x) = W([\mathcal{C}])^x$.

4.4. Preuve du théorème principal

Quitte à considérer le représentant réduit d'une classe d'isotopie d'une courbe donnée, on peut parler simplement de courbes au lieu de classes d'isotopie de courbes. Dans la suite nous notons \mathcal{C} le représentant réduit de la classe d'isotopie $[\mathcal{C}]$ et le mot réduit associé à $[\mathcal{C}]$ sera noté $W(\mathcal{C})$.

Pour commencer, nous rappelons que les tresses simples sont les tresses positives dans lesquelles chaque paire de brins se croise au plus une fois (paragraphe 2.2.1). Nous rappelons aussi (voir [19], preuve de la proposition 8) que toute tresse simple s peut se décomposer de manière unique comme un produit

$$s = \prod_{p=2}^n \Sigma_{p,k_p},$$

où $0 \leq k_p < p$ et $\Sigma_{p,0} = 1$. Cela nous permet de voir s comme une suite de mouvements des brins numérotés de 2 à n (dans cet ordre), chacun d'eux se déplaçant k_p positions vers la gauche (le nombre k_p dépend de s). Remarquons que le p -ième brin de s ne croise (dans s) aucun des brins initialement à gauche de la position $p - k_p$. Grâce à cette décomposition nous pouvons reformuler la définition de courbe presque-ronde (voir section 3.2) à l'aide des mots définis à la section 4.2. Nous observons d'abord qu'une courbe \mathcal{C} est ronde si et seulement si $W(\mathcal{C}) = i \frown j \smile$, pour $1 \leq i + 1 < j \leq n$ (modulo permutation cyclique des lettres et renversement); dans ce cas, \mathcal{C} est le cercle entourant les trous $i + 1, \dots, j$ (et on a choisi le point de base sur l'intervalle $]i, i + 1[$ et l'orientation horaire).

LEMME 4.4.1. *La complexité d'une courbe \mathcal{C} est inférieure ou égale à 1 si et seulement si le mot $W(\mathcal{C})$ (modulo permutation cyclique des lettres et renversement) peut être décomposé en deux parties : $W(\mathcal{C}) = w_1 w_2$, où tous les arcs dans w_1 sont orientés de gauche à droite tandis que tous les arcs dans w_2 sont orientés de droite à gauche. En particulier, si \mathcal{C} est une courbe presque-ronde, le mot réduit $W(\mathcal{C})$ (modulo permutation cyclique des lettres et renversement) contient un sous-mot de la forme $i \frown j \smile l$, avec $0 \leq i < j < l \leq n$.*

DÉMONSTRATION. Rappelons que les courbes de complexité au plus 1 sont les courbes rondes et les courbes presque-rondes (images des courbes rondes par l'action d'éléments simples). Soit \mathcal{C}_0 une courbe ronde et $W(\mathcal{C}_0) = i \frown j \smile$, avec $1 \leq i + 1 < j \leq n$. Observons que $W(\mathcal{C}_0) = (i \frown j) \smile = w_1 w_2$ satisfait les conditions attendues.

On peut étudier l'action d'un élément simple s sur ce mot, à l'aide des résultats de la section 4.3. Pour ce faire on décompose s en 3 parties (certaines éventuellement triviales) grâce à la remarque ci-dessus : le mouvement des brins à gauche de \mathcal{C}_0 , le mouvement des brins entourés par \mathcal{C}_0 et le mouvement des brins à droite de \mathcal{C}_0 . Le premier mouvement a un effet neutre sur $W(\mathcal{C}_0)$ (Formule (F1)). Le mouvement des brins numérotés $i + 1, \dots, j$ résulte (quitte à permuter cycliquement les lettres) en un nouveau mot de la forme $(h \frown j) w_2$, où

$$h = \min(i, \min\{l - k_l - 1, l \in \{i + 1, \dots, j\}\})$$

et w_2 est un mot dont tous les arcs sont orientés de droite à gauche (Formule (F3)). Enfin, on observe que le mouvement des brins situés à droite de \mathcal{C}_0 transforme l'arc $h \frown j$ en un mot (éventuellement plus long) dont tous les arcs sont orientés de gauche à droite (Formules (F4) et (F2)); de même l'image du mot w_2 après ce mouvement est un mot dont tous les arcs sont orientés de droite à gauche.

Réciproquement, soit \mathcal{C} une courbe telle que $W(\mathcal{C}) = w_1 w_2$, où w_1 (respectivement w_2) est un mot dont tous les arcs sont orientés de gauche à droite (respectivement de droite à gauche). La courbe \mathcal{C} a un unique minimum local (et un unique maximum local) dans la direction horizontale. Soit $*$ le point de \mathcal{C} correspondant à ce minimum local et soit i_0 l'entier tel que le point $*$ appartient à l'intervalle $]i_0, i_0 + 1[$. De la même façon, le point $*$ ' correspondant au maximum local de \mathcal{C} dans la direction horizontale appartient à un unique intervalle $]j_0, j_0 + 1[$. Choisissons l'orientation horaire pour \mathcal{C} , et remarquons que les arcs orientés de gauche à droite commençant au point $*$ forment

un sous-mot $w_1 = i_0 \frown i_1 \dots \frown j_0$ (qui termine par un arc supérieur, puisque \mathcal{C} est simple). Considérons la tresse s_h obtenue en déplaçant tous les trous (s'il y en a) qui se trouvent au-dessus de w_1 (autrement dit sur les diamètres des arcs \smile de w_1) jusqu'à la gauche de $*$. La tresse s_h est simple. Son action transforme $W(\mathcal{C})$ en $(i'_0 \frown j_0)w'_2$, avec $i'_0 \geq i_0$ et tous les arcs de w'_2 orientés de droite à gauche. La nouvelle courbe a toujours un maximum local dans la direction horizontale : $*$ ' dans l'intervalle $]j_0, j_0 + 1[$. De plus, tous les brins qui se trouvent à droite de la position i'_0 à la fin de ce mouvement ne se sont pas croisés. Considérons la tresse s_b obtenue en déplaçant tous les trous (s'il y en a) qui se trouvent au-dessous de w'_2 (autrement dit sur les diamètres des arcs \frown de w'_2) jusqu'à la droite de $*$ '. La tresse s_b est simple; de plus, le produit $s_h s_b$ est encore simple et la courbe $\mathcal{C}^{s_h s_b}$ est ronde.

Si \mathcal{C} est une courbe presque-ronde, alors dans la décomposition $W(\mathcal{C}) = w_1 w_2$ ci-dessus, au moins un des mots w_1, w_2 contient au moins deux arcs. Si w_1 contient au moins deux arcs, alors on peut écrire $w_1 = i_0 \frown i_1 \smile i_2 \dots \frown j_0$ et les valeurs $i = i_0, j = i_1$ et $l = i_2$ satisfont la dernière assertion du lemme. Si au contraire $i_1 = j_0$, alors w_2 contient au moins deux arcs et quitte à choisir l'orientation inverse pour \mathcal{C} , on peut réécrire $W(\mathcal{C}) = \tilde{w}_1 \tilde{w}_2$ avec $\tilde{w}_1 = i'_1 \smile i'_2 \frown i'_3 \dots \smile i'_k$ ($k \geq 4, i'_1 = i_0$ et $i'_k = j_0$, le dernier arc étant inférieur à cause de la simplicité de \mathcal{C}) et il suffit alors de prendre $i = i'_2, j = i'_3$ et $l = i'_4$ pour satisfaire les conditions du lemme. \square

Avant de prouver le théorème 3.3.1, nous introduisons la notion de *point d'inflexion*. On dit qu'un entier j (avec $0 < j < n$) est un point d'inflexion de la courbe \mathcal{C} (ou que la courbe \mathcal{C} admet le point d'inflexion j) si le mot réduit $W(\mathcal{C})$ admet (modulo permutation cyclique des lettres et renversement) un sous-mot de la forme $i \frown j \smile l$, où $0 \leq i < j < l \leq n$. La dernière assertion du lemme 4.4.1 affirme donc qu'une courbe presque-ronde admet au moins un point d'inflexion. Etant donné une tresse simple s , et un point d'inflexion j pour une courbe \mathcal{C} , on dit que j est *compatible* avec s si les brins numérotés j et $j + 1$ ne se croisent pas dans s .

Le lemme suivant est l'étape essentielle dans la preuve du théorème 3.3.1 :

LEMME 4.4.2. *Soient s_1, s_2 des tresses simples telles que la paire (s_1, s_2) est pondérée. Soit \mathcal{C} une courbe admettant un point d'inflexion j compatible avec s_1 . Alors la courbe \mathcal{C}^{s_1} admet un point d'inflexion j' ; de plus ce point d'inflexion est compatible avec s_2 .*

DÉMONSTRATION. Comme la paire (s_1, s_2) est pondérée, il suffit de montrer que \mathcal{C}^{s_1} admet un point d'inflexion j' tel que les brins numérotés j' et $j' + 1$ à la fin de s_1 ne se croisent pas dans s_1 (corollaire 2.2.3).

Soit

$$s_1 = \left(\prod_{p=2}^{j-1} \Sigma_{p, k_p} \right) \cdot \Sigma_{j, k_j} \cdot \Sigma_{j+1, k_{j+1}} \cdot \left(\prod_{p=j+2}^n \Sigma_{p, k_p} \right)$$

la décomposition de s_1 en termes des tresses $\Sigma_{p, k}$. Nous étudions l'action de s_1 sur \mathcal{C} à travers cette factorisation; à chaque étape, i.e. après l'action de chaque facteur dans le produit ci-dessus, la courbe obtenue admet un point d'inflexion h tel que les brins en position h et $h + 1$ à la fin de cette étape ne se sont pas encore croisés dans s_1 .

Le premier facteur $\prod_{p=2}^{j-1} \Sigma_{p, k_p}$ correspond à un mouvement de trous situés à gauche de la position j . A cause des Formules (F1) et (F3) et de la preuve du lemme 4.3.1, j est toujours un point d'inflexion pour la courbe qui résulte de cette action. De plus, les brins qui terminent dans les positions j et $j + 1$ ne se sont pas croisés dans ce premier facteur.

Le facteur Σ_{j, k_j} déplace le j -ième trou vers la gauche; encore en vertu des Formules (F1) et (F3) et de la preuve du lemme 4.3.1, le mot réduit obtenu contient un sous-mot $i' \frown j \smile$ (avec $i' < j$); j est encore un point d'inflexion pour la courbe correspondante. Remarquons que le trou numéroté antérieurement j est maintenant (en position $j - k_j$) en dessous de l'arc $i' \frown j$ et que les brins qui terminent dans les positions j et $j + 1$ ne se sont pas croisés.

Ensuite, le facteur $\Sigma_{j+1, k_{j+1}}$ meut le trou numéroté $j + 1$ vers la gauche. Comme j était un point d'inflexion de \mathcal{C} , compatible avec s_1 , les brins numérotés j et $j + 1$ ne se croisent pas dans s_1 . Ainsi, le mouvement du $(j + 1)$ -ième trou ne peut se terminer au-delà de la position $j - k_j$: le $(j + 1)$ -ième trou est envoyé sur le diamètre de l'arc supérieur $i' \frown j$ et en vertu de la Formule (F4) et de la preuve du lemme 4.3.1, l'entier $h_{j+1} := j - k_{j+1}$ est un point d'inflexion pour la courbe obtenue (voir figure 5). De plus, par construction les brins qui terminent dans les positions h_{j+1} et $h_{j+1} + 1$ ne se sont pas croisés dans s_1 .

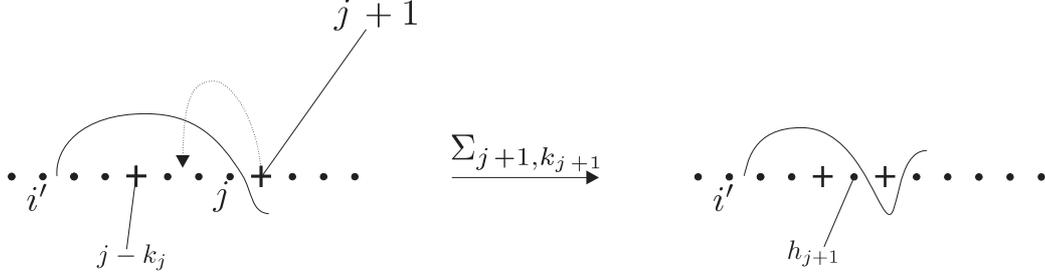


FIGURE 5. L'action de la tresse $\Sigma_{j+1, k_{j+1}}$; les brins représentés par des croix ne pouvant pas se croiser, le trou $j + 1$ est bloqué dans son mouvement vers la gauche avant la position $j - k_j$.

Finalement, on observe que pour $j + 2 \leq q \leq n$, la courbe résultant du mouvement du trou numéroté q admet toujours un point d'inflexion : il s'agit de $h_q = h_{q-1} + 1$ si le mouvement termine à gauche de h_{q-1} , et de $h_q = h_{q-1}$ sinon. Par conséquent, $j' := h_n$ est un point d'inflexion de \mathcal{C}^{s_1} et les brins en position j' et $j' + 1$ à la fin de s_1 ne se sont pas croisés dans s_1 , par construction. Cela montre que le point d'inflexion j' de \mathcal{C}^{s_1} est compatible avec s_2 . \square

Nous pouvons maintenant achever la preuve du théorème 3.3.1.

Rappelons la tresse $x = \Delta^p x_1 \dots x_r$ en forme normale, qui envoie la courbe ronde \mathcal{C} sur une courbe ronde $\mathcal{C}' = \mathcal{C}^x$. Puisque la tresse Δ correspond à une rotation dans \mathbb{D}_n , la courbe \mathcal{C}^{Δ^t} est ronde pour tout entier t et on peut supposer, quitte à multiplier par Δ^{-p} , que la forme normale de x est $x_1 \dots x_r$. Pour prouver le théorème 3.3.1, il suffit de prouver que la courbe \mathcal{C}^{x_1} est ronde, puisqu'une fois ce fait acquis, on dispose d'une tresse $x_2 \dots x_r$ en forme normale, dont l'action transforme la courbe ronde \mathcal{C}^{x_1} en la courbe ronde \mathcal{C}' . Le résultat alors s'ensuit par induction sur le nombre de facteurs dans la forme normale de x .

Nous donnons une preuve par l'absurde, en supposant que la courbe \mathcal{C}^{x_1} n'est pas ronde. Cependant elle est presque-ronde puisque x_1 est une tresse simple. Selon le lemme 4.4.1, \mathcal{C}^{x_1} admet un point d'inflexion j_1 . Remarquons que les trous qui se trouvent au-dessus de la courbe \mathcal{C}^{x_1} étaient à droite de \mathcal{C} au début de x_1 tandis que les trous qui se trouvent en dessous de \mathcal{C}^{x_1} étaient à gauche de \mathcal{C} . En vertu du lemme 4.4.1, soit le trou j_1 se trouve en dessous de la courbe \mathcal{C}^{x_1} , soit il est entouré par \mathcal{C}^{x_1} . De même, ou bien le trou $j_1 + 1$ se trouve au-dessus de la courbe, ou bien il est entouré par elle. En outre, au plus l'un des trous j_1 et $j_1 + 1$ est entouré par la courbe \mathcal{C}^{x_1} . Cela implique que les brins numérotés j_1 et $j_1 + 1$ à la fin de x_1 ne se croisent pas dans x_1 . En d'autres termes, j_1 est un point d'inflexion de \mathcal{C}^{x_1} compatible avec x_2 (comme la paire (x_1, x_2) est pondérée).

Maintenant, par récurrence sur $m = 1, \dots, r - 1$ et en vertu du lemme 4.4.2, il existe des entiers j_2, \dots, j_{r-1} tels que j_m est un point d'inflexion pour la courbe $\mathcal{C}^{x_1 \dots x_m}$ compatible avec x_{m+1} , pour tout $m = 1, \dots, r - 1$. Le lemme 4.4.2 montre aussi que $\mathcal{C}^{x_1 \dots x_r}$ a un point d'inflexion j_r .

En particulier nous avons montré que la courbe $\mathcal{C}^{x_1 \dots x_r} = \mathcal{C}^x$ n'est pas ronde, dès lors que \mathcal{C}^{x_1} ne l'est pas. C'est une contradiction ; par conséquent \mathcal{C}^{x_1} est ronde et le théorème 3.3.1 est démontré.

Le problème de réductibilité : courbes standard et la structure duale

Le résultat principal est le théorème 5.1.3, généralisation au cadre dual du théorème 3.3.1. La structure de Garside duale de B_n est la seule utilisée ici et par conséquent, des concepts tels que forme normale, Super Summit Set, etc. se réfèrent toujours à cette structure. Nous continuons à nommer simplement “courbe” une courbe fermée simple non dégénérée dans le disque \mathbb{D}_n . Dans un premier temps, la notion convenable de “rondeur” est définie (notion de *courbe standard*) et nous énonçons le théorème principal, avec une ébauche de la démonstration (section 5.1). Le plan du chapitre reproduit celui du chapitre 4 : les courbes sont décrites à l’aide de mots (section 5.2), lesquels servent à étudier l’action des tresses positives sur les courbes (section 5.3). Enfin, le théorème 5.1.3 est prouvé dans la section 5.4. Dans la section 5.5, nous décrivons un algorithme pour décider si une tresse donnée préserve la classe d’isotopie d’une courbe standard.

5.1. Enoncé du théorème principal, esquisse de la démonstration

En vue de la généralisation du théorème 3.3.1, il nous faut identifier la notion convenable de “rondeur” dans le cadre dual. De fait, la notion de courbe entourant un ensemble de trous consécutifs n’est pas la bonne, comme le montre l’exemple suivant :

EXEMPLE 5.1.1. Soit $n = 4$. Considérons la tresse $x = a_{1,2}.a_{1,4}$, qui est en forme normale telle qu’écrite. La figure 1 montre une classe d’isotopie “ronde” (entourant un ensemble de trous consécutifs) transformée par x en une classe d’isotopie “ronde” et dont l’image par le premier facteur de la forme normale de x n’a pas la même propriété.

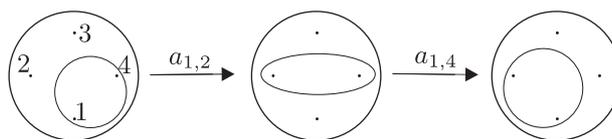


FIGURE 1. La courbe dans la partie centrale n’est pas isotope à une courbe entourant un ensemble de trous consécutifs, bien que sa classe d’isotopie est l’image par le premier facteur de la forme normale de x d’une classe d’isotopie de courbes “ronde” qui est transformée par x en une classe d’isotopie de courbes “ronde”.

Cela nous conduit à définir (voir aussi définition 5.4.1) :

DÉFINITION 5.1.2. *Une courbe dans \mathbb{D}_n est dite standard si elle est isotope à une courbe qui peut être décrite en coordonnées polaires par une fonction $\rho = \rho(\theta)$, pour $\theta \in [0, 2\pi[$. Voir figure 2(a). Une classe d’isotopie de courbes est dite standard si un de ses représentants (ou de manière équivalente si tout représentant) est standard.*

On remarque que les courbes standard correspondent aux sous-groupes paraboliques standard de la structure de Garside duale, de la même façon que les courbes rondes correspondent aux sous-groupes paraboliques standard, pour la structure classique [35].

Munis de cette définition, nous pouvons énoncer :

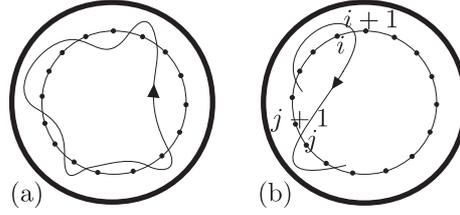


FIGURE 2. (a) Une courbe standard comme dans la définition 5.1.2. (b) Une partie d'une courbe non standard.

THÉORÈME 5.1.3. *Soit \mathcal{C} une courbe standard dans \mathbb{D}_n . Soit x une tresse dont la forme normale est $\delta^p x_1 \cdots x_r$. Si $[\mathcal{C}]^x$ est standard, alors $[\mathcal{C}]^{\delta^p x_1 \cdots x_m}$ est standard pour tout $m = 1, \dots, r$.*

La preuve du théorème 5.1.3 est calquée sur celle du théorème 3.3.1. Rappelons la paramétrisation de \mathbb{D}_n décrite aux section 1.2 et paragraphe 2.2.2. Pour fixer les idées on peut supposer que \mathbb{D} est le disque unité fermé dans \mathbb{C} , $\Gamma = \{z \in \mathbb{C}, |z| = \frac{1}{2}\}$ et pour tout $i = 1, \dots, n$, p_i est le point de Γ d'argument $-\frac{2i\pi}{n}$. On note i pour p_i ($i = 1, \dots, n$) et la tresse $a_{i,j}$ ($1 \leq i < j \leq n$) pourra être notée aussi $a_{j,i}$ indifféremment. Enfin, on note (i, j) l'arc de Γ décrit par le mouvement dans le sens horaire du trou i jusqu'à la position j ; lorsque $i = j$, on a $(i, i) = \{i\}$. On notera aussi $k \in (i, j)$ pour dire que le point k se trouve sur l'arc (i, j) de Γ .

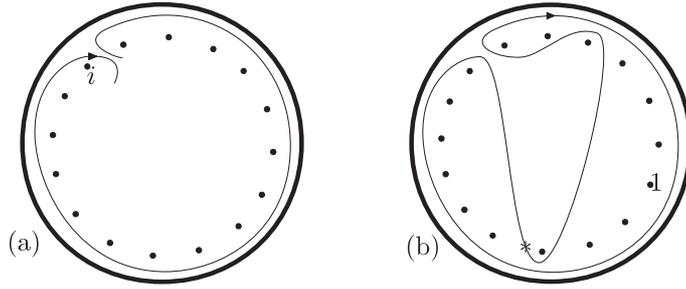
Soient \mathcal{C} et x comme dans l'énoncé. Une induction élémentaire montre qu'il est suffisant de prouver que $[\mathcal{C}]^{\delta^p x_1}$ est standard. Nous allons voir que si $[\mathcal{C}]^{\delta^p x_1}$ n'est pas standard, alors une partie (d'un représentant convenable) de $[\mathcal{C}]^{\delta^p x_1}$ intersecte le cercle Γ comme le montre la figure 2(b), pour certains entiers $1 \leq i \neq j \leq n$. De plus, la tresse $x_1 a_{i,j}$ est simple. Nous prouvons alors par récurrence que si $x_1 \cdots x_r$ est en forme normale, alors les propriétés que nous venons d'évoquer doivent être vraies pour $[\mathcal{C}]^{\delta^p x_1 \cdots x_m}$, pour tout $m = 1, \dots, r$. En d'autres termes, une partie (d'un représentant convenable) de $[\mathcal{C}]^{\delta^p x_1 \cdots x_m}$ intersecte le cercle Γ comme le montre la figure 2(b), pour certains entiers $1 \leq i_m \neq j_m \leq n$; de plus, $x_m a_{i_m, j_m}$ est simple. En particulier, cela implique que $[\mathcal{C}]^{\delta^p x_1 \cdots x_r}$ n'est pas standard; c'est la contradiction qui démontre le théorème 5.1.3.

5.2. Des mots pour décrire les courbes de \mathbb{D}_n

Soit \mathcal{C} une courbe dans \mathbb{D}_n . Supposons que \mathcal{C} a un nombre fini d'intersections avec Γ , toutes transverses. Nous allons associer à \mathcal{C} un mot $W(\mathcal{C})$ que nous définissons maintenant. Choisissons un point $*$ de \mathcal{C} qui est sur le cercle Γ (c'est possible puisque \mathcal{C} est non-dégénérée). Choisissons aussi une orientation pour \mathcal{C} . En parcourant \mathcal{C} selon l'orientation choisie, avec point de départ et d'arrivée $*$, nous construisons un mot sur l'alphabet $Y = \{\smile, \frown, \curvearrowright, \curvearrowleft, \circlearrowright, \circlearrowleft, 1, \dots, n\}$ de la manière suivante.

Chaque arc qui traverse la composante intérieure de $\mathbb{D}_n - \Gamma$ contribue une lettre \smile au mot. Chaque intersection de \mathcal{C} avec l'arc $(i, i+1)$ contribue la lettre i . Finalement, les arcs de \mathcal{C} qui traversent la composante extérieure de $\mathbb{D}_n - \Gamma$ contribuent une lettre \curvearrowright (respectivement \curvearrowleft) s'ils sont orientés dans le sens horaire (respectivement, anti-horaire), sauf ceux qui ont leurs deux extrémités sur le même arc $(i, i+1)$ de Γ et ne bordent pas un bigone avec Γ , comme sur la figure 3 (a). Ces derniers contribuent une lettre \circlearrowright ou \circlearrowleft , de manière naturelle selon leur orientation.

Le numéro correspondant au point $*$ peut être placé au début ou à la fin du mot. Nous appelons *mot associé à \mathcal{C}* le mot sur Y obtenu par ce procédé et nous le notons $W(\mathcal{C})$. Le choix d'un autre point de base $*$ ou le changement de place de la lettre associée à $*$ (au début ou à la fin) déterminent une permutation cyclique des lettres de $W(\mathcal{C})$. De plus, en choisissant l'orientation inverse pour \mathcal{C} , on obtient le renversement du mot $W(\mathcal{C})$, échangeant en outre les lettres \curvearrowright et \curvearrowleft (respectivement, \circlearrowright et \circlearrowleft). Ainsi, le mot associé à une courbe est défini modulo permutation cyclique de ses lettres et modulo renversement échangeant l'orientation des arcs extérieurs.

FIGURE 3. (a) Un arc $i \circ i$. (b) La courbe de l'Exemple 5.2.1

EXEMPLE 5.2.1. Soit \mathcal{C} la courbe de la figure 3 (b); ici $n = 16$. Le point $*$ et l'orientation sont aussi indiqués sur la figure. Le mot associé à cette courbe est

$$W(\mathcal{C}) = 4 \curvearrowright 3 \smile 13 \curvearrowleft 12 \smile 10 \circ 10 \smile .$$

Remarquons que si \mathcal{C} et \mathcal{C}' sont deux courbes isotopes via une isotopie de \mathbb{D}_n qui préserve globalement le cercle Γ , alors $W(\mathcal{C}) = W(\mathcal{C}')$. On dit que le mot associé à \mathcal{C} est *réduit* s'il ne contient aucun sous-mot de la forme $i \smile i$, $i \curvearrowright i$ ou $i \curvearrowleft i$. On dit qu'une courbe \mathcal{C} est *réduite* si le mot $W(\mathcal{C})$ est réduit. On remarque que les courbes réduites sont exactement celles qui ne bordent aucun bigone avec le cercle Γ . Selon [28], toute courbe \mathcal{C} est isotope à une courbe réduite \mathcal{C}^{red} , qui est unique modulo isotopie de \mathbb{D}_n préservant globalement le cercle Γ . Nous pouvons finalement définir, pour chaque classe d'isotopie de courbes $[\mathcal{C}]$ dans \mathbb{D}_n , le *mot réduit associé* à $[\mathcal{C}]$: $W([\mathcal{C}]) = W(\mathcal{C}^{red})$.

5.3. L'action des tresses duales positives

Au lieu du système générateur de BKL_n^+ que constitue l'ensemble des tresses $a_{i,j}$ ($1 \leq i < j \leq n$), nous allons travailler avec un système générateur plus gros, à savoir l'ensemble des polygones décrits au paragraphe 2.2.2 :

$$\mathcal{P} = \left\{ a_{i_1, i_2} a_{i_2, i_3} \cdots a_{i_{r-2}, i_{r-1}} a_{i_{r-1}, i_r}, \left. \begin{array}{l} 2 \leq r \leq n, \\ i_1, \dots, i_r \text{ tous distincts et placés dans cet ordre,} \\ \text{suivant le cercle } \Gamma \text{ dans le sens horaire de } i_1 \text{ vers } i_r \end{array} \right\}.$$

Considérons maintenant la classe d'isotopie d'une courbe \mathcal{C} ainsi que le mot réduit $W = W([\mathcal{C}])$ qui lui est associé. Etant donnée une tresse duale positive x , nous voulons décrire les transformations à effectuer sur le mot W afin d'obtenir le mot $W([\mathcal{C}]^x)$. A cet effet, nous étudions d'abord le cas $x = P \in \mathcal{P}$. On suppose que l'action de P modifie principalement les arcs intérieurs tandis que les arcs extérieurs sont transformés seulement par translation de leurs extrémités le long du cercle Γ .

Observons d'abord que chaque arc intérieur partitionne l'ensemble des trous en deux sous-ensembles : l'un contient les trous situés sur l'arc $(i+1, j)$ et l'autre les trous qui se trouvent sur l'arc $(j+1, i)$. On dit que P est *disjoint* de l'arc $i \smile j$ si tous les sommets de P appartiennent à un seul de ces ensembles. Si c'est le cas nous posons $(i \smile j)^P = i \smile j$. Dans le cas contraire, on dit que P est *transverse* à l'arc $i \smile j$. Dans ce cas, soit $p_{i,j}$ le dernier sommet de P rencontré en parcourant l'arc $(j+1, i)$ dans le sens horaire; de même soit $q_{i,j}$ le dernier sommet de P rencontré en parcourant l'arc $(i+1, j)$ dans le sens horaire. Par abus de notation, nous écrirons $i \in P$ lorsque i est un sommet de P . Observons que $p_{i,j} = i \Leftrightarrow i \in P$ et $q_{i,j} = j \Leftrightarrow j \in P$. Voir figure 4.

On définit, a priori, en s'inspirant d'un dessin :

$$(i \smile j)^P = i \smile p_{i,j} \curvearrowleft (p_{i,j} - 1) \smile (q_{i,j} - 1) \curvearrowright q_{i,j} \smile j. \quad (F')$$

La Formule (F') est représentée sur la figure 4.

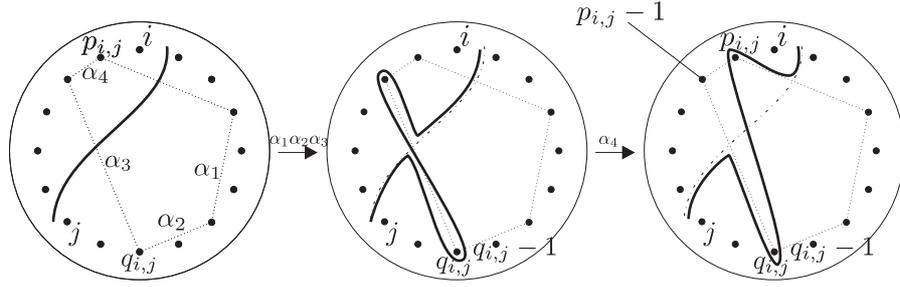


FIGURE 4. Dans cet exemple P (en traits pointillés) s'exprime comme le produit d'atomes $\alpha_1 \dots \alpha_4$; $\alpha_1 \alpha_2$ agit trivialement sur l'arc $i \smile j$, l'action de α_3 sur $i \smile j$ produit l'arc de la partie centrale, et l'action de α_4 sur ce dernier produit l'arc de la partie de droite, qui est $(i \smile j)^P$, l'image de l'arc $(i \smile j)$ sous l'action de P (voir Formule (F')).

Cependant, on remarque que l'application de la Formule (F') produit des bigones bordés par l'arc $(i \smile j)^P$ et le cercle Γ , dès lors que $i \in P$ ou $j \in P$. Pour cette raison, nous définissons :

$$(i \smile j)^P = \begin{cases} i \smile p_{i,j} \frown (p_{i,j} - 1) \smile (q_{i,j} - 1) \curvearrowright q_{i,j} \smile j & \text{si } i \notin P \text{ et } j \notin P \quad (F'0) \\ i \smile p_{i,j} \frown (p_{i,j} - 1) \smile (j - 1) & \text{si } i \notin P \text{ et } j \in P \quad (F'1) \\ (i - 1) \smile (q_{i,j} - 1) \curvearrowright q_{i,j} \smile j & \text{si } i \in P \text{ et } j \notin P \quad (F'2) \\ (i - 1) \smile (j - 1) & \text{si } i \in P \text{ et } j \in P \quad (F'3) \end{cases}$$

La Remarque suivante est aussi représentée sur le figure 4 :

REMARQUE 5.3.1. L'image d'un arc intérieur $i \smile j$ sous l'action d'un polygone P se trouve (modulo déformation) dans un voisinage tubulaire de la réunion de $i \smile j$ et de P .

Remplaçons maintenant chaque sous-mot $(i \smile j)$ de W par le sous-mot correspondant $(i \smile j)^P$ défini ci-dessus. Cela transforme les arcs extérieurs de W en décalant leurs extrémités le long du cercle Γ . De plus, chaque lettre \curvearrowright (respectivement \frown) de W doit être transformée en \smile (respectivement \smile) si elle provient d'un arc $(c+1) \curvearrowright c$ de W dont l'extrémité $c+1$ est décalée à la position c (respectivement si elle provient d'un arc $(c-1) \frown c$ de W dont l'extrémité c est décalée à la position $c-1$). Voir figure 5 (a). De manière similaire, chaque lettre \smile (respectivement \smile) doit être changée en \curvearrowright (respectivement \frown) si les extrémités de l'arc concerné correspondent à des lettres différentes après la translation convenable.

Soit \widetilde{W} le mot sur Y obtenu de cette façon. Remarquons que \widetilde{W} n'est pas nécessairement réduit, de sorte que $W([\mathcal{C}]^P)$ n'est pas nécessairement le même mot que \widetilde{W} . Le lemme suivant est l'analogie du lemme 4.3.1 dans le cadre dual :

LEMME 5.3.2. Soit $[\mathcal{C}]$ une classe d'isotopie de courbes, et $W = W([\mathcal{C}])$. Soit $P \in \mathcal{P}$ un polygone. Soit \widetilde{W} comme ci-dessus, et soit W^P le mot obtenu à partir de \widetilde{W} en enlevant toutes les occurrences de sous-mots de la forme $(p-1) \curvearrowright (p-1) \smile$ (ou $(p-1) \frown (p-1) \smile$) où p est un sommet de P et $p-1$ n'en est pas un. Alors $W^P = W([\mathcal{C}]^P)$.

DÉMONSTRATION. Observons que les formules définissant $(i \smile j)^P$ ne contiennent aucun sous-mot de la forme $c \smile c$ ni $c \frown c$ (\frown désigne \curvearrowright ou \frown). La présence d'un tel sous-mot dans \widetilde{W} provient donc de la transformation d'un arc extérieur de W . Selon les formules ci-dessus, les transformations possibles pour un arc extérieur $c \frown d$ de W consistent à translater les extrémités c et d vers les positions respectives k et l , avec $k \in \{c, c-1\}$ et $l \in \{d, d-1\}$. Remarquons d'abord que les transformations d'arcs extérieurs de la forme $c \smile c$ ou $c \smile c$ ne peuvent pas créer de sous-mots de la forme $c \frown c$. Maintenant, un arc $c \frown d$ de W (et donc satisfaisant $c \neq d$) se transforme en un arc bordant un bigone avec le cercle Γ seulement si les entiers k et l ci-dessus sont égaux et

$|c - d| = 1$. Modulo renversement, il existe deux configurations, représentées par la figure 5, dans lesquelles les conditions $|c - d| = 1$ et $k = l$ sont satisfaites.

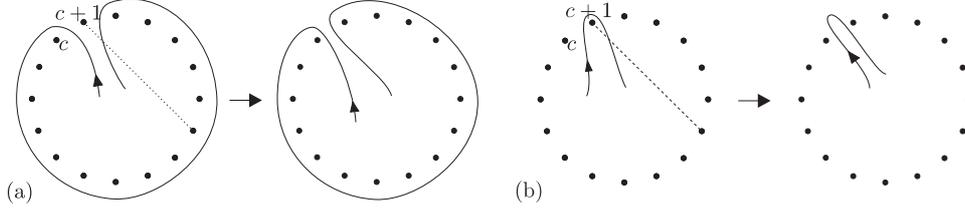


FIGURE 5. Transformation d'un arc extérieur $c \frown d$ de W , avec $|c-d| = 1$, vers un arc extérieur $k \frown l$ de \widetilde{W} avec $k = l$ (une arête de P est représentée en pointillés). (a) La transformation $c \frown (c+1) \rightsquigarrow c \frown c$ mentionnée précédemment : aucun bigone n'est formé. (b) Modulo renversement, la seule façon d'obtenir un bigone : $c \frown (c+1) \rightsquigarrow c \frown c$.

Finalement, en vertu des formules définissant $(i \smile j)^P$, pour que l'une des situations représentées sur la figure 5 ait lieu, il est nécessaire que $c+1$ soit un sommet de P et que c n'en soit pas un. Cela démontre en particulier qu'aucun sous-mot de la forme $c \smile c$ n'apparaît dans \widetilde{W} , et que les seuls sous-mots de \widetilde{W} de la forme $c \frown c$ possibles sont $(p-1) \frown (p-1)$, où p est un sommet de P tandis que $p-1$ n'en est pas un (figure 5 (b)).

Nous affirmons maintenant que l'élimination de toutes les occurrences de tels sous-mots est suffisante pour faire de \widetilde{W} un mot réduit ; autrement dit, tout sous-mot de la forme $(p-1) \frown (p-1)$ dans \widetilde{W} est un sous-mot d'un sous-mot plus long de \widetilde{W} de la forme

$$a \smile (p-1) \frown (p-1) \smile b,$$

avec $a \neq b$. Soit $r \smile (p-1) \frown p \smile v$ un sous-mot de W dont l'image par l'action de P est le mot ci-dessus (en particulier, P est transverse à l'arc $p \smile v$). Voir figure 6.

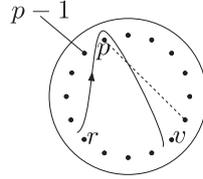


FIGURE 6. L'arc $r \smile (p-1) \frown p \smile v$ et une arête de P en pointillés.

Puisque $p-1$ n'est pas un sommet de P et p en est un, les Formules (F') donnent :

$$(r \smile (p-1))^P = \begin{cases} r \smile (p-1) & \text{si } P \text{ disjoint de } r \smile (p-1), \\ \dots (q_{r,p-1} - 1) \frown q_{r,p-1} \smile (p-1) & \text{sinon,} \end{cases}$$

et

$$(p \smile v)^P = \begin{cases} (p-1) \smile (q_{p,v} - 1) & \text{si } v \in P, \\ (p-1) \smile (q_{p,v} - 1) \frown q_{p,v} \smile v & \text{si } v \notin P. \end{cases}$$

Par conséquent, il nous reste à prouver que les entiers $a \in \{r, q_{r,p-1}\}$ et $b = q_{p,v} - 1$ sont distincts. On remarque que par définition, $q_{p,v}$ se trouve sur l'arc $(p+1, v)$ de sorte que $b = q_{p,v} - 1$ se trouve sur l'arc $(p, v-1)$. Par ailleurs, comme la courbe C^{red} est simple et W est le mot réduit associé à \mathcal{C} , $r \in (v, p-2)$ (voir figure 6). Finalement, par définition, $q_{r,p-1}$ est sur l'arc $(r+1, p-1) \subset (v+1, p-1)$. Ainsi, quelle que soit la valeur de $a \in \{r, q_{r,p-1}\}$, $a \in (v, p-1)$; cela montre que $a \neq b$ et termine la preuve du lemme 5.3.2. \square

On peut donc associer à chaque classe d'isotopie de courbes $[\mathcal{C}]$ et chaque tresse $P \in \mathcal{P}$ le mot $W([\mathcal{C}])^P$ construit par le procédé ci-dessus. Nous sommes maintenant capables de définir l'image W^x du mot $W = W([\mathcal{C}])$, pour toute classe d'isotopie de courbes $[\mathcal{C}]$ et toute tresse positive x . En effet, si x est exprimé comme un produit $x = \prod_{m=1}^r P_m$ (où chaque facteur est un polygone), alors en vertu du lemme 5.3.2, la formule de récurrence

$$W^x = (W^{\prod_{m=1}^{r-1} P_m})^{P_r}$$

définit un mot sur Y qui est le mot réduit associé à $[\mathcal{C}]^x$. Ainsi, cela ne dépend pas de la décomposition de x en fonction des polygones). En d'autres termes, pour tout $x \in BKL_n^+$ et toute courbe \mathcal{C} , on a $W([\mathcal{C}]^x) = W([\mathcal{C}])^x$.

5.4. Preuve du théorème principal

Dans cette section, nous parlons de “courbes” au lieu de classes d'isotopies de courbes ; “la courbe” signifie en fait “le représentant réduit de la classe d'isotopie de la courbe” et nous notons \mathcal{C} le représentant réduit de $[\mathcal{C}]$, de même que $W(\mathcal{C})$ le mot réduit correspondant. Nous commençons par reformuler la définition 5.1.2 :

DÉFINITION 5.4.1. *On appelle standard une courbe \mathcal{C} si $W(\mathcal{C})$ s'écrit seulement avec des lettres dans $\{1, \dots, n, \curvearrowright, \curvearrowleft\}$ (ou dans $\{1, \dots, n, \curvearrowright, \curvearrowleft\}$, modulo renversement).*

Rappelons que toute tresse simple s'exprime de manière unique comme un produit de polygones disjoints (paragraphe 2.2.2). La Remarque 5.3.1 nous dit alors que si $s = P_1 \dots P_g$ est la décomposition en polygones disjoints d'un élément simple s et \mathcal{C} une courbe, les arcs intérieurs de la forme $(i-1) \curvearrowright (j-1)$ avec $i, j \in P_l$ résultant de l'application des Formules (F') à un arc intérieur de \mathcal{C} et pour un polygone P_l ($l = 1, \dots, g$) sont invariants sous l'action de P_k , $k = 1, \dots, g$, $k \neq l$. Voir figure 7.

Nous introduisons maintenant la notion de *virage* d'une courbe (analogue à celle de point d'inflexion dans le cadre classique). On dit qu'une paire non-ordonnée i, j ($1 \leq i \neq j \leq n$) est un virage pour une courbe \mathcal{C} de \mathbb{D}_n si le mot réduit $W(\mathcal{C})$ contient un sous-mot de la forme $\curvearrowright i \curvearrowleft j \curvearrowright$, ou $\curvearrowright i \curvearrowleft j \curvearrowleft$ (modulo renversement). De plus, on dit qu'un virage i, j pour une courbe \mathcal{C} est *compatible* avec un élément simple s si $a_{i,j}$ n'est pas un préfixe de s .

Nous énonçons maintenant le lemme fondamental en vue du théorème 5.1.3; c'est l'analogue du lemme 4.4.2 pour le cadre dual :

LEMME 5.4.2. *Soient s_1, s_2 deux tresses simples telles que la paire (s_1, s_2) est pondérée. Soit \mathcal{C} une courbe et i, j un virage de cette courbe, qui est compatible avec s_1 . Alors il existe un virage i', j' pour \mathcal{C}^{s_1} ; de plus, ce virage est compatible avec s_2 .*

DÉMONSTRATION. Considérons la décomposition $s_1 = P_1 \dots P_g$ de s_1 , où les P_i sont des éléments 2 à 2 disjoints de \mathcal{P} . Comme la paire (s_1, s_2) est pondérée, $a_{i',j'}$ n'est pas un préfixe de s_2 dès lors que $s_1 a_{i',j'}$ est simple; il est donc suffisant de chercher un virage i', j' de \mathcal{C}^{s_1} tel que $s_1 a_{i',j'}$ est simple.

Par hypothèse, $a_{i,j}$ n'est pas un préfixe de s . Ainsi, i et j ne peuvent être simultanément sommets du même polygone parmi P_1, \dots, P_g (lemme 2.2.5). Si l'un de ces polygones est disjoint de l'arc $i \curvearrowleft j$ de $W(\mathcal{C})$, alors son action crée une courbe qui a toujours i, j pour virage (voir la preuve du lemme 5.3.2). De plus, toujours en vertu du lemme 2.2.5, si P est un tel polygone, alors $Pa_{i,j}$ est simple.

Nous étudions l'action des polygones parmi P_1, \dots, P_g qui sont transverses à l'arc $i \curvearrowleft j$ de la manière suivante (voir figure 7). Les polygones mis en jeu sont naturellement ordonnés en parcourant l'arc $i \curvearrowleft j$ à partir de l'arc $(i, i+1)$ de $\Gamma : Q_1, \dots, Q_h$.

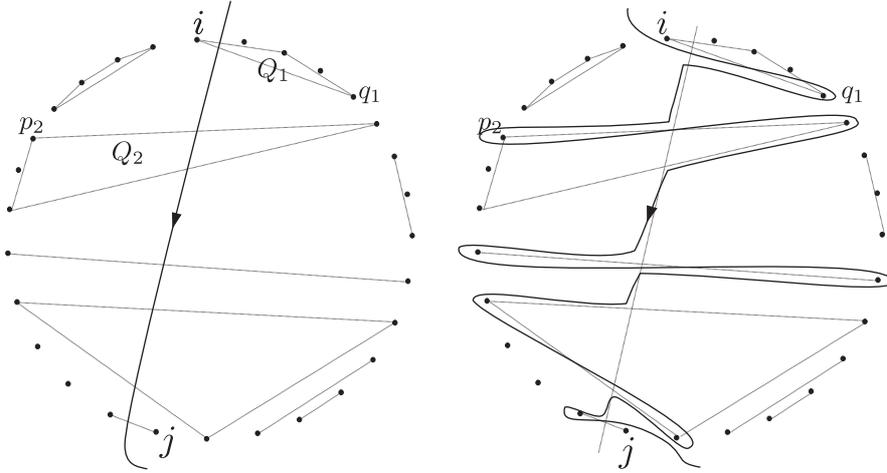


FIGURE 7. La tresse s_1 , comme produit de polygones deux à deux disjoints, est représentée en pointillés. De gauche à droite, on peut voir son action sur l'arc $i \sim j$.

Pour $t = 1, \dots, h$, si p_t est le sommet de Q_t le plus à droite le long de l'arc $(j+1, i)$ et q_t est le sommet de Q_t le plus à droite le long de l'arc $(i+1, j)$, alors en vertu des Formules (F') et de la preuve du lemme 5.3.2, la paire

$$i', j' = \begin{cases} q_1, p_2 & \text{si } h > 1 \\ i, p_1 & \text{si } h = 1 \text{ et } i \text{ n'est pas un sommet de } Q_1 \\ q_1, j & \text{si } h = 1 \text{ et } j \text{ n'est pas un sommet de } Q_1 \end{cases}$$

est un virage pour la courbe \mathcal{C}^{s_1} . De plus, en vertu du lemme 2.2.5, dans tous les cas la tresse $s_1 a_{i', j'}$ est simple. Par conséquent la paire i', j' est un virage pour la courbe \mathcal{C}^{s_1} qui est compatible avec s_2 . \square

Nous terminons maintenant la preuve du théorème 5.1.3. Rappelons la tresse en forme normale $x = \delta^p x_1 \dots x_r$, qui envoie la courbe standard \mathcal{C} sur une courbe standard $\mathcal{C}' = \mathcal{C}^x$. Pour tout $t \in \mathbb{Z}$, δ^t est une rotation de \mathbb{D}_n et envoie donc toute courbe standard sur une courbe standard. Nous pouvons donc supposer, quitte à multiplier x par une puissance de δ , que x est une tresse positive dont la forme normale est $x_1 \dots x_r$. Par récurrence sur le nombre de facteurs dans la forme normale de x , il est suffisant de montrer que \mathcal{C}^{x_1} est standard. Nous prouvons ce fait par contradiction, en supposant que \mathcal{C}^{x_1} n'est pas standard. Nous allons montrer (par induction sur $m = 1, \dots, r$) que sous cette hypothèse, aucune courbe $\mathcal{C}^{x_1 \dots x_m}$ pour $1 \leq m \leq r$ ne peut être standard, contredisant le fait que \mathcal{C}^x est standard.

Soit $x_1 = P_1 \dots P_g$ la décomposition de x_1 en polygones disjoints. Par ailleurs, supposons aussi que $W(\mathcal{C})$ est écrit uniquement avec des lettres dans $\{\smile, \frown, 1, \dots, n\}$ (autrement dit on choisit l'orientation anti-horaire pour \mathcal{C}).

Comme \mathcal{C}^{x_1} n'est pas standard, ainsi en est-il de \mathcal{C}^{P_t} pour au moins un $t = 1, \dots, g$ (en vertu de la Remarque 5.3.1). On peut supposer que \mathcal{C}^{P_1} n'est pas standard. Il existe donc un arc $i \sim j$ dans $W(\mathcal{C})$ tel que P_1 est transverse à $i \sim j$ et j n'est pas un sommet de P_1 (ainsi $W(\mathcal{C}^{P_1})$ contient au moins une lettre \frown , en vertu des Formules $(F'0)$ et $(F'2)$).

Considérons tous les polygones parmi P_1, \dots, P_g qui sont transverses à l'arc $i \sim j$. Par la Remarque 5.3.1, ce sont les seuls polygones dans la décomposition de x_1 qui témoignent de l'action de x_1 sur $i \sim j$. En parcourant l'arc $i \sim j$ à partir de l'arc $(i, i+1)$ de Γ , on ordonne ces polygones de manière naturelle (voir la preuve du lemme 5.4.2): Q_1, \dots, Q_h . Soit q_1 le sommet de Q_1 le plus

à droite le long de l'arc $(i + 1, j)$ (de sorte que $q_1 \neq j$) et si $h > 1$ soit p_2 le sommet de Q_2 le plus à droite le long de l'arc $(j + 1, i)$.

Nous définissons alors $i_1 = q_1$ et $j_1 = p_2$ si $h > 1$, $j_1 = j$ sinon. Les Formules (F') et le lemme 5.3.2 impliquent que $W(\mathcal{C}^{x_1})$ contient le sous-mot $\curvearrowright i_1 \smile j_1 \curvearrowleft$ (ou $\curvearrowright i_1 \smile j_1 \curvearrowright$). Par construction, la tresse $x_1 a_{i_1, j_1}$ est simple en vertu du lemme 2.2.5. Autrement dit, i_1, j_1 est un virage pour la courbe \mathcal{C}^{x_1} ; puisque la paire (x_1, x_2) est pondérée, ce virage est compatible avec x_2 .

Il s'ensuit par induction sur m et grâce au lemme 5.4.2 que l'on peut trouver un virage i_m, j_m pour la courbe $\mathcal{C}^{x_1 \cdots x_m}$ qui est compatible avec x_{m+1} , ce pour tout $m = 1, \dots, r - 1$. L'existence d'un virage i_r, j_r pour la courbe $\mathcal{C}^{x_1 \cdots x_r}$ est également une conséquence du Lemme 5.4.2.

En particulier, nous avons montré que la courbe $\mathcal{C}^{x_1 \cdots x_r} = \mathcal{C}^x$ n'est pas standard. Cela contredit nos hypothèses et termine la preuve du théorème 5.1.3.

5.5. Reconnaissance algorithmique de courbes de réduction standard

Les analogues des proposition 3.3.3 et corollaire 3.3.4 se déduisent, comme dans le cas classique, du théorème 5.1.3. Cela fournit, dans le cadre dual, un algorithme à la Benardete, Gutierrez et Nitecki pour décider de la réductibilité d'une tresse donnée, si l'on est capable de détecter efficacement la présence de courbes de réduction standard. On observe que les classes d'isotopie de courbes standard sont en nombre exponentiel (en fonction de n); par conséquent, nous devons éviter un test exhaustif. C'est l'objet du résultat suivant, qui s'inspire du théorème 2.9 de [40]. Nous continuons à écrire "courbe" pour signifier "classe d'isotopie de courbes".

THÉORÈME 5.5.1. *Il existe un algorithme qui décide si une tresse $x \in BKL_n$ donnée en forme normale $x = \delta^p x_1 \dots x_\ell$ préserve une courbe standard de \mathbb{D}_n . De plus, cet algorithme est de complexité $O(\ell \cdot n^4)$.*

DÉMONSTRATION. Soit I_0 un sous-ensemble $\{1, \dots, n\}$ (satisfaisant

$$2 \leq \#(I_0) \leq n - 1)$$

et x une tresse en forme normale $x = \delta^p x_1 \dots x_\ell$. La principale étape de l'algorithme consiste à construire un sous-ensemble $S(I_0, x)$ de $\{1, \dots, n\}$, avec au moins le même cardinal que I_0 et satisfaisant la propriété suivante : si \mathcal{C} est une courbe standard entourant les trous de I_0 et telle que \mathcal{C}^x est standard, alors tous les trous de $S(I_0, x)$ doivent être entourés par \mathcal{C}^x . La construction repose sur le lemme suivant :

LEMME 5.5.2. *Soit s une tresse simple, exprimée comme le produit de polygones disjoints : $s = P_1 \dots P_g$. Soit I un sous-ensemble strict de $\{1, \dots, n\}$ de cardinal au moins 2, dont les éléments sont énumérés a_1, \dots, a_k dans cet ordre (modulo permutation cyclique) en parcourant le cercle Γ dans le sens horaire (on note $a_{k+1} = a_1$). Pour tout $i = 1, \dots, k$, considérons tous les polygones parmi P_1, \dots, P_g dont au moins un sommet, mais pas tous, sont dans l'arc $(a_i + 1, a_{i+1} - 1)$ de Γ et dont a_i n'est pas un sommet. Pour chacun d'eux, choisissons son sommet le plus à gauche dans l'arc $(a_i + 1, a_{i+1} - 1)$. Soit I' la réunion de I avec tous les trous collectés de cette manière. Si \mathcal{C} est une courbe standard entourant les trous de I (et éventuellement d'autres trous) telle que \mathcal{C}^s est standard, alors \mathcal{C} entoure les trous dans I' . De plus, si $I' = I$, la courbe standard entourant exactement les trous de I est transformée en une courbe standard par s .*

DÉMONSTRATION. On observe d'abord que l'image d'une courbe standard par l'action de s est standard si et seulement si l'image de cette courbe par l'action de chaque polygone P_i ($i = 1, \dots, g$) est une courbe standard (Remarque 5.3.1). Or, pour un polygone Q et une courbe standard \mathcal{C} orientée dans le sens anti-horaire, les conditions suivantes sont équivalentes en vertu des Formules (F') :

- \mathcal{C}^Q est standard,
- pour tout arc intérieur $a \smile b$ de \mathcal{C} qui est transverse à Q , le trou b est un sommet de Q .

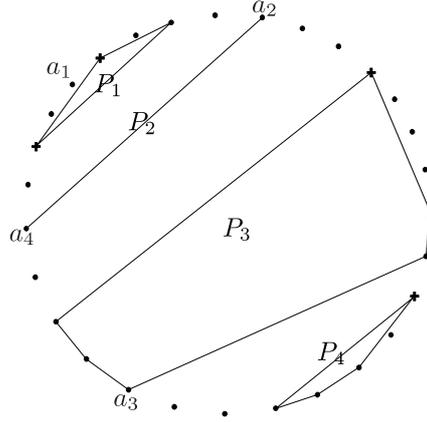


FIGURE 8. Un exemple qui illustre le lemme 5.5.2: ici la tresse simple s est décomposée comme $s = P_1 \dots P_4$, et I est formé des 4 trous a_1, a_2, a_3, a_4 . En parcourant chaque arc (a_i, a_{i+1}) , on peut construire l'ensemble I' , en ajoutant à I les trous représentés par des croix.

Soit \mathcal{C} une courbe standard (orientée dans le sens anti-horaire) entourant les trous de I , telle que \mathcal{C}^s est standard. Les trous de $I' - I$ (i.e. les trous ajoutés à I par le procédé du lemme 5.5.2) ne peuvent pas se trouver dans la composante extérieure de $\mathbb{D}_n - \mathcal{C}$. En effet, si c'était le cas, on aurait un arc intérieur $a \sim b$ de \mathcal{C} , transverse à un polygone intervenant dans la décomposition de s et n'ayant pas b pour sommet ; cela contredirait la remarque ci-dessus. Voir figure 8.

Soit \mathcal{C}_I la courbe standard entourant exactement les trous de I (orientée dans le sens anti-horaire) et supposons que le procédé du lemme 5.5.2 nous donne $I' = I$. Alors, dès qu'un polygone P_i et un arc intérieur $a \sim b$ de \mathcal{C}_I sont transverses, le trou b est un sommet dudit polygone (sinon au moins un trou sur l'arc $(b+1, a)$ serait ajouté à I par le procédé du lemme 5.5.2). Par la remarque ci-dessus, la courbe \mathcal{C}_I^s est standard, comme nous voulions montrer. \square

L'ensemble I' du lemme précédent dépend seulement de I et de s , et nous notons $S(I, s)$ l'ensemble $\rho(s)(I')$ (où ρ est le morphisme canonique $B_n \rightarrow S_n$).

Le lemme 5.5.2 nous dit que si \mathcal{C} est une courbe standard entourant les trous de I et \mathcal{C}^s est standard, alors \mathcal{C}^s doit entourer les trous de $S(I, s)$. En utilisant le théorème 5.1.3 et une récurrence sur le nombre de facteurs distincts de δ dans la forme normale de x , nous construisons l'ensemble $S(I_0, x)$.

On pose d'abord $S(I_0, \delta^p x_1) = S(\rho(\delta^p)(I_0), x_1)$. On définit ensuite, pour $i = 1, \dots, \ell - 1$,

$$S(I_0, \delta^p x_1 \dots x_{i+1}) = S(S(I_0, \delta^p x_1 \dots x_i), x_{i+1}).$$

Remarquons que l'ensemble $S(I_0, x)$ est calculable en temps $O(\ell \cdot n)$. Remarquons aussi qu'en vertu du lemme 5.5.2, l'égalité $S(I, x) = I$ implique que la courbe entourant exactement les trous dans I est invariante sous l'action de x .

La dernière étape dans la preuve du théorème 5.5.1 est l'énoncé suivant :

PROPOSITION 5.5.3. *Soit a, b une paire de trous dans $\{1, \dots, n\}$. Il existe un algorithme qui décide si une tresse $x \in BKL_n$ de longueur canonique ℓ donnée en forme normale préserve une courbe de réduction standard entourant les trous a et b . De plus, la complexité de cet algorithme est $O(\ell \cdot n^2)$.*

DÉMONSTRATION. Il suffit de suivre les étapes suivantes :

- poser $I_0 = \{a, b\}$,
- pour $m = 1, \dots, n - 2$, calculer l'ensemble $I_m = S(I_{m-1}, x) \cup I_{m-1}$.

Par construction, $I_{i-1} \subset I_i$ pour tout i . Si $I_{n-2} = \{1, \dots, n\}$, alors l'algorithme répond négativement ; sinon, la courbe standard qui entoure exactement les trous dans I_{n-2} est invariante

sous l'action de x . En effet, dans le dernier cas, il existe un entier k , $1 \leq k < n - 2$, tel que $\#(I_k) = \#(I_{k+1})$, et donc $I_k = I_{k+1} = I_{n-2}$. Autrement dit, on a l'égalité $S(I_k, x) = I_k$ et donc la courbe standard entourant exactement les trous de I_{n-2} (et donc en particulier les trous a et b) est invariante sous l'action de x . La complexité de cet algorithme est $O(\ell \cdot n^2)$, selon l'estimation ci-dessus de la complexité du calcul de $S(I_0, x)$. \square

En répétant cet algorithme pour toute paire de trous dans $\{1, \dots, n\}$, on obtient l'algorithme promis par le théorème 5.5.1. Puisque le nombre de paires de trous dans $\{1, \dots, n\}$ est $\frac{n \cdot (n-1)}{2}$, la complexité de l'algorithme est $O(\ell \cdot n^4)$ comme nous voulions montrer. \square

L'analogie de l'algorithme de Benardete, Gutierrez et Nitecki dans le cadre dual souffre du même inconvénient que dans le cadre classique : la taille des ensembles de circuits glissants. Nous terminons par un contre-exemple qui montre que, outre le théorème 3.3.1, les difficultés rencontrées dans le cadre classique elles aussi se généralisent au cadre dual.

EXEMPLE 5.5.4. Considérons la tresse à 4 brins

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

en forme normale à gauche, rigide. Cette tresse est réductible mais n'admet aucune courbe de réduction standard. Voir figure 9.

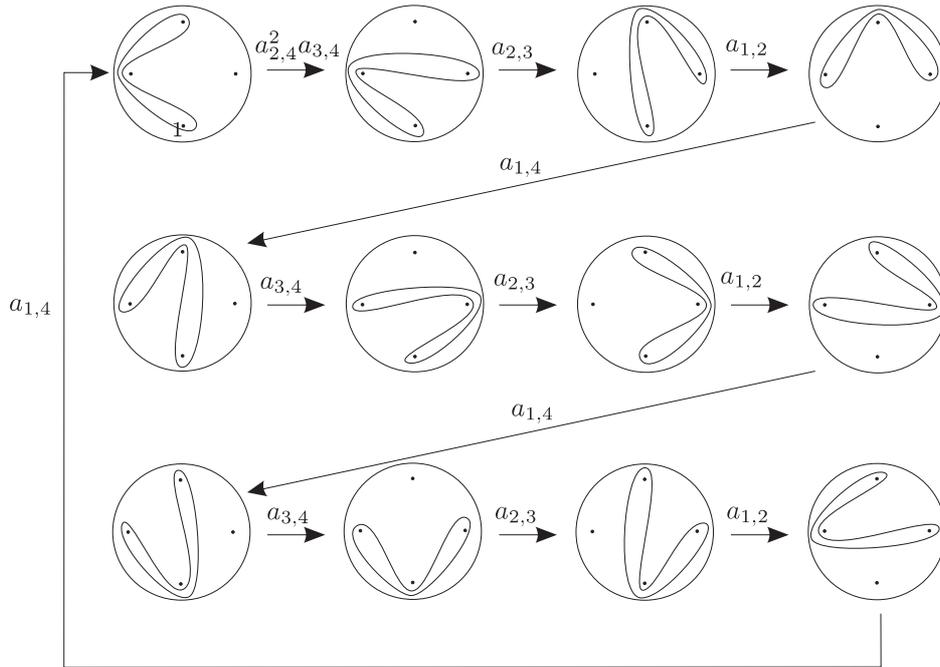


FIGURE 9. La tresse x de l'Exemple 5.5.4; et sur la première vignette en haut à gauche, une courbe non standard invariante sous l'action de x .

Le problème de réductibilité : le cas des tresses à 4 brins

6.1. Énoncé des principaux résultats

Après les résultats généraux des Chapitres 3 à 5, nous particularisons l'étude du problème de réductibilité au cas du groupe des tresses à 4 brins B_4 . Dans ce chapitre, nous reprenons les résultats de [15]. Contrairement à la situation générale où le Super Summit Set d'une tresse réductible peut contenir des éléments dont les courbes de réduction sont plutôt compliquées (Exemple 3.3.6), nous allons voir que dans le cas des tresses à 4 brins, la réductibilité est relativement aisée à décider, pour *tout* élément du Super Summit Set. Ensemble avec le théorème 2.3.7, cela donne lieu à un algorithme de complexité quadratique en fonction de la longueur pour résoudre le problème de réductibilité :

THÉORÈME 6.1.1. *Il existe un algorithme qui décide, étant donné une tresse x à 4 brins exprimée comme un produit des générateurs d'Artin et de leurs inverses de longueur au plus l , le type de Nielsen-Thurston de x et dont la complexité est $O(l^2)$.*

De plus, nous développons une méthode algorithmique, également polynômiale, pour déterminer le système de réduction canonique de x . Cela nous permet de résoudre le problème de conjugaison pour des tresses à 4 brins non pseudo-Anosov :

COROLLAIRE 6.1.2. *Les problèmes DC et RC admettent une solution polynômiale dans B_4 dans le cas non pseudo-Anosov, c'est à dire qu'on peut décider si deux tresses à 4 brins, dont au moins une n'est pas pseudo-Anosov, sont conjuguées et trouver un élément les conjuguant le cas échéant. De plus, la complexité de cet algorithme est $O(l^3)$ si l est le maximum des longueurs des entrées exprimées comme des mots sur les lettres $\sigma_i^{\pm 1}$.*

Les deux algorithmes sont détaillés dans la section 6.2. La plupart des détails techniques de la démonstration sont renvoyés à la section 6.3. Dans tout le chapitre, seule la structure de Garside classique est utilisée. Les classes d'isotopie de courbes fermées simples non dégénérées dans le disque \mathbb{D}_4 sont appelées simplement "courbes".

6.2. Description de l'algorithme

Notre raisonnement est basé sur le résultat technique crucial suivant :

PROPOSITION 6.2.1. *Soit $x \in B_4$ une tresse réductible telle que $x \in SSS(x)$. Supposons que x admet une courbe de réduction essentielle entourant 3 trous. Alors cette courbe est ronde ou presque-ronde.*

Nous admettons cela dans la présente section et reportons la preuve à la section 6.3. Rappelons que pour une tresse x , $CRS(x)$ désigne le système de réduction canonique de x , qui est l'ensemble de ses courbes de réduction essentielles. Rappelons aussi la relation liant entre le système de réduction canonique d'une tresse x et celui des puissances de x : pour tout entier m non nul, $CRS(x^m) = CRS(x)$. Observons que le disque \mathbb{D}_4 contient seulement 2 courbes rondes et 4 courbes presque rondes entourant 3 trous (voir figure 1).

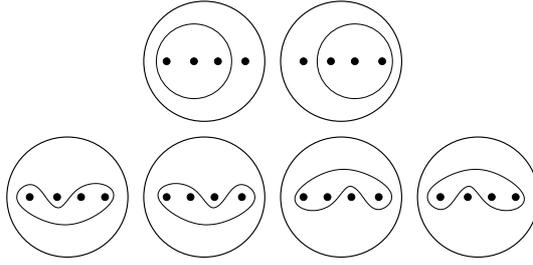


FIGURE 1. La partie supérieure représente les courbes rondes entourant 3 trous dans \mathbb{D}_4 ; la partie inférieure, l'ensemble des courbes obtenues à partir de celles du dessus en faisant agir des tresses simples, autrement dit l'ensemble des courbes presque rondes entourant 3 trous.

Lorsqu'une tresse $x \in B_4$ préserve l'une des courbes de la figure 1, on peut aisément déterminer une courbe de réduction essentielle de x ; c'est l'objet du lemme ci-dessous. Remarquons que si la courbe préservée est l'une des courbes presque-rondes, on peut se ramener au cas où la courbe est ronde, quitte à conjuguer x par un élément simple. Enfin, remarquons que si $x \in B_4$ est une tresse réductible avec une courbe de réduction essentielle entourant 3 trous, cette dernière est nécessairement fixée par x (on ne peut pas trouver deux courbes entourant 3 trous dans \mathbb{D}_4 et qui sont disjointes).

LEMME 6.2.2. *Soit $x \in B_4$ une tresse réductible préservant une courbe ronde \mathcal{C} entourant 3 trous connue explicitement. Alors on peut déterminer une courbe de réduction essentielle de x en temps $O(l^3)$, où l est la longueur de x exprimé comme un mot sur les lettres $\sigma_i^{\pm 1}$.*

DÉMONSTRATION. Afin de faire cela, on cherche à décider le type de Nielsen-Thurston de la tresse $\hat{x} \in B_3$ obtenue en oubliant le brin de x qui n'est pas entouré par \mathcal{C} (on peut obtenir un mot représentant \hat{x} à partir d'un mot représentant x en temps linéaire). En vertu de la proposition 3.3.5, le type de Nielsen-Thurston de \hat{x} peut être décidé en temps $O(l^3)$, et on obtient en outre un élément $\hat{P} \in B_3$ tel que \hat{x} est réductible si et seulement si $\hat{x}^{\hat{P}}$ préserve une courbe ronde \mathcal{C}_0 entourant 2 trous; \mathcal{C}_0 est alors une courbe de réduction essentielle. Sous cette hypothèse, la courbe $\mathcal{C}_0^{P^{-1}}$ est une courbe de réduction essentielle de x (où P est l'élément de B_4 obtenu en ajoutant un brin trivial à \hat{P}). Sinon (i.e. si \hat{x} est périodique ou pseudo-Anosov) alors \mathcal{C} est une courbe de réduction essentielle pour x . \square

Notons que la proposition 6.2.1 ne permet pas a priori de décider de la réductibilité d'une tresse à 4 brins. En effet, si $x \in B_4$ et $y \in SSS(x)$ ne préserve aucune des courbes de la figure 1, on peut seulement déduire que x n'a pas de courbe de réduction essentielle entourant 3 trous. Pour pallier l'absence d'un résultat analogue à la proposition 6.2.1 pour les courbes de réduction entourant 2 trous, nous allons considérer les tresses à 4 brins comme des éléments de $Mod(\mathbb{S}_5)$. Dans la sphère, nous imaginons les 5 trous sur l'équateur et nous les numérotions de 1 à 5, le cinquième étant le trou issu de $\partial\mathbb{D}_4$, à l'arrière de la sphère. Dans la construction subséquente, la tresse $x \in B_4$ est choisie pure; notons que cette condition est satisfaite quitte à prendre la seconde, la troisième ou la quatrième puissance de x .

Pour $j = 1, \dots, 4$, en "ouvrant" la sphère \mathbb{S}_5 au niveau du j -ième trou, ce dernier devenant le bord d'un nouveau disque \mathbb{D}_4 , on obtient une nouvelle tresse à 4 brins que nous notons \tilde{x}_j .

LEMME 6.2.3. *Pour $j = 1, \dots, 4$, la longueur $l(\tilde{x}_j)$ de \tilde{x}_j en terme des générateurs d'Artin est bornée supérieurement par $3l(x)$.*

DÉMONSTRATION. Nous montrons que chaque lettre de x donne lieu à au plus 3 lettres dans \tilde{x}_j . Pour ce faire nous décrivons en détail comment la première lettre de x est transformée. Pour identifier le j -ième trou avec le bord du nouveau disque, on effectue une rotation de l'équateur qui

transporte le j -ième trou à l'arrière de la sphère à la place du cinquième et une renumérotation des trous selon la règle :

$$\begin{aligned} i &\rightsquigarrow i - j + 5 && \text{si } i \leq j, \\ i &\rightsquigarrow i - j && \text{si } i > j. \end{aligned}$$

Si la première lettre de x est σ_i , avec $1 \leq i \leq j-2$, respectivement $j+1 \leq i \leq n-1$, alors son image dans \tilde{x}_j est σ_{i-j+5} , respectivement σ_{i-j} . Supposons $j \geq 2$. La lettre σ_{j-1} de x correspond à un mouvement du trou numéroté $(j-1)$ qui se déplace vers la droite en dessous du trou numéroté j . Après la rotation convenable, le mouvement correspondant implique le quatrième trou qui se déplace en dessous des autres trous jusqu'à la première position. La tresse correspondante est $\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}$. De manière similaire on peut calculer les images de toutes les lettres possibles, soit en formules :

$$\begin{aligned} \sigma_i^{\pm 1} &\rightsquigarrow \sigma_{i-j+5}^{\pm 1} && \text{si } i < j-1, \\ \sigma_i^{\pm 1} &\rightsquigarrow \sigma_{i-j}^{\pm 1} && \text{si } i > j, \\ \sigma_{j-1}^{\pm 1} &\rightsquigarrow \sigma_3^{\mp 1}\sigma_2^{\mp 1}\sigma_1^{\mp 1} && (\text{pour } j \geq 2), \\ \sigma_j^{\pm 1} &\rightsquigarrow \sigma_1^{\mp 1}\sigma_2^{\mp 1}\sigma_3^{\mp 1} && (\text{pour } j \leq 3). \end{aligned}$$

Remarquons que la première lettre de x induit une permutation des trous qui peut envoyer le trou numéroté j vers une autre position. Alors, calculer l'image de la deuxième lettre de x à l'aide des formules ci-dessus requiert une renumérotation des trous, selon la permutation convenable. Les images de toutes les autres lettres de x sont calculées de la même manière. On obtient ainsi un mot représentant \tilde{x}_j de longueur supérieurement bornée par $3l(x)$. \square

LEMME 6.2.4. *Soit $x \in B_4$ une tresse pure réductible n'admettant pas de courbe de réduction essentielle entourant 3 trous. Alors il existe un entier j ($1 \leq j \leq 4$) tel que \tilde{x}_j est réductible avec une courbe de réduction essentielle entourant 3 trous.*

DÉMONSTRATION. La réductibilité de x est équivalente à celle de \tilde{x}_j pour tout $j = 1, \dots, 4$ (en effet une courbe de réduction essentielle de x , en particulier qui entoure 2 ou 3 trous, fournit une courbe de réduction essentielle de \tilde{x}_j et vice versa). Sous l'hypothèse du lemme, x admet une courbe de réduction essentielle entourant 2 trous. Dans \mathbb{S}_5 , cette courbe divise la sphère en deux composantes connexes, l'une avec 2 trous, l'autre avec 3 trous, cette dernière contenant le nouveau trou issu du bord de \mathbb{D}_4 . En prenant j comme le numéro de l'un des deux premiers, la tresse \tilde{x}_j satisfait la conclusion souhaitée. \square

Ainsi, une tresse pure $x \in B_4$ non périodique est réductible si et seulement s'il existe $j = 0, \dots, 4$ tel que tout élément du Super Summit Set de \tilde{x}_j (avec $\tilde{x}_0 = x$) préserve l'une des courbes de la figure 1. Nous sommes maintenant prêts pour décrire l'algorithme qui résout le problème de réductibilité dans B_4 .

ALGORITHME 6.2.5. Pour décider le type de Nielsen-Thurston de $x \in B_4$.

0. ENTREE: Une tresse $x \in B_4$ exprimée comme un produit des lettres $\sigma_i^{\pm 1}$ de longueur au plus l .
1. Calculer une puissance pure x^t de x et changer $x := x^t$.
2. Calculer la forme normale de x .
3. Tester si x est périodique. Si oui, alors répondre " x est périodique" et STOP.
4. Appliquer l'opération \mathfrak{s} itérativement à x jusqu'à ce que la longueur canonique n'ait pas diminué au cours des 5 dernières itérations.
5. Tester si l'élément y de $SSS(x)$ obtenu à l'étape précédente préserve l'une des 6 courbes de la figure 1. Si oui, répondre " x est réductible" et STOP.
6. Pour $j = 1, \dots, 4$, calculer \tilde{x}_j , appliquer à \tilde{x}_j les étapes 2 et 4. Tester si l'élément de \tilde{y}_j de $SSS(\tilde{x}_j)$ obtenu ainsi préserve l'une des courbes de la figure 1. Si la réponse est positive pour un certain j , répondre " x est réductible" et STOP. Sinon répondre " x est pseudo-Anosov" et STOP.

L'étape 1 consiste à calculer l'ordre dans le groupe symétrique sur 4 éléments d'un produit de l transpositions et coûte $O(l)$. En vertu des résultats dans la section 3.1, les étapes 2 et 3 sont quadratiques en l (remarquons que l'étape 3 consiste seulement à vérifier (comme x est pure) si x est une puissance de Δ^2). Le calcul de $y \in SSS(x)$ coûte $O(l^2)$ (étape 4). Enfin, l'étape 5 coûte $O(l)$. L'étape 6 consiste à appliquer les étapes précédentes à des tresses dont la longueur est linéairement bornée par l (en vertu du lemme 6.2.3); par conséquent cette étape est aussi quadratique. La totalité de l'algorithme a donc complexité $O(l^2)$, comme annoncé.

DÉMONSTRATION. (corollaire 6.1.2). Etant donnés deux mots de tresses $w^{(1)}$ et $w^{(2)}$ de longueur l en terme des générateurs $\sigma_i^{\pm 1}$ ($i = 1, 2, 3$), nous voulons tester s'ils sont conjugués, et ce en temps $O(l^3)$. Nous testons d'abord si les deux tresses ont le même type de Nielsen-Thurston (une condition nécessaire pour être conjuguées), en utilisant l'algorithme ci-dessus. Si c'est le cas, ou bien $w^{(1)}$ et $w^{(2)}$ sont périodiques et on peut résoudre DC et RC facilement [7], ou bien les deux tresses sont réductibles (nous avons supposé qu'elles n'étaient pas toutes deux pseudo-Anosov).

Considérons la puissance douzième $x^{(k)}$ de $w^{(k)}$, qui est une tresse pure ($k = 1, 2$). Pour tout $j = 0, \dots, 4$, considérons la tresse $\tilde{x}_j^{(k)}$ (avec $\tilde{x}_0^{(k)} = x$). Pour $j = 0, \dots, 4$ on peut calculer en temps $O(l^2)$ un élément $\tilde{y}_j^{(k)} \in SSS(\tilde{x}_j^{(k)})$ et une tresse $\tilde{P}_j^{(k)}$ (qui est le produit des différents éléments conjugués impliqués au cours des glissements cycliques itérés) telle que $\tilde{y}_j^{(k)} = (\tilde{x}_j^{(k)})^{\tilde{P}_j^{(k)}}$. Pour $j = 0, \dots, 4$, on teste alors si $\tilde{y}_j^{(k)}$ préserve une des courbes de la figure 1. Ces calculs sont effectués tant que $\tilde{y}_j^{(k)}$ ne préserve aucune des courbes de la figure 1. Par le lemme 6.2.4 et la proposition 6.2.1, pour au moins un j , $\tilde{y}_j^{(k)}$ préserve une courbe de la figure 1. On peut alors calculer en temps $O(l^3)$, quitte à conjuguer $y_j^{(k)}$ davantage comme dans la preuve du lemme 6.2.2, un élément conjugué $\tilde{Q}_j^{(k)}$ qui conjugue $y_j^{(k)}$ à une tresse dont on connaît une courbe de réduction essentielle *ronde*. L'homéomorphisme de \mathbb{S}_5 correspondant à ce conjugué de $\tilde{x}_j^{(k)}$ préserve aussi une courbe de réduction essentielle intersectant l'équateur seulement 2 fois. Alors, comme dans la preuve du lemme 6.2.3, on peut trouver à partir de $\tilde{P}_j^{(k)}\tilde{Q}_j^{(k)}$ une tresse $P^{(k)}$ qui conjugue $x^{(k)}$ à une tresse préservant une courbe de réduction *essentielle* ronde \mathcal{C}_k . Cette dernière tresse admet pour racine douzième $y^{(k)} = (w^{(k)})^{P^{(k)}}$; la courbe \mathcal{C}_k est alors une courbe de réduction essentielle de $y^{(k)}$.

Si les courbes \mathcal{C}_k ($k = 1, 2$) n'entourent pas le même nombre de trous, alors les tresses $w^{(k)}$ ne sont pas conjuguées. Si elles entourent toutes deux trois trous, alors $w^{(1)}$ et $w^{(2)}$ sont conjuguées si et seulement si les tresses intérieures (comme décrites dans la preuve du lemme 6.2.2) sont conjuguées et le brin qui ne se trouve pas entouré par la courbe dans $w^{(1)}$ et $w^{(2)}$ fait le même nombre de tours autour de la tresse intérieure. On peut vérifier ces deux conditions ainsi que rechercher un élément conjugué pour les tresses intérieures en temps $O(l^3)$ (corollaire 2.3.20).

Si les deux courbes \mathcal{C}_k entourent 2 trous, on détermine le type de Nielsen-Thurston de la tresse à 3 brins $z^{(k)}$ obtenue en considérant les deux brins entourés par \mathcal{C}_k comme formant un gros brin (c'est encore faisable en temps $O(l^3)$). Alors pour que $w^{(1)}$ et $w^{(2)}$ soient conjuguées il est nécessaire que $z^{(1)}$ et $z^{(2)}$ aient le même type de Nielsen-Thurston.

Si les tresses $z^{(k)}$ ($k = 1, 2$) sont périodiques ou pseudo-Anosov, alors les tresses $x^{(k)}$ sont conjuguées si et seulement si deux conditions sont vérifiées : le nombre de croisements des deux brins entourés par \mathcal{C}_k est le même, et les deux tresses $z^{(k)}$ sont conjuguées. Encore une fois, cela peut être testé très rapidement. Si les deux tresses $z^{(k)}$ sont réductibles, on peut trouver des tresses à 4 brins $u^{(k)}$ conjuguées à $x^{(k)}$ telles que $u^{(k)}$ a deux courbes de réduction rondes, chacune d'elles entourant 2 trous. L'élément conjugué peut être exprimé explicitement; d'abord en calculant une tresse à 3 brins qui conjugue $z^{(k)}$ vers une tresse $\hat{u}^{(k)}$ avec une courbe de réduction ronde; puis en dupliquant dans cette dernière tresse le brin correspondant à la courbe \mathcal{C}_k . Alors, $x^{(1)}$ et $x^{(2)}$

sont conjuguées si et seulement si les deux gros brins dans les $u^{(k)}$ ont le même nombre de croisements et si les paires non ordonnées des nombres de croisements des brins à l'intérieur des courbes coïncident dans $u^{(1)}$ et $u^{(2)}$. Tout cela est faisable en temps $O(l^3)$. \square

6.3. La réductibilité est aisée à détecter dans le Super Summit Set

Nous prouvons maintenant la proposition 6.2.1.

6.3.1. Notations et schéma de la preuve. Nous raisonnons par contradiction. Supposons donc qu'il existe une tresse réductible à 4 brins, élément de son propre Super Summit Set, et admettant une courbe de réduction essentielle de complexité supérieure ou égale à 2 et entourant 3 trous. On peut supposer que cette tresse est positive, quitte à multiplier par une puissance de Δ^2 . De plus, on peut supposer que la courbe de réduction considérée est de complexité exactement 2 (en vertu du théorème 3.2.4 et de la connexité des Super Summit Sets (propriété 2.3.3), la conjugaison par un préfixe convenable du standardisateur d'une courbe de complexité strictement supérieure à 2 fournit un autre élément du Super Summit Set avec une courbe de réduction essentielle de complexité 2). Enfin, on peut supposer que $\ell(x) > 1$ car aucune tresse de longueur canonique inférieure ou égale à 1 dans B_4 ne satisfait les conditions précédentes.

Soit donc $x \in B_4^+$ réductible, avec $\ell(x) > 1$, $x \in SSS(x)$ et admettant une courbe de réduction essentielle de complexité 2 entourant 3 trous. Soit \mathcal{C} cette courbe. Rappelons que \mathcal{C} est nécessairement fixée par l'action de x . La tresse x admet un brin pur, correspondant au trou qui n'est pas entouré par \mathcal{C} ; on appelle ce brin le *brin extérieur*. Les trois autres brins sont dits *intérieurs*. De plus, on note \hat{x} la tresse à 3 brins obtenue à partir de x en enlevant le brin extérieur.

La preuve se déroule de la façon suivante. D'abord, nous donnons une liste des courbes de complexité 2 entourant 3 trous dans \mathbb{D}_4 . Ensuite, nous prouvons que x et \hat{x} ont la même longueur canonique, et que $\hat{x} \in SSS(\hat{x})$, ainsi (proposition 2.3.18) \hat{x} est une tresse rigide. Enfin, nous montrons, à l'aide de la proposition 3.3.2 et de la rigidité de \hat{x} , qu'aucune des courbes de la liste dressée au paragraphe 6.3.2 ne peut être une courbe de réduction essentielle de x . Cela est mené à bien grâce à une étude détaillée des liens entre les formes normales de x et de \hat{x} .

6.3.2. Courbes de complexité 2 entourant 3 trous dans \mathbb{D}_4 . Nous classifions les (classes d'isotopie de) courbes fermées simples non dégénérées de complexité 2 entourant 3 trous dans \mathbb{D}_4 . Les (classes d'isotopie de) courbes entourant 3 trous dans \mathbb{D}_4 peuvent être décrites à l'aide de classes d'homotopie d'arcs reliant un des trous au bord $\partial\mathbb{D}_4$. Les homotopies permises ont lieu relativement au trou mis en jeu et autorisent des glissements de l'autre extrémité le long de $\partial\mathbb{D}_4$. Etant donné un tel arc γ , le bord du complémentaire dans \mathbb{D}_4 d'un voisinage tubulaire de $\gamma \cup \partial\mathbb{D}_4$ est alors la courbe fermée simple associée à γ . De plus, les arcs associés à des courbes de complexité 2 ont un nombre d'intersection au plus 1 avec chaque ligne verticale dans le disque et au moins 1 avec le diamètre horizontal (sans compter les extrémités).

La figure 2 représente toutes les possibilités de tels arcs. Les deux commentaires suivants concernant cette figure seront utiles au paragraphe 6.3.4.

REMARQUE 6.3.1. (1) Les courbes de type 1 et 2 sont les symétriques l'une de l'autre par rapport au diamètre horizontal. Ainsi, cette symétrie est préservée en faisant agir σ_i sur l'une d'elles et σ_i^{-1} sur l'autre. Les courbes 3 et 4 sont reliées par la même symétrie.

(2) On peut obtenir les courbes 3 à partir des courbes 2 (et 4 à partir de 1) par action de Δ . De plus, cette symétrie est préservée par les actions respectives d'une tresse x et de son conjugué $\tau(x)$.

6.3.3. Les deux tresses x et \hat{x} ont la même longueur canonique. Pour une tresse réductible $y \in B_4$ avec une courbe de réduction essentielle entourant 3 points, on note v_y le nombre de croisements dans y , comptés avec signe, dans lesquels le brin extérieur est mis en jeu. Le nombre v_y est un invariant de la classe de conjugaison de y .

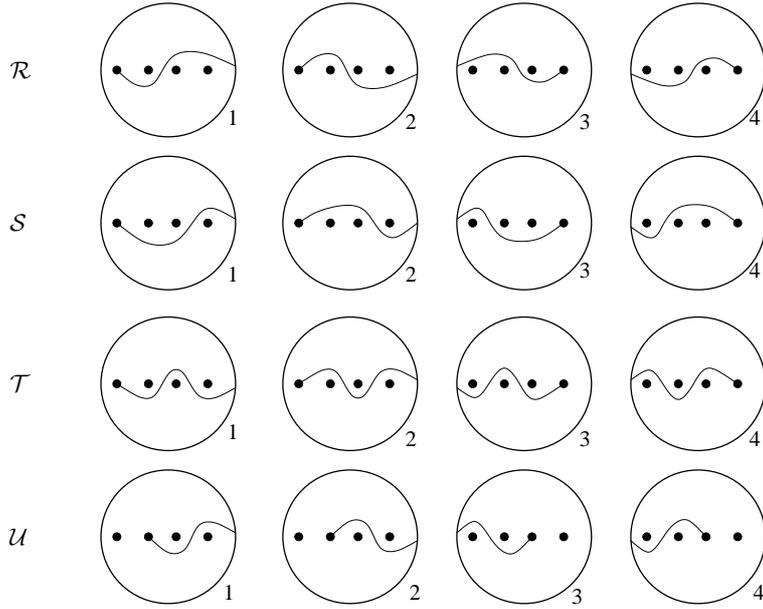


FIGURE 2

LEMME 6.3.2. *Soit $y \in B_4$ une tresse positive réductible avec une courbe de réduction essentielle de complexité 2 entourant 3 trous. Alors $v_y < 3 \sup(y)$.*

DÉMONSTRATION. Comme $y \in B_4^+$, y est le produit de $\sup(y)$ éléments simples. Or dans chaque tresse simple le brin extérieur a au plus 3 croisements, d'où $v_y \leq 3 \sup(y)$. Supposons que l'on ait l'égalité. Alors le brin extérieur croise tous les autres brins dans chaque facteur de la forme normale de y . Si le brin extérieur est le premier ou le quatrième, alors $\sup(y)$ doit être pair (ce brin extérieur est pur) et la courbe ronde entourant les trous 2,3 et 4 (respectivement 1,2 et 3) est préservée par y . C'est une contradiction car ces deux courbes rondes ont une intersection non vide avec chaque courbe de la figure 2.

Si le brin extérieur est le second ou le troisième, alors les facteurs de la forme normale de y distincts de Δ doivent être alternativement $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2$ et $\sigma_2\sigma_3\sigma_2\sigma_1\sigma_2$, de sorte que $\sup(y)$ est encore pair (le brin extérieur est pur) et les courbes rondes entourant les trous numérotés 1 et 2 d'une part, 3 et 4 d'autre part, sont préservées par y . C'est encore une contradiction. \square

Voyons maintenant que la longueur canonique n'est pas affectée en enlevant le brin extérieur de x :

PROPOSITION 6.3.3. *On a les égalités $\inf(\hat{x}) = \inf(x)$ et $\sup(\hat{x}) = \sup(x)$.*

DÉMONSTRATION. D'abord, remarquons que $\sup(\hat{x}) \leq \sup(x)$ et $\inf(\hat{x}) \geq \inf(x)$ puisque \hat{x} est obtenu de x en enlevant un brin. Soit P le standardisateur de \mathcal{C} . En enlevant le brin extérieur de x^P on obtient une tresse à 3 brins x' , conjuguée à \hat{x} : si $P' \in B_3$ est obtenu à partir de P en enlevant le brin extérieur, alors $x' = \hat{x}^{P'}$. Puisque x^P préserve une courbe ronde entourant 3 trous, on peut écrire (voir [42])

$$x^P = \langle x_0 \rangle x_1,$$

avec $x_0 \in B_2$ and $x_1 \in B_3$. (Cette notation signifie que x_1 est la tresse obtenue à partir de x^P en enlevant le brin extérieur et x_0 est la tresse à 2 brins obtenue en considérant x_1 comme un gros brin.) Remarquons que $x_1 = x'$. Ainsi si P'' est la tresse à 4 brins obtenue à partir de P' en ajoutant un brin "trivial" à la position convenable et si on définit $X = x^{PP''^{-1}}$, alors $X = \langle x_0 \rangle \hat{x}$; autrement dit X est un conjugué de x dans lequel on a une tresse tubulaire égale à \hat{x} et un brin extérieur qui se croisent $\frac{v_x}{3}$ fois : $x_0 = \sigma_1^{v_x/3}$).

Maintenant, on a ([42], lemme 3.6)

$$\sup(X) = \max(\sup(x_0), \sup(\hat{x}))$$

et puisque $x \in SSS(x)$ on a $\sup(X) \geq \sup(x)$.

Nous prouvons maintenant que $\sup(x_0) < \sup(X)$ (et en particulier $\sup(X) = \sup(\hat{x})$). En effet, si on avait $\sup(X) = \sup(x_0)$, alors on aurait l'égalité $v_X = 3 \sup(X)$ car la courbe préservée par X est ronde. On a aussi, puisque x et X sont conjuguées, $v_x = v_X$. Or, en vertu du lemme 6.3.2, $v_x < 3 \sup(x)$. Ainsi,

$$v_x < 3 \sup(x) \leq 3 \sup(X) = v_X = v_x,$$

contradiction. La deuxième partie de la proposition en découle puisqu'alors

$$\sup(\hat{x}) \leq \sup(x) \leq \sup(X) = \sup(\hat{x}).$$

De manière similaire,

$$\inf(X) = \min(\inf(x_0), \inf(\hat{x})).$$

De plus, on a $\inf(X) < \inf(x_0)$, puisqu'en cas d'égalité, $\Delta^{-\inf(X)}X$ appartiendrait au sous-groupe de B_4 engendré par σ_1 et σ_2 (ou au sous-groupe engendré par σ_2 et σ_3). Dans la terminologie de la section 6 de [42], une tresse conjuguée à une tresse appartenant à un sous-groupe parabolique standard strict de B_n est appelée *split*. De plus, $\inf(X)$ doit être pair (puisque le brin extérieur est pur), et dans ce cas, $\Delta^{-\inf(X)}x$ (conjuguée à $\Delta^{-\inf(X)}X$) serait aussi *split* et positive (puisque $x \in SSS(x)$, on a $\inf(X) \leq \inf(x)$) de sorte que la proposition 6.2 de [42] impliquerait que les courbes extérieures de $CRS(\Delta^{-\inf(X)}x) = CRS(x)$ sont rondes. C'est impossible puisque les seuls cercles qui ne croisent pas les courbes de la figure 2 sont strictement entourés par ces courbes. Ainsi,

$$\inf(X) = \inf(\hat{x}) \geq \inf(x) \geq \inf(X),$$

la dernière inégalité puisque $x \in SSS(x)$. On obtient finalement

$$\inf(X) = \inf(\hat{x}) = \inf(x).$$

Cela prouve la proposition et nous remarquons aussi que $X \in SSS(x)$. □

COROLLAIRE 6.3.4. *Avec les notations précédentes, on a $\hat{x} \in SSS(\hat{x})$.*

DÉMONSTRATION. Supposons au contraire qu'il existe une tresse \hat{z} conjuguée à \hat{x} avec $\inf(\hat{z}) > \inf(\hat{x})$ ou $\sup(\hat{z}) < \sup(\hat{x})$. Soit aussi \hat{y} l'élément les conjuguant, i.e. $\hat{z} = \hat{x}^{\hat{y}}$. Soit X comme dans la preuve de la proposition 6.3.3, i.e. $X = \langle x_0 \rangle \hat{x}$. Soit z la tresse à 4 brins obtenue en conjuguant X par \hat{y} augmenté d'un brin trivial en position convenable, de sorte que z a la même courbe de réduction essentielle que X et $z = \langle x_0 \rangle \hat{z}$.

A l'aide du même argument (basé sur le lemme 6.3.2) que dans la preuve de la proposition 6.3.3 et avec z jouant le rôle de X , on a $\sup(z) = \sup(\hat{z})$ et $\inf(z) = \inf(\hat{z})$.

Cela apporte la condition souhaitée puisque $x \in SSS(x)$ et z est un conjugué de x pour lequel notre hypothèse implique :

$$\sup(z) = \sup(\hat{z}) < \sup(\hat{x}) = \sup(x);$$

ou

$$\inf(z) = \inf(\hat{z}) > \inf(\hat{x}) = \inf(x).$$

□

COROLLAIRE 6.3.5. *La tresse \hat{x} est rigide.*

DÉMONSTRATION. On a $\ell_s(\hat{x}) = \ell(\hat{x}) = \ell(x) > 1$; voir alors la proposition 2.3.18. □

6.3.4. Analyse de la forme normale de x . Nous démontrons par l'absurde la Proposition 6.2.1, grâce au lemme suivant :

LEMME 6.3.6. *Aucune des courbes représentées dans la figure 2 ne peut être une courbe de réduction essentielle pour x .*

La preuve de cet énoncé repose sur une analyse détaillée des facteurs de la forme normale de x . Ceux-ci sont composés d'une tresse à 3 brins (intérieure) et, éventuellement, d'un mouvement du brin extérieur. A cause des égalités $\sup(x) = \sup(\hat{x})$ et $\inf(x) = \inf(\hat{x})$ (voir proposition 6.3.3), aucun des facteurs de x n'a sa composante intérieure triviale ou égale à Δ_3 . Selon la Proposition 2.3.17, les facteurs de la forme normale de \hat{x} sont exactement les composantes intérieures des facteurs de la forme normale de x . Rappelons que les seuls éléments simples distincts de Δ et de 1 dans B_3 sont σ_1 , σ_2 , $\sigma_1\sigma_2$ et $\sigma_2\sigma_1$.

Numéro du brin extérieur \ Facteur intérieur	1	2
σ_1	σ_2 $\sigma_2\sigma_1$ $\sigma_2\sigma_1\sigma_2$ $\sigma_2\sigma_1\sigma_2\sigma_3$	$\sigma_1\sigma_2$ $\sigma_1\sigma_2\sigma_1$ $\sigma_2\sigma_1$ $\sigma_2\sigma_1\sigma_3$
$\sigma_1\sigma_2$	$\sigma_2\sigma_3$ $\sigma_2\sigma_1\sigma_3$ $\sigma_2\sigma_1\sigma_3\sigma_2$ $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3$	$\sigma_1\sigma_2\sigma_3$ $\sigma_1\sigma_2\sigma_1\sigma_3$ $\sigma_2\sigma_1\sigma_3\sigma_2$ $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3$
σ_2	σ_3 $\sigma_3\sigma_1$ $\sigma_1\sigma_2\sigma_3\sigma_2$ $\sigma_3\sigma_1\sigma_2$	σ_3 $\sigma_3\sigma_1$ $\sigma_3\sigma_2$ $\sigma_3\sigma_2\sigma_3$
$\sigma_2\sigma_1$	$\sigma_3\sigma_2\sigma_1$ $\sigma_3\sigma_1\sigma_2\sigma_1$ $\sigma_3\sigma_2$ $\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1$	$\sigma_3\sigma_2\sigma_1$ $\sigma_3\sigma_1\sigma_2$ $\sigma_3\sigma_2\sigma_3\sigma_1$ $\sigma_3\sigma_1\sigma_2\sigma_1$

TABLE 1.

La table 1 décrit toutes les valeurs que peut prendre un élément simple non trivial distinct de Δ dans B_4 , selon la position initiale du brin extérieur et la valeur de la tresse intérieure (dans B_3). Chaque valeur possible pour la tresse intérieure donne lieu à 4 tresses simples à 4 brins, selon le mouvement du brin extérieur. Jusqu'à la fin de cette section, nous ne répétons pas "non trivial, distinct de Δ ", cela est toujours implicitement supposé.

On a vu que les courbes pour lesquelles le brin extérieur est le troisième ou le quatrième sont images sous l'action de Δ de courbes dont le brin extérieur est le deuxième, respectivement le premier. Ainsi, si le brin extérieur est en troisième (ou en quatrième position), les éléments simples de B_4 dont le facteur intérieur est σ_1 , $\sigma_1\sigma_2$, σ_2 , ou $\sigma_2\sigma_1$ sont les images par l'automorphisme τ de B_4 des éléments simples de B_4 avec brin extérieur en deuxième (ou première) position et tresse intérieure égale respectivement à σ_2 , $\sigma_2\sigma_1$, σ_1 , ou $\sigma_1\sigma_2$. Cela nous permet de construire le reste de la table 1 (que nous ne représentons pas ici), c'est à dire les situations où le brin extérieur porte le numéro 3 ou 4.

6.3.5. Preuve du lemme 6.3.6. Nous devons garder à l'esprit la proposition 3.3.2, dont nous faisons un usage constant. Cette proposition affirme que si la forme normale de x est $\Delta^p x_1 \cdots x_r$ et si x préserve une courbe de complexité 2, alors pour tout $i = 1, \dots, r$, l'image de la courbe en question sous l'action de $\Delta^p x_1 \cdots x_i$ est une courbe de complexité au plus 2.

Les 4 lemmes suivants éliminent toutes les courbes représentées dans la figure 2.

LEMME 6.3.7. *Aucune courbe de type \mathcal{T} ne peut être une courbe de réduction essentielle pour x .*

DÉMONSTRATION. Remarquons d'abord qu'à cause des symétries entre les courbes, il est suffisant de prouver le lemme pour les courbes \mathcal{T}_1 et \mathcal{T}_2 .

Pour chacune des courbes \mathcal{T}_1 et \mathcal{T}_2 , le brin extérieur est le premier brin. Les tresses simples à 4 brins dont le brin extérieur est le premier et dont la composante intérieure commence par la lettre σ_2 (respectivement σ_1) envoient la courbe \mathcal{T}_2 (respectivement \mathcal{T}_1) sur une courbe strictement plus complexe. A cause des symétries évoquées plus haut, les tresses simples à 4 brins dont le brin extérieur est le quatrième et dont la composante intérieure commence par la lettre σ_1 (respectivement σ_2) envoient la courbe \mathcal{T}_3 (respectivement \mathcal{T}_4) sur une courbe strictement plus complexe. De même, en vertu de la Remarque 6.3.1, l'action de l'inverse d'une tresse simple à 4 brins dont le brin extérieur est le premier et dont la composante intérieure commence par la lettre σ_1^{-1} (respectivement σ_2^{-1}) sur la courbe \mathcal{T}_2 (respectivement \mathcal{T}_1) résulte en une courbe strictement plus complexe (et ainsi en est il également de l'action de l'inverse d'une tresse simple à 4 brins dont le brin extérieur est en quatrième position et dont la composante intérieure commence avec la lettre σ_2^{-1} (respectivement σ_1^{-1}) sur la courbe \mathcal{T}_3 (respectivement \mathcal{T}_4).

Supposons maintenant que l'une des courbes \mathcal{T}_1 ou \mathcal{T}_2 est une courbe de réduction essentielle pour x .

Si $\inf(x)$ est pair, alors le premier facteur de $\Delta^{-\inf(x)}\hat{x}$ doit commencer par la lettre σ_2 (respectivement σ_1), en vertu de la proposition 3.3.2 et du paragraphe précédent.

La rigidité de \hat{x} implique alors que le dernier facteur de \hat{x} (qui est la composante intérieure du dernier facteur de x) doit se terminer par la lettre σ_2 (respectivement σ_1). A cause des symétries entre les courbes \mathcal{T}_1 et \mathcal{T}_2 , l'image de la courbe de réduction essentielle au début du dernier facteur de x doit être de complexité strictement supérieure à 2. Cela contredit la proposition 3.3.2.

Si $\inf(x)$ est impair, alors la courbe de réduction essentielle au début du premier facteur de x distinct de Δ est \mathcal{T}_4 (respectivement \mathcal{T}_3). Par conséquent la première lettre de $\Delta_3^{-\inf(x)}\hat{x}$ doit être σ_1 (respectivement σ_2). Et par la rigidité de \hat{x} , la dernière lettre de \hat{x} doit donc être σ_2 (respectivement σ_1). On obtient une contradiction comme précédemment en considérant les symétries par rapport à l'axe horizontal.

Ces deux cas et la remarque au début de la preuve concluent la démonstration du lemme 6.3.7. \square

Les ingrédients principaux des preuves des 3 lemmes suivants sont la proposition 3.3.2 et la pondération des paires de facteurs consécutifs dans la forme normale de \hat{x} ; nous utilisons ces deux faits implicitement de nombreuses fois.

LEMME 6.3.8. *Aucune courbe de type \mathcal{U} ne peut être une courbe de réduction essentielle pour x .*

DÉMONSTRATION. Comme précédemment nous prouvons le lemme seulement pour les courbes \mathcal{U}_1 et \mathcal{U}_2 . Pour obtenir une contradiction, nous supposons que l'une des courbes \mathcal{U}_1 ou \mathcal{U}_2 est une courbe de réduction essentielle pour x . La proposition 3.3.2 implique alors que l'image de cette courbe après chaque facteur de la forme normale de x est une courbe de complexité au plus 2.

AFFIRMATION 6.3.9. Supposons que la courbe \mathcal{U}_1 est une courbe de réduction essentielle pour x . Alors la première lettre de $\Delta_3^{-\inf(x)}\hat{x}$ est

$$\begin{cases} \sigma_1 & \text{si } \inf(x) \text{ est pair,} \\ \sigma_2 & \text{si } \inf(x) \text{ est impair.} \end{cases}$$

DÉMONSTRATION. Pour montrer l'Affirmation 6.3.9, il est suffisant de prouver que si l'infimum de x est nul et la première lettre de \hat{x} est σ_2 , alors x ne peut transformer \mathcal{U}_1 ni en \mathcal{U}_1 ni en \mathcal{U}_4 .

Cela prouve en effet la première partie de l'affirmation. Pour la seconde partie ($\text{inf}(x)$ impair), si \mathcal{U}_1 est préservée par x , $\Delta^{-\text{inf}(x)}x$ doit transformer $\mathcal{U}_1^\Delta = \mathcal{U}_4$ en \mathcal{U}_1 . Mais cela est impossible si la première lettre de $\Delta^{-\text{inf}(x)}\hat{x}$ est σ_1 , comme le montre notre assertion après conjugaison par Δ . La figure 3(a) illustre la preuve de cette affirmation.

Supposons donc que $\text{inf}(x) = 0$. Nous voulons montrer que si la première lettre de \hat{x} est σ_2 , alors l'action de x sur \mathcal{U}_1 ne peut jamais produire \mathcal{U}_1 ni \mathcal{U}_4 . Nous regardons quelles tresses simples à 4 brins pourraient être les facteurs de la forme normale de x , en supposant que la première lettre de \hat{x} est σ_2 . Parmi les 8 tresses simples à 4 brins dont le brin extérieur est en deuxième position et la composante intérieure commence par la lettre σ_2 , seulement 2 n'augmentent pas la complexité de la courbe \mathcal{U}_1 . Ce sont $\sigma_3\sigma_2\sigma_3$ et $\sigma_3\sigma_2\sigma_3\sigma_1$.

La première envoie \mathcal{U}_1 sur \mathcal{T}_4 et la seconde sur \mathcal{S}_4 . Leur composante intérieure est σ_2 , respectivement $\sigma_2\sigma_1$. Or, la courbe \mathcal{T}_4 est envoyée sur des courbes de complexité strictement plus grande par des tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_2 (voir lemme 6.3.7). La seule possibilité restante est donc la seconde.

Les seules tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_1 , dont le brin extérieur est le quatrième (comme dans la courbe \mathcal{S}_4) et dont l'action n'augmente pas la complexité de la courbe \mathcal{S}_4 sont $\sigma_1\sigma_3\sigma_2\sigma_1$ et $\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1$. La première transforme \mathcal{S}_4 en \mathcal{T}_1 et sa tresse intérieure est σ_1 , tandis que la seconde envoie \mathcal{S}_4 sur \mathcal{S}_1 et sa tresse intérieure est $\sigma_1\sigma_2$. Le lemme 6.3.7 exclut le premier cas. Examinons la deuxième alternative. Le prochain facteur de la forme normale de x est précédé par la courbe \mathcal{S}_1 et sa composante intérieure commence par la lettre σ_2 . Cette situation est l'image sous l'action de Δ de la situation que nous venons de décrire au début du facteur précédent. Par conséquent, ce troisième facteur doit être $\tau(\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1) = \sigma_1\sigma_2\sigma_3\sigma_2\sigma_1$. Après son action, la courbe obtenue est \mathcal{S}_4 . Au total on voit que si la tresse intérieure commence par la lettre σ_2 , la courbe \mathcal{U}_1 ne peut être ni préservée ni transformée en \mathcal{U}_4 par x . Cela montre l'Affirmation 6.3.9. \square

AFFIRMATION 6.3.10. Supposons que la courbe \mathcal{U}_2 est une courbe de réduction essentielle pour x . Alors la première lettre de $\Delta_3^{-\text{inf}(x)}\hat{x}$ est

$$\begin{cases} \sigma_2 & \text{si } \text{inf}(x) \text{ est pair,} \\ \sigma_1 & \text{if } \text{inf}(x) \text{ est impair.} \end{cases}$$

DÉMONSTRATION. Il est suffisant de prouver que si $\text{inf}(x) = 0$ et la première lettre de \hat{x} est σ_1 , alors x ne peut transformer \mathcal{U}_2 ni en \mathcal{U}_2 ni en $\mathcal{U}_3 (= \mathcal{U}_2^\Delta)$. La figure 3(b) illustre la preuve de cette affirmation.

Seule l'action de deux des 8 tresses simples à 4 brins dont le brin extérieur est en deuxième position et dont la composante intérieure commence par la lettre σ_1 n'augmente pas la complexité de la courbe \mathcal{U}_2 . Les tresses concernées sont $\sigma_1\sigma_2$ et $\sigma_1\sigma_2\sigma_3$.

La première a sa tresse intérieure égale à σ_1 et envoie \mathcal{U}_2 sur \mathcal{S}_2 . La seconde a sa tresse intérieure égale à $\sigma_1\sigma_2$ et envoie \mathcal{U}_2 sur \mathcal{T}_2 . Le lemme 6.3.7 exclut ce cas puisque la courbe \mathcal{T}_2 est toujours envoyée sur une courbe strictement plus complexe par un élément simple dont la composante intérieure commence par la lettre σ_2 . Nous examinons donc la première alternative.

Les seules tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_1 avec le brin extérieur en première position (comme dans la courbe \mathcal{S}_2) et dont l'action n'augmente pas la complexité de la courbe \mathcal{S}_2 sont σ_2 (tresse intérieure σ_1) dont l'action fixe \mathcal{S}_2 et $\sigma_2\sigma_3$ (tresse intérieure $\sigma_1\sigma_2$) dont l'action transforme \mathcal{S}_2 en \mathcal{T}_2 . Encore une fois, le lemme 6.3.7 exclut ce dernier cas. Au total, on a montré que si la première lettre de \hat{x} est σ_1 , la courbe \mathcal{U}_2 ne peut être fixée par x , ni transformée en \mathcal{U}_3 . Cela démontre l'Affirmation 6.3.10. \square

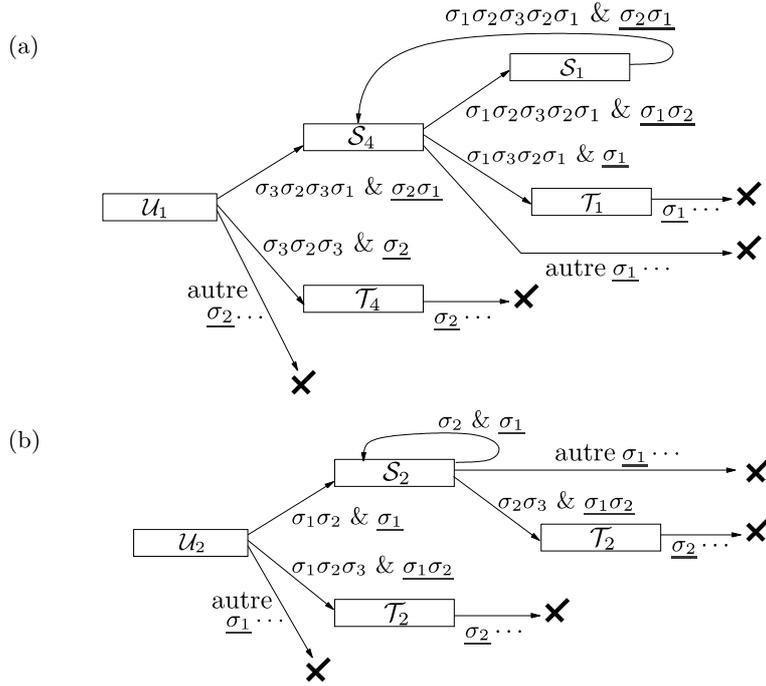


FIGURE 3. (a) Les tresses simples à 4 brins dont la composante intérieure commence avec la lettre σ_2 agissant sur la courbe \mathcal{U}_1 . (b) Les tresses simples à 4 brins dont la composante intérieure commence avec la lettre σ_1 agissant sur la courbe \mathcal{U}_2 . Les lettres soulignées indiquent les tresses intérieures (à 3 brins). Les croix en gras indiquent des courbes de complexité strictement plus grande que 2. Dans la partie (a) on peut également voir l'action sur la courbe \mathcal{S}_4 des tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_1 ; et dans la partie (b) l'action sur la courbe \mathcal{S}_2 des tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_2 . Nous ferons usage de cette observation au lemme 6.3.11.

Supposons maintenant que \mathcal{U}_1 est préservée par l'action de x . On a donc aussi $(\mathcal{U}_1)^{x^{-1}} = \mathcal{U}_1$. En utilisant la symétrie par rapport à l'axe horizontal, cela implique $\mathcal{U}_2^{\text{rev}(x)} = \mathcal{U}_2$, (où rev est l'anti-automorphisme $\sigma_i \mapsto \sigma_i$).

La tresse intérieure de $\text{rev}(x)$ est $\text{rev}(\hat{x})$ et en vertu de la proposition 2.3.17, si $\Delta_3^p \hat{x}_1 \dots \hat{x}_r$ est la forme normale de \hat{x} , alors $\text{rev}(\hat{x}_r) \dots \text{rev}(\hat{x}_1)$ est la forme normale de $\text{rev}(\hat{x}) \Delta_3^{-p}$.

Puisque \hat{x} est rigide, l'Affirmation 6.3.9 implique que la dernière lettre de \hat{x} doit être σ_1 . En d'autres termes la première lettre de $\text{rev}(\hat{x}_r)$ doit être σ_1 . En reprenant la preuve de l'Affirmation 6.3.10, on voit alors que $\text{rev}(x) \Delta^{-\text{inf}(x)}$ ne peut transformer la courbe \mathcal{U}_2 en aucune des courbes de type \mathcal{U} (voir figure 3); contradiction.

Si \mathcal{U}_2 est préservée par x , la rigidité de \hat{x} et l'Affirmation 6.3.10 impliquent que la dernière lettre de \hat{x} doit être σ_2 . Cela conduit à une contradiction de la même manière que précédemment. \square

LEMME 6.3.11. *Aucune courbe de type \mathcal{S} ne peut être une courbe de réduction essentielle pour x .*

DÉMONSTRATION. Le schéma de la preuve est similaire à celui de la preuve du lemme 6.3.8; voir aussi le diagramme de la figure 3. Notons que l'hypothèse que la courbe est *essentielle* n'est pas utilisée dans la preuve du lemme 6.3.8, mais seulement le fait que la courbe est préservée. Cette hypothèse n'est pas superflue dans le cas des courbes \mathcal{S} .

D'une part, il existe une tresse à 4 brins d'infimum 0 dont la composante intérieure commence par la lettre σ_2 et qui transforme \mathcal{S}_1 en \mathcal{S}_1 (respectivement \mathcal{S}_4). Il s'agit de $(\sigma_1\sigma_3\sigma_2\sigma_1\sigma_3)^m$, pour m pair (respectivement m impair). Mais si $\Delta^{-\inf(x)}x = (\sigma_1\sigma_3\sigma_2\sigma_1\sigma_3)^m$ pour un entier m , alors x préserve les cercles entourant d'une part les trous 1 et 2 et d'autre part les trous 3 et 4; ainsi \mathcal{S}_1 ne peut être une courbe de réduction essentielle.

D'autre part, il existe une tresse à 4 brins d'infimum 0 dont la composante intérieure commence par la lettre σ_1 et qui préserve \mathcal{S}_2 : il s'agit de σ_2^m , pour un entier m positif. Mais si $x = \Delta^{\inf(x)}\sigma_2^m$ et fixe \mathcal{S}_2 , alors $\inf(x)$ doit être pair et alors le cercle entourant les trous 1, 2 et 3, qui a une intersection non vide avec \mathcal{S}_2 , est préservé par x , contredisant le fait que \mathcal{S}_2 est une courbe de réduction essentielle.

A ce stade, nous avons prouvé les analogues des Affirmations 6.3.9 et 6.3.10 du lemme 6.3.8; la conclusion, se fait de manière similaire, en utilisant la rigidité de \hat{x} . \square

LEMME 6.3.12. *Aucune courbe de type \mathcal{R} ne peut être une courbe de réduction essentielle pour x .*

DÉMONSTRATION. La preuve est inspirée de celle du lemme 6.3.8. Encore une fois, nous prouvons l'énoncé seulement pour les courbes \mathcal{R}_1 et \mathcal{R}_2 .

AFFIRMATION 6.3.13. Supposons que la courbe \mathcal{R}_1 est une courbe de réduction essentielle pour x . Alors la première lettre de $\Delta_3^{-\inf(x)}\hat{x}$ est

$$\begin{cases} \sigma_2 & \text{si } \inf(x) \text{ est pair,} \\ \sigma_1 & \text{si } \inf(x) \text{ est impair.} \end{cases}$$

DÉMONSTRATION. Pour montrer cette affirmation, nous procédons comme au lemme 6.3.8 en montrant que si $\inf(x) = 0$ et la première lettre de \hat{x} est σ_1 , alors x ne peut transformer \mathcal{R}_1 en \mathcal{R}_1 ni \mathcal{R}_4 , sauf à contredire le fait que \mathcal{R}_1 est une courbe de réduction essentielle de x .

Le raisonnement est illustré par la figure 4 (a). Supposons que $\inf(x) = 0$ et que la première lettre de \hat{x} est σ_1 . Les seules tresses simples à 4 brins dont le brin extérieur est en première position, dont la composante intérieure commence par la lettre σ_1 et dont l'action n'augmente pas la complexité de la courbe \mathcal{R}_1 sont $\sigma_2\sigma_1\sigma_2$, $\sigma_2\sigma_1\sigma_2\sigma_3$ et $\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$. Les deux premières induisent σ_1 sur les brins intérieurs. Leur action transforme \mathcal{R}_1 en \mathcal{U}_4 , respectivement \mathcal{T}_3 . En vertu du lemme 6.3.7, on peut exclure $\sigma_2\sigma_1\sigma_2\sigma_3$. L'autre cas est l'image sous l'action de Δ_4 de la situation décrite au lemme 6.3.8. Dans aucun de ces cas la courbe \mathcal{R}_1 ne peut être préservée par x ni transformée en \mathcal{R}_4 .

Ainsi, la seule possibilité restante est $\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$, dont la tresse intérieure est $\sigma_1\sigma_2$. L'action de cette tresse transforme \mathcal{R}_1 en \mathcal{R}_4 . Selon la discussion que nous venons de mener, le facteur suivant dans la forme normale de x doit être $\tau(\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3) = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ (puisque $\mathcal{R}_4 = \mathcal{R}_1^\Delta$). Cet élément simple a pour tresse intérieure $\sigma_2\sigma_1$ et son action sur \mathcal{R}_4 fournit la courbe \mathcal{R}_1 . Ainsi, la tresse x doit consister en une succession des facteurs $\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$ et $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ alternativement. Mais alors x préserve des courbes rondes (les deux cercles entourant respectivement les trous 1 et 2 et les trous 3 et 4) qui ont une intersection non vide avec la courbe \mathcal{R}_1 . Cela achève la preuve de notre affirmation. \square

AFFIRMATION 6.3.14. Supposons que la courbe \mathcal{R}_2 est une courbe de réduction essentielle pour x . Alors la première lettre de $\Delta_3^{-\inf(x)}\hat{x}$ est

$$\begin{cases} \sigma_1 & \text{si } \inf(x) \text{ est pair,} \\ \sigma_2 & \text{si } \inf(x) \text{ est impair.} \end{cases}$$

DÉMONSTRATION. Il s'agit de prouver que si $\inf(x) = 0$ et la première lettre de \hat{x} est σ_2 , alors la courbe \mathcal{R}_2 ne peut pas être préservée par x (ni envoyée sur \mathcal{R}_3) à moins de ne pas être essentielle.

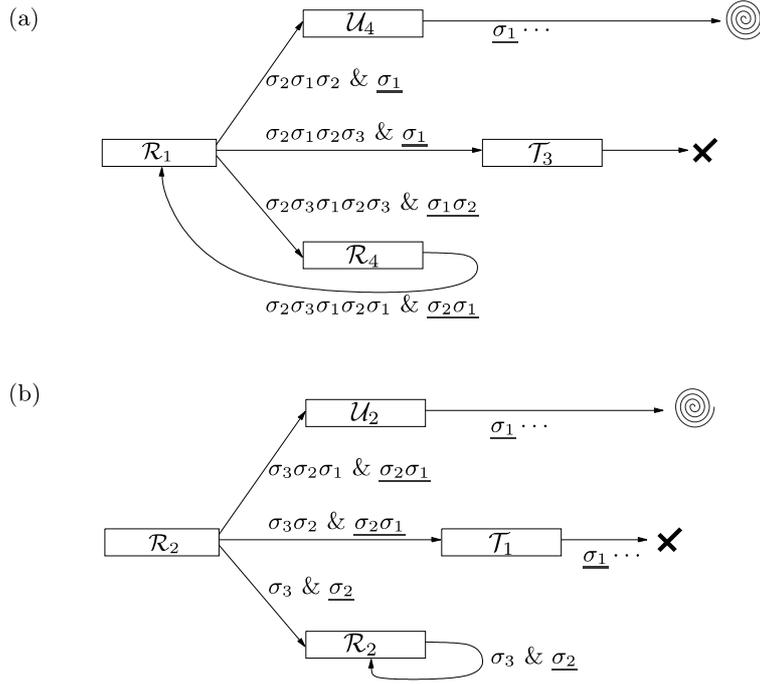


FIGURE 4. (a) Les tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_1 agissant sur \mathcal{R}_1 . (b) Les tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_2 agissant sur \mathcal{R}_2 . Les lettres soulignées désignent les facteurs intérieurs. Les croix en gras indiquent des courbes de complexité strictement supérieure à 2. Les facteurs dont l'action fournit immédiatement des courbes de complexité strictement supérieure à 2 ne sont pas représentés. La spirale dans la partie (a) renvoie à la figure 3 (a) (après l'action de Δ), celle de la Partie (b) à la figure 3 (b).

La figure 4(b) illustre la démonstration. Les seules tresses simples à 4 brins dont la composante intérieure commence par la lettre σ_2 et dont l'action n'augmente pas la complexité de la courbe \mathcal{R}_2 sont σ_3 , $\sigma_3\sigma_2$ et $\sigma_3\sigma_2\sigma_1$. La première a pour tresse intérieure σ_2 , les deux autres $\sigma_2\sigma_1$.

L'action de $\sigma_3\sigma_2$ et $\sigma_3\sigma_2\sigma_1$ transforme \mathcal{R}_2 en \mathcal{T}_1 et \mathcal{U}_2 , respectivement. Le Lemme 6.3.7 exclut $\sigma_3\sigma_2$ et en vertu du lemme 6.3.8, la tresse x ne peut préserver la courbe \mathcal{R}_2 ni la transformer en \mathcal{R}_3 si le premier facteur de $\Delta^{-\text{inf}(x)}$ est $\sigma_3\sigma_2\sigma_1$.

Enfin, si le premier facteur est σ_3 (avec facteur intérieur σ_2), la courbe \mathcal{R}_2 est invariante sous l'action de ce facteur et dans ce cas, x préserve \mathcal{R}_2 si et seulement si $x = \Delta^{\text{inf}(x)}\sigma_3^m$, pour un certain entier naturel m . Dans ce cas, x préserve une courbe ronde (i.e. le cercle entourant les trous numérotés 2,3 et 4) dont l'intersection avec \mathcal{R}_2 n'est pas vide. Cela termine la preuve de notre affirmation. \square

A cause des Affirmations 6.3.13 et 6.3.14, la dernière lettre de \hat{x} est déterminée puisque \hat{x} est rigide et on peut conclure exactement comme dans la preuve du lemme 6.3.8. Cela achève la preuve du lemme 6.3.12. \square

Les 4 lemmes précédents impliquent le lemme 6.3.6; puisque nous avons une description exhaustive des courbes de complexité 2 de \mathbb{D}_4 entourant 3 trous, cela prouve la proposition 6.2.1.

Pour conclure ce chapitre, nous donnons maintenant quelques exemples en lien avec la proposition 6.2.1. Les exemples en question ont été obtenus à l'aide de [37].

Le cas des courbes presque-rondes dans la proposition 6.2.1 ne peut pas être omis ; il existe des tresses réductibles à 4 brins dans leur Super Summit Set qui préservent une courbe de réduction essentielle presque-ronde entourant trois trous.

EXEMPLE 6.3.15. Considérons la tresse

$$x = \sigma_1 \sigma_2 \sigma_3 \sigma_2 \cdot \sigma_2 \sigma_1 \sigma_3 \cdot \sigma_3 \sigma_1 \cdot \sigma_3 \sigma_2 \sigma_1 \cdot \sigma_1 \in B_4,$$

qui est ainsi écrite en forme normale. Alors $x \in SSS(x)$ et x préserve une courbe de réduction essentielle entourant 3 trous. Voir figure 5(a).

Des exemples similaires existent avec des courbes de réduction entourant 2 trous :

EXEMPLE 6.3.16. Soit $y \in B_4$ donnée par

$$y = \sigma_2 \sigma_3 \sigma_1 \cdot \sigma_1 \sigma_2 \sigma_3 \sigma_2 \cdot \sigma_2 \cdot \sigma_2 \sigma_3.$$

Alors y est un élément de son propre SSS , n'a pas de courbe de réduction ronde, et préserve une courbe de réduction presque-ronde entourant 2 trous. Voir figure 5(b).

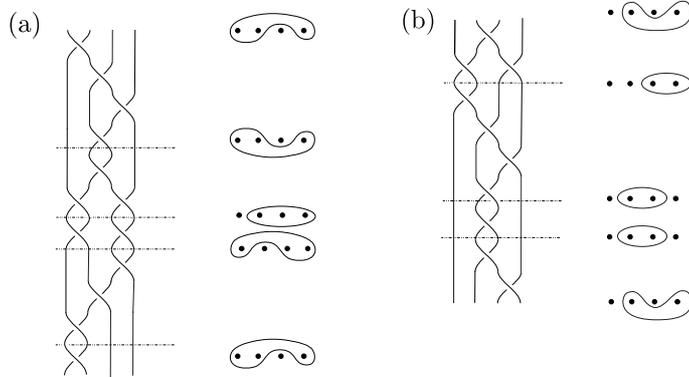


FIGURE 5. Les tresses x et y et leurs courbes de réduction essentielles. Les traits pointillés séparent les différents facteurs de la forme normale.

Enfin, nous conjecturons que l'on peut étendre les techniques de la présente section pour démontrer l'analogie de la proposition 6.2.1 pour des courbes entourant 2 trous, évitant ainsi le recours au groupe modulaire de la sphère \mathbb{S}_5 . Toutefois, les courbes de complexité 2 entourant 2 trous sont plus nombreuses que celles entourant 3 trous, rendant ainsi le raisonnement encore plus compliqué et technique.

Le problème de réductibilité et la propriété de borne linéaire

Dans ce chapitre, nous faisons entrer en jeu le théorème 1.3.5. Ce résultat d'une très grande importance va nous permettre de démontrer, dans le cas des tresses rigides pseudo-Anosov, la Conjecture 2.3.9 (c'est l'objet de la section 7.1). A l'aide d'un résultat de Birman, Gebhardt et González-Meneses sur les tresses pseudo-Anosov, nous en déduisons dans la section 7.2 un nouvel algorithme pour résoudre le problème de réductibilité dans B_n , suivant l'article [12]. Notre algorithme est de complexité quadratique par rapport à la longueur, pour tout n fixé. Toutefois, nous devons constater que la constante apparaissant dans l'énoncé du théorème 1.3.5 n'est pas explicitement connue (même dans le cas des groupes de tresses). Ainsi l'algorithme que nous développons ne peut être implémenté effectivement pour le moment ; le théorème 7.2.1 est seulement un résultat d'existence, dans l'état actuel des connaissances.

7.1. La borne linéaire sur les éléments conjugués

Dans la suite, nous supposons qu'une des structures de Garside classique ou duale de B_n a été fixée. Rappelons de la section 2.1 que pour $x \in B_n$, $|x|$ est la longueur de x par rapport à l'ensemble des éléments simples (c'est à dire la longueur de sa forme canonique mixte). La présente section est consacrée à la démonstration du résultat suivant :

THÉORÈME 7.1.1. *Il existe une constante $C(n)$ (qui dépend seulement de n et de la structure de Garside choisie) telle que pour toute tresse $x \in SSS(x)$ pseudo-Anosov on a l'équivalence suivante : x a un conjugué rigide si et seulement si $\mathfrak{s}^{C(n) \cdot |x|}(x)$ est rigide.*

Nous observons que cela donne une preuve partielle de la Conjecture 2.3.9, comme nous l'avions annoncé. Etant donné une tresse x pseudo-Anosov admettant un conjugué rigide et telle que $x \in SSS(x)$, le théorème 7.1.1 garantit qu'un conjugué rigide (ou de manière équivalente un élément de $SC(x)$) est trouvé après seulement $C(n) \cdot |x|$ itérations de l'opération \mathfrak{s} . Autrement dit, si une tresse pseudo-Anosov (dans son Super Summit Set) a des conjugués rigides, alors le glissement cyclique converge vers l'un d'eux en temps linéaire par rapport à la longueur de la tresse.

La preuve du théorème 7.1.1 repose sur deux résultats importants. Le premier d'entre eux est la propriété de borne linéaire sur les éléments conjugués dans le groupe modulaire (Théorème 1.3.5). Comme nous l'avons mentionné, la preuve du théorème 1.3.5 repose sur la classification de Nielsen-Thurston et a été établie en deux parties : la plus récente dans le cas réductible et périodique, due à Jing Tao, complète le travail de Masur et Minsky [44] où seuls les éléments pseudo-Anosov étaient considérés. Nous ne faisons pas usage de toute la généralité de ce résultat : seul le cas pseudo-Anosov va être utilisé. De plus, comme nous sommes intéressés spécialement par les groupes de tresses, nous reformulons une version restreinte du théorème 1.3.5 adaptée à nos desseins :

THÉORÈME 7.1.2. ([44], Theorem 7.2). *Soit \mathcal{G} un système de générateurs du groupe modulaire $Mod(\mathbb{S}_{n+1})$. Il existe une constante $\gamma(\mathcal{G})$, qui dépend seulement de \mathcal{G} , telle que deux éléments pseudo-Anosov conjugués de $Mod(\mathbb{S}_{n+1})$ peuvent l'être par un élément w satisfaisant*

$$|w|_{\mathcal{G}} \leq \gamma(\mathcal{G})(|x|_{\mathcal{G}} + |y|_{\mathcal{G}}),$$

(où $|\cdot|_{\mathcal{G}}$ est la longueur des mots par rapport au système générateur \mathcal{G}).

Nous en déduisons un résultat analogue pour les groupes de tresses. Nous l'énonçons à l'aide du système générateur que constituent les éléments simples de la structure de Garside choisie, mais le résultat est vrai, à l'instar du théorème 7.1.2, pour tout système générateur.

PROPOSITION 7.1.3. ¹ *Il existe une constante $c(n)$, qui dépend seulement de n et de la structure de Garside choisie, telle que deux tresses pseudo-Anosov à n brins conjuguées peuvent l'être par un élément $w \in B_n$ satisfaisant*

$$|w| \leq c(n)(|x| + |y|).$$

DÉMONSTRATION. Nous rappelons que B_n/ZB_n est isomorphe au groupe modulaire du disque \mathbb{D}_n . Pour une tresse $x \in B_n$, notons \hat{x} son image dans le quotient B_n/ZB_n . L'ensemble des éléments simples induit une mesure de longueur des éléments du quotient B_n/ZB_n que nous notons $\|\cdot\|$ (remarquons que pour toute tresse x , $\|\hat{x}\| \leq |x|$). Rappelons aussi que B_n/ZB_n est un sous-groupe d'indice $n+1$ de $Mod(\mathbb{S}_{n+1})$, le sous-groupe des éléments qui fixent l'un des trous. Le groupe $Mod(\mathbb{S}_{n+1})$ est muni d'un système de générateurs \mathcal{G}_n qui contient exactement les éléments simples (ou plus précisément leurs projections dans le quotient B_n/ZB_n) et une rotation d'angle $\frac{2\pi}{n+1}$ (remarquons que pour tout $u \in B_n/ZB_n$, on a $|u|_{\mathcal{G}_n} \leq \|u\|$). Dans ce contexte, l'inclusion $B_n/ZB_n \hookrightarrow \mathcal{MCG}(\mathbb{S}_{n+1})$ est un plongement lipschitzien, i.e. il existe une constante $\kappa(n)$ (qui dépend aussi de la structure de Garside choisie pour B_n) telle que pour tout $u \in B_n/ZB_n$, l'inégalité $\|u\| \leq \kappa(n)|u|_{\mathcal{G}_n}$ est vérifiée.

Maintenant, pour tout couple de tresses à n brins pseudo-Anosov conjuguées x et y , nous connaissons un élément conjugant entre \hat{x} et \hat{y} , disons v , $v \in B_n/ZB_n$. La preuve du théorème 7.1.2 donnée dans [44] construit un élément conjugant court v' entre \hat{x} et \hat{y} dans $Mod(\mathbb{S}_{n+1})$. L'élément v' est le produit $\hat{x}^m v$, pour un entier m et par conséquent v' est en fait un élément du sous-groupe B_n/ZB_n de $Mod(\mathbb{S}_{n+1})$. De plus,

$$|v'|_{\mathcal{G}_n} \leq \gamma(\mathcal{G}_n)(|\hat{x}|_{\mathcal{G}_n} + |\hat{y}|_{\mathcal{G}_n}) \leq \gamma(\mathcal{G}_n)(\|\hat{x}\| + \|\hat{y}\|)$$

et donc

$$\|v'\| \leq \kappa(n)\gamma(\mathcal{G}_n)(\|\hat{x}\| + \|\hat{y}\|).$$

Finalement, comme $ZB_n = \langle \Delta^2 \rangle = \langle \delta^n \rangle$ et puisqu'une tresse x conjuguée à y ne peut pas être conjuguée à $\Delta^{2k}y$ pour $k \neq 0$, tout représentant de v' dans B_n conjugue x à y et on peut en choisir un, disons w , tel que $|w| = \|v'\|$. Par conséquent, la constante $c(n) = \kappa(n)\gamma(\mathcal{G}_n)$, satisfait les conclusions de la proposition 7.1.3. \square

La deuxième étape dans la preuve du théorème 7.1.1 est un résultat de la théorie de Garside. Il affirme que si un élément d'un groupe de Garside qui est dans son propre Super Summit Set possède un conjugué rigide, alors le glissement cyclique itéré est la manière la plus courte de produire un tel conjugué rigide.

THÉORÈME 7.1.4. ([33], corollaires 9 et 12) *Soit $x \in B_n$ et supposons que x est conjugué à une tresse rigide.*

- (1) *Il existe une unique tresse positive $\rho(x)$ telle que $x^{\rho(x)}$ est rigide et $\rho(x) \preceq g$ pour toute tresse positive g telle que x^g est rigide.*
- (2) *Si $y \in SSS(x)$, alors (sauf si y est déjà rigide) il existe un entier $k > 0$ tel que $\rho(y) = \prod_{i=1}^k \mathbf{p}(\mathbf{s}^{i-1}(y))$. Autrement dit, $\rho(y)$ est le produit des k éléments conjugués mis en jeu lorsqu'on applique k itérations du glissement cyclique à y .*

Nous sommes maintenant prêts pour la preuve du théorème 7.1.1, qui est un assemblage des propositions 7.1.3 et théorème 7.1.4.

1. Remerciements à Jing Tao pour son aide concernant cette proposition

DÉMONSTRATION. (Théorème 7.1.1). Soit x une tresse pseudo-Anosov telle que $x \in SSS(x)$. Supposons que x a un conjugué rigide z . En vertu de la proposition 7.1.3, il existe $w \in B_n$ tel que $z = x^w$ et $|w| \leq c(n)(|x| + |z|)$. Puisque $x, z \in SSS(x)$, on a $|x| = |z|$. Soit r le nombre de facteurs négatifs dans la forme canonique mixte de w . Soit f l'ordre de l'élément de Garside dans B_n/ZB_n ($f = 2$ pour la structure classique et $f = n$ pour la structure duale). Soit $\bar{r} \in \{1, \dots, f\}$ un entier congru à r modulo f . Posons $w' = \delta^{r+(f-\bar{r})}w$ (dans cette expression la puissance de δ est centrale). Alors w' est une tresse positive qui conjugue x à z et telle que $|w'| \leq |w| + (f - \bar{r}) \leq (2c(n) + n)|x|$ (on peut supposer que $|x| \geq 1$).

Soit k et $\rho(x) = \prod_{i=1}^k \mathfrak{p}(\mathfrak{s}^{i-1}(x))$ comme dans le théorème 7.1.4. Alors par minimalité de ρ dans le théorème 7.1.4, $\rho(x) \preceq w'$. Il s'ensuit que $|\rho(x)| \leq |w'|$. Soit q la longueur de l'élément de Garside par rapport aux atomes. Comme la tresse $\rho(x)$ est un produit de k éléments simples, on a $\frac{k}{q} \leq |\rho(x)|$. Finalement, $k \leq q \cdot (2c(n) + n)|x|$. Alors la constante $C(n) = q \cdot (2c(n) + n)$ (qui dépend seulement de n et de la structure de Garside choisie), satisfait: x a un conjugué rigide si et seulement si $\mathfrak{s}^{C(n) \cdot |x|}(x)$ est rigide (remarquons que $\mathfrak{s}^m(z) = z$ pour toute tresse rigide z et tout entier $m \in \mathbb{N}$). \square

7.2. Un nouvel algorithme pour le problème de réductibilité

Nous avons vu que l'absence d'une preuve pour la Conjecture 2.3.9 était la seule obstruction à l'obtention d'un algorithme pour résoudre le problème de réductibilité dans B_n en temps polynômial en fonction de n et l (voir section 3.4). Munis des résultats de la section 7.1, nous adaptons l'algorithme de González-Meneses et Wiest pour obtenir un algorithme quadratique par rapport à la longueur, pour n fixé. De plus, la complexité de cet algorithme est également polynômiale en n pourvu que la constante $c(n)$ de la proposition 7.1.3 soit connue explicitement et dépende polynômialement de n . Sauf mention du contraire, nous considérons la structure de Garside classique, puisque les résultats de [40] s'inscrivent dans ce cadre.

THÉORÈME 7.2.1. *Il existe un algorithme qui décide le type de Nielsen-Thurston d'une tresse à n brins x exprimée comme un produit des éléments simples et de leurs inverses avec au plus l facteurs. La complexité de cet algorithme est $O(l^2)$ pour tout n fixé.*

Pour contourner la difficulté posée par la Conjecture 2.3.9 dans l'estimation de la complexité de l'algorithme de González-Meneses et Wiest, l'idée est de ne calculer un élément de l'ensemble des circuits glissants que lorsque l'on en est "capable" en temps polynômial, c'est à dire dans le cas rigide pseudo-Anosov. Ici réside de fait tout l'inconvénient de l'algorithme subséquent : nous disposons d'une méthode pour effectuer le calcul souhaité (à savoir le glissement cyclique itéré) ainsi que d'une borne théorique (théorème 7.1.1) sur le nombre d'opérations requis mais cette borne n'est pas explicitement connue et par conséquent on ne peut pas implémenter ce calcul.

Le théorème suivant, obtenu par Birman, Gebhardt et González-Meneses via l'étude des centralisateurs d'éléments pseudo-Anosov dans B_n est la dernière pierre dans notre construction.

THÉORÈME 7.2.2. ([6], théorème 3.37) *Soit $x \in B_n$ une tresse pseudo-Anosov. Il existe un entier positif $m < \|\Delta\|^3$ tel que x^m est conjugué à une tresse rigide.*

Dans l'énoncé du théorème 7.2.2, on peut choisir la structure de Garside classique ou duale et $\|\Delta\|$ désigne ici la longueur de l'élément de Garside en fonction des atomes, pour l'une ou l'autre structure. Rappelons que pour la structure classique, $\|\Delta\| = \frac{n(n-1)}{2}$. Nous pouvons maintenant décrire l'algorithme promis par le théorème 7.2.1.

ALGORITHME 7.2.3. Pour décider le type de Nielsen-Thurston d'une tresse $x \in B_n$.

En entrée une tresse x à n brins exprimée comme un produit des éléments simples et de leurs inverses avec au plus l facteurs.

En sortie, "périodique", "réductible" ou "pseudo-Anosov".

1. Si x^{n-1} ou x^n est une puissance de Δ^2 , répondre “périodique” et STOP.
2. Pour $i = 1, \dots, \left(\frac{n(n-1)}{2}\right)^3 - 1$, calculer x^i . Appliquer itérativement le glissement cyclique à x^i jusqu’à ce que la longueur canonique n’ait pas diminué au cours des $\frac{n(n-1)}{2} - 1$ dernières itérations. Cela calcule $y_i \in SSS(x^i)$. Calculer ensuite $z_i = \mathfrak{s}^{C(n) \cdot |y_i|}(y_i)$. Si aucune des tresses z_i n’est rigide, répondre “réductible” et STOP. Sinon, soit j un entier tel que z_j est rigide.
3. Pour $k = 1, \dots, n$, tester si la tresse z_j^k préserve une courbe de réduction ronde ; appliquer l’algorithme du théorème 3.4.4 aux tresses $\Delta^{-\inf(z_j^k)} z_j^k$ et $z_j^{-k} \Delta^{\sup(z_j^k)}$. Si une courbe de réduction invariante ronde ou presque-ronde est trouvée, alors répondre “réductible” et STOP.
4. Répondre “pseudo-Anosov”.

Comme nous l’avons déjà mentionné, cet algorithme (et spécifiquement l’étape 2), n’est pas bien défini puisque la constante $C(n)$ n’est pas explicitement connue.

DÉMONSTRATION. (Théorème 7.2.1). Nous démontrons l’exactitude de chacune des étapes de l’algorithme 7.2.3 et étudions leurs complexités respectives.

La justesse de l’étape 1 a déjà été vue précédemment (section 3.1). Cette étape a un coût $O(l^2)$, pour tout n fixé.

Montrons maintenant que l’étape 2 est correcte. D’abord, en vertu du théorème 2.3.7, la tresse y_i est un élément de $SSS(x^i)$. Maintenant, si x est pseudo-Anosov, en vertu du théorème 7.2.2, au moins l’une des tresses x^i (et donc y_i) est pseudo-Anosov avec un conjugué rigide et grâce au théorème 7.1.1, au moins l’une des tresses z_i est rigide.

Calculons la complexité de l’étape 2. Rappelons que la mise en forme normale de x (respectivement x^i) est faisable en temps $O(l^2)$ (respectivement $O((li)^2) = O(l^2)$), puis chaque itération du glissement cyclique est linéaire par rapport à la longueur. Le nombre de ces itérations est aussi linéaire (en fonction de l en vertu du théorème 2.3.7) ; l’étape 2 est donc de complexité $O(l^2)$, pour tout n fixé.

La validité de l’étape 3 découle du théorème 3.4.3. Cette étape consiste à appliquer l’algorithme de [2] à au plus n tresses de longueur canonique au plus njl et l’algorithme du théorème 3.4.4 à au plus $2n$ tresses de longueur canonique au plus njl (avec j borné par $\left(\frac{n(n-1)}{2}\right)^3$). Ces deux algorithmes ont une complexité linéaire en fonction de la longueur canonique, pour tout n fixé ; l’étape 3 est donc linéaire en l , pour tout n fixé. \square

On remarque que l’algorithme 7.2.3 ne donne pas toujours les courbes de réduction des tresses réductibles (ce défaut a lieu si la réductibilité est détectée à l’étape 2).

Le problème de conjugaison des tresses à 4 brins

8.1. Énoncé des principaux résultats

Le chapitre 2 fournit des méthodes pour résoudre le problème de conjugaison (DC et RC) dans un groupe de Garside, et donc en particulier dans les groupes de tresses B_n . Malheureusement, l'algorithme 2.3.4, avec pour invariant de conjugaison l'ensemble des circuits glissants et avec les techniques les plus sophistiquées pour effectuer chacune des étapes [32] n'est pas de complexité polynômiale (ni en n ni en ℓ) dans le cas des groupes de tresses puisqu'il est nécessaire de calculer l'intégralité de l'ensemble des circuits glissants dont la taille peut dépendre exponentiellement de n et de ℓ (voir [39], proposition 5.5).

Dans [6], il est proposé une nouvelle approche pour résoudre DC et RC en temps polynômial dans les groupes de tresses. L'idée est d'utiliser la classification de Nielsen-Thurston et de résoudre DC et RC séparément pour chaque type de Nielsen-Thurston. Pour cette raison, il est important de pouvoir décider le type de Nielsen-Thurston d'une tresse donnée ainsi que d'exhiber le système de réduction canonique d'une tresse réductible en temps polynômial (Question ouverte 1 dans [6]). On peut alors utiliser le système de réduction canonique d'une tresse réductible pour "découper" cette dernière en composantes irréductibles pour lesquelles à leur tour on cherchera à résoudre DC et RC (de fait, c'est exactement ce qui a été fait au chapitre 6, dans la preuve du corollaire 6.1.2).

Une autre question importante est donc la capacité à résoudre DC et RC pour des tresses irréductibles, c'est à dire pseudo-Anosov ou périodiques. Le cas des tresses périodiques a été étudié dans [7] (théorème 1) où un algorithme de complexité $O(l^3 n^2 \log n)$ est développé pour résoudre DC et RC pour des tresses périodiques. La résolution de DC et RC pour des tresses pseudo-Anosov en temps polynômial demeure un problème ouvert. À l'aide de la propriété de borne linéaire sur un élément conjuguant deux tresses pseudo-Anosov, nous apportons une solution à ce problème dans le cas des tresses à 4 brins, complétant ainsi le corollaire 6.1.2. Le résultat suivant est l'objet principal de [14] ; le présent chapitre est dédié à sa démonstration.

THÉORÈME 8.1.1. *Il existe un algorithme qui résout DC et RC dans le groupe B_4 et dont la complexité est cubique par rapport à la longueur des entrées.*

Notre solution est basée sur l'étude de la structure de l'ensemble des circuits glissants pour la structure duale des tresses rigides pseudo-Anosov ; nous montrons que ces derniers sont "petits" :

THÉORÈME 8.1.2. *Pour tout $x \in B_4$ pseudo-Anosov rigide par rapport à la structure duale, le cardinal de $SC(x)$ pour la structure duale est borné supérieurement par $O(\ell(x)^2)$.*

Ce résultat donne une réponse partielle (dans le cas des tresses à 4 brins pseudo-Anosov) à la Question ouverte 2 dans [6] (existe-t-il un polynôme $P(n, l)$ tel que la taille de $USS(x)$, x rigide, est bornée par $P(n, \ell(x))$?) Le théorème 8.1.2 implique que l'algorithme donné dans [32] pour résoudre DC et RC a une complexité $O(\ell^3)$ lorsqu'il est appliqué à deux tresses pseudo-Anosov rigides à 4 brins de longueur canonique au plus ℓ .

La réduction du cas pseudo-Anosov au cas pseudo-Anosov rigide s'effectue à l'aide du Théorème 7.2.2 en passant aux puissances : pour toute tresse pseudo-Anosov x , il existe un entier strictement positif m tel que x^m est conjugué à une tresse rigide. De plus lorsque n est fixé, cet entier m est borné par une constante indépendante de x .

L'étape suivante dans la réduction au cas rigide est l'observation [38] qu'une tresse pseudo-Anosov admet au plus *une* racine m -ième, pour $m \in \mathbb{N}$, $m \neq 0$. Par conséquent, pour des tresses $x, y \in B_n$ pseudo-Anosov, un entier non nul $m \in \mathbb{N}$ et une tresse $z \in B_n$, les relations $x = y^z$ et $x^m = (y^m)^z$ sont équivalentes. Le seul problème restant est de produire, pour toute paire x, y de tresses pseudo-Anosov, une puissance s convenable et des conjugués rigides \bar{x} de x^s et \bar{y} de y^s .

L'existence d'un algorithme polynômial qui construit, pour une tresse pseudo-Anosov donnée, un conjugué rigide (s'il existe) et un élément conjugant est une conséquence du théorème 7.1.1. Nous en déduisons le résultat suivant, valable pour la structure classique comme pour la structure duale :

THÉORÈME 8.1.3. *Il existe un algorithme avec les propriétés suivantes:*

- en entrée, deux tresses pseudo-Anosov $x, y \in B_n$, exprimées comme des produits de longueurs au plus l des éléments simples et de leurs inverses,
- en sortie un entier s , et des tresses à n brins \bar{x}, \bar{y}, z_1 et z_2 tels que \bar{x} et \bar{y} sont rigides et satisfont $\bar{x} = (x^s)^{z_1}$ et $\bar{y} = (y^s)^{z_2}$,
- pour chaque n fixé, sa complexité est $O(l^2)$.

Nous sommes maintenant en mesure de décrire l'algorithme promis par le théorème 8.1.1.

ALGORITHME 8.1.4. Pour résoudre DC et RC dans B_4 .

ENTREE : Deux éléments x et y exprimés comme des mots de longueur au plus l dans les générateurs d'Artin.

SORTIE : si x et y sont conjugués ou non et s'ils le sont, un élément $z \in B_4$ tel que $x = y^z$.

- 1) Déterminer le type dynamique de x et y (algorithme 6.2.5). Si ce n'est pas le même, répondre " x et y ne sont pas conjugués."
- 2) Si x et y sont périodiques utiliser [7] et STOP.
- 3) Si x et y sont réductibles, utiliser le corollaire 6.1.2 et STOP.
- 4) Si x et y sont pseudo-Anosov, utiliser l'algorithme du théorème 8.1.3 pour produire $s, \bar{x}, \bar{y}, z_1, z_2$ avec les propriétés ci-dessus.
- 5) Appliquer l'algorithme 3 de [32] à \bar{x} et \bar{y} . Si \bar{x} et \bar{y} sont conjugués, l'algorithme produit aussi c tel que $\bar{x} = \bar{y}^c$. Dans ce cas répondre " x est conjugué à y par $z_2 c z_1^{-1}$." et STOP.
- 6) Répondre " x et y ne sont pas conjugués".

8.2. Etude des éléments pseudo-Anosov rigides de BKL_4

Dans cette section, nous allons prouver le théorème 8.1.2. Notre stratégie est voisine des arguments utilisés dans la preuve de la proposition 2.3.19. Il s'agit de borner le nombre de sommets du graphe $\widehat{SCG}(x)$, pour x rigide. Avant de détailler davantage la structure de la démonstration, nous introduisons quelques notations appropriées pour travailler avec les tresses duales à 4 brins.

8.2.1. Rappels sur la structure BKL_4 . Nous commençons par fixer quelques notations pour travailler avec la structure duale BKL_4 . Rappelons que BKL_4^+ est le sous-monoïde de B_4 engendré par les tresses $a_{p,q}$, $1 \leq p < q \leq 4$ (les atomes), où

$$\begin{aligned} a_{p,p+1} &= \sigma_p \text{ pour } p = 1, \dots, 3, \\ a_{1,3} &= \sigma_2^{-1} \sigma_1 \sigma_2, \\ a_{2,4} &= \sigma_3^{-1} \sigma_2 \sigma_3, \\ a_{1,4} &= \sigma_3^{-1} \sigma_2^{-1} \sigma_1 \sigma_2 \sigma_3. \end{aligned}$$

Paramétrons le disque \mathbb{D}_4 comme le disque unité dans \mathbb{C} avec les trous donnés par les points $\frac{1}{2}e^{-\frac{ik\pi}{4}}$, $k = 1, 3, 5, 7$. La représentation géométrique des éléments de BKL_4 donnée au paragraphe 2.2.2 nous conduit au type de symboles suivants : par exemple $a_{2,4}$ est noté (\swarrow) , $a_{1,4}$ est représenté par $(: |)$ et ainsi de suite. Les relations auxquelles sont sujets les générateurs $a_{p,q}$ s'écrivent alors :

$$(: |)(| :) = (| :)(: |) = (| |), \quad (\swarrow)(\swarrow) = (\swarrow)(\swarrow) = (\swarrow),$$

$$\begin{aligned} (\cdot)(\cdot) &= (\cdot)(\cdot) = (\cdot)(\cdot) = (\cdot)(\cdot), & (\cdot)(\cdot) &= (\cdot)(\cdot) = (\cdot)(\cdot) = (\cdot)(\cdot), \\ (\cdot)(\cdot) &= (\cdot)(\cdot) = (\cdot)(\cdot) = (\cdot)(\cdot), & (\cdot)(\cdot) &= (\cdot)(\cdot) = (\cdot)(\cdot) = (\cdot)(\cdot). \end{aligned}$$

L'élément de Garside s'écrit $\delta = (\square)$, et la conjugaison τ par δ correspond à une rotation d'un quart de tour dans le sens anti-horaire; c'est un automorphisme d'ordre 4. Ainsi, la partie (iii) du lemme 2.3.13 spécialisée à la structure BKL_4 nous dit que l'orbite (sous cyclage et conjugaison par δ , voir définition 2.3.12) d'une tresse rigide x contient au plus $4 \cdot \ell(x)$ éléments.

Notre argument repose principalement sur la simplicité du treillis des éléments simples de BKL_4 . Ils sont au nombre de 14 :

$$1, (\cdot), \delta.$$

Rappelons enfin que pour toute tresse positive $x \in BKL_4^+$, $\|x\|$ désigne la longueur en fonction des atomes de tout mot positif représentant x . La fonction $x \mapsto \|x\|$ s'étend en un morphisme de groupes $\lambda : B_4 \rightarrow \mathbb{Z}$ (qui envoie chaque atome sur 1). Pour $x \in BKL_4$, on appelle *poids* de x l'entier $\lambda(x)$. Remarquons que cela n'est pas spécifique aux tresses à 4 brins. Comme il a été remarqué dans ([9], paragraphe 5.2), $\lambda(\delta) = 3$ et pour les autres éléments simples non triviaux on a $\lambda(s) = 1$ ou 2. Cette remarque fournit, en plus de la longueur canonique, du supremum et de l'infimum, une quantité invariante à l'intérieur du Super Summit Set d'une tresse $x \in BKL_4$:

LEMME 8.2.1. *Soit $x \in BKL_4$. Soit $y \in SSS(x)$. Pour tout $z \in SSS(x)$, la forme normale de z contient autant de facteurs de poids 2 et autant de facteurs de poids 1 que celle de y .*

DÉMONSTRATION. Pour toute tresse $x \in BKL_4$, si k_1 est le nombre de facteurs de poids 1 et k_2 le nombre de facteurs de poids 2 dans la forme normale de x , on a $\ell(x) = k_1 + k_2$ et $\lambda(x) = 3 \inf(x) + 2k_2 + k_1$, de sorte que k_1 et k_2 sont constants dans le Super Summit Set puisque la longueur canonique, le poids et l'infimum y sont constants. \square

On a en outre la remarque suivante :

REMARQUE 8.2.2. Soient a et b deux éléments simples pour BKL_4 . Si a est de poids 2 et que δ ne divise pas le produit ab , alors $a.b$ est en forme normale.

Rappelons maintenant l'étude des *flèches minimales* et des graphes de circuits glissants menée dans la section 2.3.2. On remarque que dans la structure BKL_4 , si x est un élément rigide et $y, z \in SC(x)$, l'existence d'une flèche minimale utile s entre $y' \in O_y$ et $z' \in O_z$ équivaut à l'existence d'une flèche minimale utile de $z' \in O_z$ vers un élément de O_y . En effet, d'après la Remarque 2.3.15, une telle flèche minimale s est un préfixe *strict* de $\iota(y')$ ou de $\partial(\varphi(y'))$. Par conséquent $\lambda(s) = 1$ et on a une flèche minimale (car de poids 1) donnée par $s^{-1}\iota(y')$ (respectivement $s^{-1}\partial(\varphi(y'))$) entre z' et $\mathbf{c}(y')$ (respectivement $\tau\mathbf{d}(y')$). Chaque arête du graphe $\widetilde{SCG}(x)$ porte donc une double orientation.

8.2.2. Stratégie de la preuve du théorème 8.1.2. Selon l'hypothèse du théorème 8.1.2, nous considérons une tresse rigide x pseudo-Anosov. On remarque par une analyse exhaustive que l'hypothèse que x est pseudo-Anosov entraîne que la longueur canonique de x est strictement supérieure à 1. La preuve du théorème 8.1.2 est divisée en trois parties. La disjonction des cas repose sur l'analyse des éléments simples de BKL_4 menée dans la partie 8.2.1. Nous considérons successivement les cas suivants :

- La forme normale de x contient au moins un facteur de poids 1 et un facteur de poids 2 (voir proposition 8.2.3). (Remarquons que tous les éléments de $SC(x)$ auront la même propriété par le lemme 8.2.1).
- Il existe un élément y de $SC(x)$ tel que les facteurs distincts de δ dans la forme normale de y sont tous des éléments de $\{(\cdot), (\cdot), (\cdot), (\cdot)\}$, respectivement de $\{(\cdot), (\cdot), (\cdot), (\cdot)\}$ (voir proposition 8.2.6).

- Pour tout élément y de $SC(x)$, les facteurs distincts de δ dans la forme normale de y sont de poids 1, respectivement de poids 2, et l'un d'entre eux est (\setminus) ou (\sphericalangle) , respectivement (\downarrow) ou (\sqcap) (voir proposition 8.2.14).

Dans les deux premiers cas, l'hypothèse que x est pseudo-Anosov est superflue. Dans ces deux cas on démontre en fait une borne linéaire sur $\#SC(x)$. Le troisième cas est conceptuellement plus ardu et fournit un exemple démontrant l'optimalité de la borne quadratique.

8.2.3. Un cas particulier simple. Nous décrivons maintenant un cas particulier très simple où le théorème 8.1.2 peut être prouvé de manière élémentaire.

PROPOSITION 8.2.3. *Soit $x \in BKL_4$ une tresse rigide dont la forme normale contient au moins un facteur de poids 1 et un facteur de poids 2. Alors l'ensemble $SC(x)$ est réduit à O_x et donc $\#SC(x) \leq 4 \cdot \ell(x)$.*

La preuve de cette proposition repose sur le lemme suivant :

LEMME 8.2.4. *Soit $x \in BKL_4$ une tresse rigide dont la forme normale contient au moins un facteur de poids 1 et un facteur de poids 2. Alors pour tout $y \in SC(x)$, aucun préfixe strict de $\iota(y)$ ni de $\partial(\varphi(y))$ n'est une flèche minimale pour y .*

DÉMONSTRATION. Par le lemme 8.2.1, la forme normale de tout élément de $SSS(x)$ (et donc de $SC(x)$) contient au moins un facteur de poids 1 et un facteur de poids 2. Soit $y \in SC(x)$. Soit $\delta^p y_1 \dots y_r$ la forme normale de y . Par hypothèse, il existe $1 \leq k, l \leq r$ tels que $\lambda(y_k) = 1$ et $\lambda(y_l) = 2$. Soit t un élément simple non trivial tel que $t \prec \tau^{-p}(y_1)$ ou $t \prec \partial(y_r)$ et $y^t \in SSS(x)$. On va montrer que y^t ne peut pas être rigide. Quitte à considérer l'inverse de y , on peut supposer que $t \prec \tau^{-p}(y_1)$.

Nécessairement, $\lambda(t) = 1$ et $\lambda(y_1) = 2$ (si $\lambda(y_1) = 1$, y_1 ne peut pas avoir de préfixe strict) de sorte que l'on peut prendre $l = 1$. De plus, on peut choisir k comme le plus petit indice d'un facteur de poids 1. Ainsi, pour $1 \leq j < k$, $\lambda(y_j) = 2$. Considérons

$$y^t = t^{-1} \delta^p y_1 \dots y_r t.$$

Comme y était rigide, la paire $y_r.t$ est en forme normale. En outre, on va montrer que $\varphi(y^t) = t$. En écrivant $t_1 = \tau^p(t)$, le calcul de la forme normale de y^t se fait via $k - 1$ glissements locaux successifs:

$$(t_j^{-1} y_j) y_{j+1} = (t_j^{-1} y_j t_{j+1}) (t_{j+1}^{-1} y_{j+1}) = y'_j (t_{j+1}^{-1} y_{j+1}), \text{ pour } j = 1, \dots, k-1,$$

avec $t_{j+1} = \partial(t_j^{-1} y_j) \wedge y_{j+1}$. Pour tout $j = 1, \dots, k-1$, $t_j \neq 1$ (c'est à dire que la paire $(t_j^{-1} y_j) y_{j+1}$ n'est pas en forme normale comme écrite) car sinon on aurait $\sup(y^t) > \sup(y)$. De plus, δ n'est pas un préfixe de $t_1^{-1} y_1 \dots y_r t$. On a ainsi, $\lambda(t_j) = 1$ pour $j = 1, \dots, k-1$. Comme $\lambda(y_k) = 1$, on a aussi $t_k = y_k$ et y'_{k-1} est de poids 2. Maintenant, par la Remarque 8.2.2, la paire $y'_{k-1} \cdot y_{k+1}$ (avec $y_{k+1} = t$ si $k = r$) est en forme normale. L'affirmation $\varphi(y^t) = t$ est donc montrée.

Cela implique que y^t n'est pas rigide. En effet

$$\iota(y^t) \wedge \partial(\varphi(y^t)) = \tau^{-p}(t_1^{-1} y_1 t_2) \wedge \partial(t) = t^{-1} \iota(y) \tau^{-p}(t_2) \wedge \partial(t).$$

Ainsi, la paire $\varphi(y^t) \iota(y^t)$ n'est pas pondérée à gauche puisque $t^{-1} \iota(y)$ est un préfixe commun non trivial de $\iota(y^t)$ et $\partial(\varphi(y^t))$. La tresse y^t n'est donc pas rigide : t n'était pas une flèche minimale pour y . \square

Maintenant, la preuve de la proposition 8.2.3 découle du lemme précédent et du Lemme 2.3.13(iii) : $SC(x)$ contient une seule orbite, dont le cardinal est majoré par $4\ell(x)$.

En vertu de la proposition 8.2.3, il reste à étudier les tresses rigides dont tous les facteurs de la forme normale (sauf δ) sont de même poids. Quitte à considérer les inverses on peut se restreindre à l'étude des tresses rigides dont tous les facteurs sont de poids 1. Désormais, x est donc une tresse rigide dont tous les facteurs de la forme normale sont de poids 1. Par le lemme 8.2.1, cette

propriété sur les facteurs de la forme normale de x est invariante dans $SSS(x)$. Enfin, il résulte de notre hypothèse et de la Remarque 2.3.15 que pour tout $y \in SC(x)$, les éventuelles flèches minimales utiles pour y sont des préfixes stricts de $\partial(\varphi(y))$ (il n'existe pas de préfixe strict non trivial de $\iota(y)$ puisque $\lambda(\iota(y)) = 1$), ainsi la valence d'un sommet de $\widetilde{SCG}(x)$ est au plus 3.

Notre première observation est aussi simple qu'utile :

LEMME 8.2.5. *Supposons que la forme normale de $y \in SC(x)$ a au moins un de ses facteurs égal à $(\cdot \cdot)$ ou à $(\cdot \cdot)$. Alors le sommet O_y de $\widetilde{SCG}(x)$ est au plus bivalent.*

DÉMONSTRATION. Quitte à remplacer y par $y' \in O_y$ on peut supposer que $\varphi(y) = (\cdot \cdot)$. Mais $\partial((\cdot \cdot)) = (\cdot \cdot)$. Cet élément simple a exactement 2 préfixes stricts positifs. \square

Nous séparons notre argument en deux parties. Dans le paragraphe 8.2.4, nous étudions le cas où $SC(x)$ contient un élément ne satisfaisant pas les hypothèses du lemme 8.2.5, c'est à dire un élément dont les facteurs de la forme normale sont tous des éléments de $\{(\cdot \cdot), (1 \cdot), (\cdot \cdot), (\cdot 1)\}$; pour brièveté nous notons \mathcal{E} cet ensemble. Par contraste, le paragraphe 8.2.5 traite le cas où tous les éléments de $SC(x)$ satisfont les hypothèses du lemme 8.2.5.

8.2.4. Un élément de $SC(x)$ a tous ses facteurs dans \mathcal{E} . On suppose dans toute cette partie que $SC(x)$ contient un élément dont les facteurs de la forme normale sont tous des éléments de $\mathcal{E} = \{(1 \cdot), (\cdot \cdot), (\cdot 1), (\cdot \cdot)\}$. Sous cette hypothèse, le théorème 8.1.2 admet une preuve élémentaire. Plus précisément, on va montrer le résultat suivant :

PROPOSITION 8.2.6. *Soit $x \in BKL_4$ une tresse rigide. Supposons qu'il existe un élément y de $SC(x)$ dont tous les facteurs de la forme normale sont dans \mathcal{E} . Alors le graphe $\widetilde{SCG}(x)$ a au plus 6 sommets. Ainsi, $\#SC(x) \leq 24 \cdot \ell(x)$.*

La seconde partie de la proposition 8.2.6 découle de la première partie combinée avec le Lemme 2.3.13 (iii).

Notons que le résultat de la proposition 8.2.6 est assuré dès lors que l'on peut montrer, pour un certain entier non nul $m \in \mathbb{N}$, que le graphe $\widetilde{SCG}(x^m)$ a au plus 6 sommets. En effet, puisque les tresses considérées sont rigides, on a une injection entre $\widetilde{SC}(x)$ et $\widetilde{SC}(x^m)$, qui à une orbite O_y associe l'orbite O_{y^m} .

Quitte à prendre x^4 au lieu de x , nous pouvons donc supposer que l'infimum de x est un multiple de 4, et de là, puisque la multiplication par une puissance $m \in \mathbb{Z}$ de δ^4 induit un isomorphisme entre $SC(x)$ et $SC(\delta^{4m}x)$, que l'infimum de x est nul.

Nous commençons par une observation sur les éléments de \mathcal{E} :

REMARQUE 8.2.7. La conjugaison par δ induit une permutation de \mathcal{E} . De plus, pour tous $s, t \in \mathcal{E}$, le produit st est en forme normale si et seulement si $t \in \{s, \tau(s)\}$.

Désormais, y est un élément de $SC(x)$ tel que tous les facteurs de la forme normale de y sont dans \mathcal{E} . Remarquons que cette propriété est alors vraie pour tout élément de O_y . La Remarque 8.2.7 nous permet de décrire la forme normale de y de manière précise :

LEMME 8.2.8. *Soit $y \in BKL_4$ une tresse rigide dont tous les facteurs sont dans \mathcal{E} et dont l'infimum est nul. Alors quitte à remplacer y par un autre élément de O_y bien choisi, la forme normale de y est de la forme*

$$y = \prod_{j=1}^r \tau^{-r+j} \left((1 \cdot)^{k_j} \right),$$

où les $k_j, j = 1, \dots, r$ sont des entiers strictement positifs et $r = 1$ ou $r \equiv 0 \pmod{4}$.

DÉMONSTRATION. Quitte à conjuguer y par une puissance de δ , on peut supposer $\varphi(y) = (1 \cdot)$. Par la Remarque 8.2.7 et notre hypothèse sur y , la forme normale de y est bien un produit de la forme

$$y = \tau^{-(r-1)} \left((1 \cdot)^{k_1} \right) \dots (1 \cdot)^{k_r}$$

pour des entiers $r > 0$ et k_1, \dots, k_r strictement positifs. Ensuite, à cause de la rigidité et par la Remarque 8.2.7, on a $\iota(y) = \varphi(y)$ ou $\iota(y) = \tau(\varphi(y))$. Supposons que $r > 1$. Quitte à cycler, on peut supposer $\iota(y) = \tau(\varphi(y))$, soit $\tau^{-r+1}((1 \cdot)) = \tau((1 \cdot))$. Cela implique $r \equiv 0 \pmod{4}$. \square

LEMME 8.2.9. *Si $r = 1$ dans le lemme 8.2.8, alors $\#SC(x) = 6$.*

DÉMONSTRATION. On a en effet :

$$SC(x) = \{(1 \cdot)^{k_1}, (\overleftarrow{\cdot})^{k_1}, (\cdot 1)^{k_1}, (\overleftarrow{\cdot})^{k_1}, (\overrightarrow{\cdot})^{k_1}, (\overleftarrow{\cdot})^{k_1}\}.$$

\square

LEMME 8.2.10. *Si $r > 1$ dans le lemme 8.2.8, alors il existe une flèche minimale pour y si et seulement si $r \equiv 0 \pmod{3}$. Dans ce cas, y admet trois flèches minimales. Sinon, le graphe $\widetilde{SCG}(x)$ comporte un seul sommet.*

DÉMONSTRATION. Selon notre hypothèse, $r \equiv 0 \pmod{4}$ d'après le lemme 8.2.8 et on peut réécrire

$$y = \prod_{j=1}^m \left((\overleftarrow{\cdot})^{k_{j,1}} (\cdot 1)^{k_{j,2}} (\overleftarrow{\cdot})^{k_{j,3}} (1 \cdot)^{k_{j,4}} \right) := \prod_{j=1}^m \alpha_j,$$

avec $m := \frac{r}{4}$ et $k_{j,i} > 0$ pour tous $1 \leq j \leq m$ et $1 \leq i \leq 4$. Les éventuelles flèches minimales utiles pour y sont les préfixes stricts de $\partial((1 \cdot))$, à savoir $(\overleftarrow{\cdot})$, $(\cdot 1)$ et $(\overrightarrow{\cdot})$.

La preuve du lemme réside essentiellement dans les calculs suivants, où les membres de droite (à l'exception de leur premier facteur), c'est à dire A_j , B_j et C_j , sont des formes normales, indépendamment des puissances mises en jeu dans les formules (rappelons que pour $j = 1, \dots, m$, $\alpha_j = (\overleftarrow{\cdot})^{k_{j,1}} (\cdot 1)^{k_{j,2}} (\overleftarrow{\cdot})^{k_{j,3}} (1 \cdot)^{k_{j,4}}$) :

$$\alpha_j(\overleftarrow{\cdot}) = (\overrightarrow{\cdot}) \left((\overleftarrow{\cdot}) (\overrightarrow{\cdot})^{k_{j,1}-1} (\cdot 1)^{k_{j,2}} (\overleftarrow{\cdot}) (1 \cdot)^{k_{j,3}} (\overleftarrow{\cdot})^{k_{j,4}-1} \right) := (\overrightarrow{\cdot}) A_j,$$

$$\alpha_j(\overrightarrow{\cdot}) = (\cdot 1) \left((\overleftarrow{\cdot}) (\cdot 1)^{k_{j,1}} (\overleftarrow{\cdot})^{k_{j,2}-1} (\overleftarrow{\cdot})^{k_{j,3}} (1 \cdot)^{k_{j,4}} (\overleftarrow{\cdot})^{k_{j,4}-1} \right) := (\cdot 1) B_j,$$

$$\alpha_j(\cdot 1) = (\overleftarrow{\cdot}) \left((\overleftarrow{\cdot})^{k_{j,1}} (\cdot 1) (\overleftarrow{\cdot})^{k_{j,2}} (\overrightarrow{\cdot})^{k_{j,3}-1} (1 \cdot)^{k_{j,4}} \right) := (\overleftarrow{\cdot}) C_j.$$

On remarque que, indépendamment de j et des puissances mises en jeu, les "paires" $A \cdot C$, $B \cdot A$ et $C \cdot B$ sont en forme normale. Cela montre que si $r \equiv 1$ ou $r \equiv 2 \pmod{3}$ et pour tout $u \prec \partial((1 \cdot))$, $u \not\prec yu$ de sorte que $y^u \notin SSS(x)$. De plus, cela implique aussi que pour $m \equiv 0 \pmod{3}$, les trois tresses

$$y^{(\overleftarrow{\cdot})} = \left(\prod_{j=1}^{\frac{m}{3}} \alpha_{3j-2} \alpha_{3j-1} \alpha_{3j} \right)^{(\overleftarrow{\cdot})} = \prod_{j=1}^{\frac{m}{3}} C_{3j-2} B_{3j-1} A_{3j},$$

$$y^{(\cdot 1)} = \prod_{j=1}^{\frac{m}{3}} B_{3j-2} A_{3j-1} C_{3j} \quad \text{et} \quad y^{(\overrightarrow{\cdot})} = \prod_{j=1}^{\frac{m}{3}} A_{3j-2} C_{3j-1} B_{3j}$$

sont rigides. \square

On suppose désormais que $r \equiv 0 \pmod{3}$ (et selon notre précédente hypothèse $r \equiv 0 \pmod{12}$); cela est toujours vérifié quitte à prendre une puissance de x . Soit $u \prec \partial((:))$. Il découle de la preuve du lemme 8.2.10 que l'on peut toujours trouver, quitte à permuter cycliquement les facteurs, un élément de O_{y^u} de la forme

$$z = \prod_{j=1}^{\frac{m}{3}} C_{3j-2} B_{3j-1} A_{3j},$$

en choisissant convenablement les indices et les puissances à l'intérieur des facteurs.

On peut alors réécrire y sous la forme

$$y = \prod_{\nu=1}^{\frac{m}{3}} (:)^{a_\nu} (:1)^{b_\nu} (\overleftarrow{:})^{c_\nu} (1:)^{d_\nu} (\overleftarrow{:})^{e_\nu} (:1)^{f_\nu} (\overleftarrow{:})^{g_\nu} (1:)^{h_\nu} (\overleftarrow{:})^{i_\nu} (:1)^{j_\nu} (\overleftarrow{:})^{k_\nu} (1:)^{l_\nu},$$

avec des entiers $a_\nu, b_\nu, \dots, l_\nu$ strictement positifs pour tout $\nu = 1, \dots, \frac{m}{3}$, et z devient

$$z = \prod_{\nu=1}^{\frac{m}{3}} (:)^{a_\nu} (:1)^{b_\nu} (\overleftarrow{:})^{c_\nu-1} (1:)^{d_\nu} (\overleftarrow{:})^{e_\nu} (:1)^{f_\nu-1} (\overleftarrow{:})^{g_\nu} (1:)^{h_\nu} (\overleftarrow{:})^{i_\nu-1} (:1)^{j_\nu} (\overleftarrow{:})^{k_\nu} (\overleftarrow{:})^{l_\nu-1}.$$

LEMME 8.2.11. *Si la forme normale de z contient un facteur $(\overleftarrow{:})$ ou $(\overleftarrow{:})$, alors z admet une unique flèche minimale utile, autrement dit le sommet O_z de $\widetilde{SCG}(x)$ est un point extrêmeal.*

DÉMONSTRATION. Quitte à cycler ou conjuguer par δ on peut supposer que le dernier facteur de z est $(\overleftarrow{:})$, et $l_{\frac{m}{3}} > 1$. Les flèches minimales pour z sont au maximum 2 : $(:1)$ et $(1:)$. Un calcul de forme normale montre que $(1:) \not\prec z(1:)$, et donc $z \stackrel{(1:)}{\prec} \notin SSS(x)$, ce qui prouve le lemme. On a en effet

$$(\overleftarrow{:})^{l_\nu-1} (1:) = (\overleftarrow{:})(\overleftarrow{:})^{l_\nu-2}.$$

Puis, pour des entiers $a, b > 0$ quelconques,

$$\left((:1)^a (\overleftarrow{:}) (1:)^b \right) (\overleftarrow{:}) = (1:) \left((:1)^a (\overleftarrow{:}) (1:) (\overleftarrow{:})^{b-1} \right).$$

Notons que le premier facteur dans le membre de droite est indépendant des entiers mis en jeu. De plus, la paire $(\overleftarrow{:})(1:)$ est en forme normale. Ainsi, la dernière ligne de calcul se transporte vers la gauche le long de la forme normale de z jusqu'à rencontrer un éventuel facteur $(\overleftarrow{:})$ ou $(\overleftarrow{:})$ (chaque déplacement est en outre accompagné d'une conjugaison par δ).

Cela montre que la multiplication de z par $(1:)$ à droite ne peut modifier le début de la forme normale de z que si $(\overleftarrow{:})^{l_{\frac{m}{3}}-1}$ est la seule occurrence de $(\overleftarrow{:})$ ou $(\overleftarrow{:})$ dans z (et dans ce cas, le facteur initial de $z(1:)$ est $(\overleftarrow{:})$). Ceci achève la démonstration. \square

LEMME 8.2.12. *Supposons que la forme normale de z ne contient pas de facteur $(\overleftarrow{:})$ ou $(\overleftarrow{:})$.*

- (i) *Les trois préfixes stricts de $\partial(\varphi(z))$ sont des flèches minimales pour z ,*
- (ii) *si v est une flèche minimale utile pour z qui conjugue z vers une tresse rigide dont la forme normale ne contient aucun facteur $(\overleftarrow{:})$ ou $(\overleftarrow{:})$, alors $z^v \in O_y$ et $v = (:1)$.*

DÉMONSTRATION. Notre hypothèse permet, au vu des formules dans la preuve du Lemme 8.2.10, de réécrire

$$y = \prod_{\nu=1}^{\frac{m}{3}} (:)^{a_\nu} (:1)^{b_\nu} (\overleftarrow{:}) (1:)^{d_\nu} (\overleftarrow{:})^{e_\nu} (:1)^{f_\nu} (\overleftarrow{:})^{g_\nu} (1:)^{h_\nu} (\overleftarrow{:}) (1:)^{j_\nu} (\overleftarrow{:})^{k_\nu} (1:)$$

et

$$z = \prod_{\nu=1}^{\frac{m}{3}} (\overleftarrow{\cdot})^{a_\nu} (\cdot \overrightarrow{\cdot})^{b_\nu} (\overleftarrow{\cdot})^{d_\nu} (\overleftarrow{\cdot})^{e_\nu} (\overleftarrow{\cdot})^{g_\nu} (\overleftarrow{\cdot})^{h_\nu} (\cdot \overrightarrow{\cdot})^{j_\nu} (\overleftarrow{\cdot})^{k_\nu}.$$

(i) En vertu du lemme 8.2.10, z admet trois flèches minimales.

(ii) Soit v une flèche minimale utile pour z telle que z^v ne contient aucun facteur $(\overleftarrow{\cdot})$ ou $(\cdot \overrightarrow{\cdot})$. Remarquons qu'une telle flèche existe puisque $O_y \neq O_z$. On sait que $v \in \{(\overleftarrow{\cdot}), (\cdot \overrightarrow{\cdot}), (\overleftarrow{\cdot})\}$. En vertu des formules données dans la preuve du lemme 8.2.10 l'hypothèse $v = (\overleftarrow{\cdot})$ implique, puisque z^v ne contient pas de facteur $(\overleftarrow{\cdot})$ ni $(\cdot \overrightarrow{\cdot})$, les égalités $b_\nu = 1, e_\nu = 1, h_\nu = 1, k_\nu = 1$. Mais alors $z = z^{(\overleftarrow{\cdot})}$, ce qui contredit l'utilité de v donc $v \neq (\overleftarrow{\cdot})$.

De manière analogue, en supposant $v = (\cdot \overrightarrow{\cdot})$, on a au vu des formules dans la preuve du Lemme 8.2.10, $a_\nu = 1, d_\nu = 1, g_\nu = 1, j_\nu = 1$. Mais alors

$$z = \prod_{\nu=1}^{\frac{m}{3}} (\overleftarrow{\cdot})^{a_\nu} (\cdot \overrightarrow{\cdot})^{b_\nu} (\overleftarrow{\cdot})^{d_\nu} (\overleftarrow{\cdot})^{e_\nu} (\overleftarrow{\cdot})^{g_\nu} (\overleftarrow{\cdot})^{h_\nu} (\cdot \overrightarrow{\cdot})^{j_\nu} (\overleftarrow{\cdot})^{k_\nu}$$

et

$$z^{(\overleftarrow{\cdot})} = \prod_{\nu=1}^{\frac{m}{3}} (\overleftarrow{\cdot})^{a_\nu} (\cdot \overrightarrow{\cdot})^{b_\nu} (\overleftarrow{\cdot})^{d_\nu} (\overleftarrow{\cdot})^{e_\nu} (\overleftarrow{\cdot})^{g_\nu} (\overleftarrow{\cdot})^{h_\nu} (\cdot \overrightarrow{\cdot})^{j_\nu} (\overleftarrow{\cdot})^{k_\nu - 1}.$$

En d'autres termes, $\mathbf{c}(z^{(\overleftarrow{\cdot})}) = \tau(z)$. L'utilité de v implique $v \neq (\overleftarrow{\cdot})$. Donc $v = (\cdot \overrightarrow{\cdot})$ et $z^v \in O_y$. \square

Le lemme 8.2.12 prouve que le graphe $\widetilde{SCG}(x)$ ne peut pas contenir une chaîne de 3 sommets dont les éléments s'écrivent sans facteur $(\overleftarrow{\cdot})$ ni $(\cdot \overrightarrow{\cdot})$. Par le lemme 8.2.11, tous les autres sommets (i.e. ceux dont les éléments s'écrivent avec au moins un facteur $(\overleftarrow{\cdot})$ ou $(\cdot \overrightarrow{\cdot})$) sont monovalents. Le nombre de sommets dans $\widetilde{SCG}(x)$ est donc borné par 6. Cela achève la preuve de la Proposition 8.2.6.

8.2.5. Tous les éléments de $SC(x)$ ont au moins un facteur qui n'est pas dans \mathcal{E} .

Dans cette partie on suppose que tous les éléments de $SC(x)$ ont au moins un facteur de leur forme normale égal à $(\overleftarrow{\cdot})$ ou $(\cdot \overrightarrow{\cdot})$. D'après le lemme 8.2.5, le graphe $\widetilde{SCG}(x)$ est alors une ligne (éventuellement fermée). En vue de prouver le théorème 8.1.2, nous cherchons à borner la longueur de cette ligne, c'est à dire le nombre de sommets dans le graphe $\widetilde{SCG}(x)$. La tâche n'est pas si aisée qu'au précédent paragraphe et nous n'avons pas de démonstration élémentaire du théorème 2 sous les présentes hypothèses. A titre d'indication, nous montrons d'abord que la borne quadratique du théorème 8.1.2 est optimale. L'exemple suivant a été obtenu à l'aide du programme GAP [47] :

EXEMPLE 8.2.13. Pour tout $k \in \mathbb{N}$, la tresse

$$\beta_k = (\overleftarrow{\cdot})(\cdot \overrightarrow{\cdot})(\overleftarrow{\cdot})(\overleftarrow{\cdot})(\cdot \overrightarrow{\cdot})(\cdot \overrightarrow{\cdot})^k.$$

est rigide (pseudo-Anosov) avec $\ell(\beta_k) = 3k+5$. De plus, pour tout entier $k \in \mathbb{N}$, le graphe $\widetilde{SCG}(\beta_k)$ est une ligne (non fermée) avec $3k+2$ sommets et $\#SC(\beta_k) = 4 \cdot (3k+2) \cdot (3k+5)$.

La preuve du théorème 8.1.2 sous les présentes hypothèses repose sur le théorème de borne linéaire sur la longueur d'un élément conjuguant deux tresses pseudo-Anosov. En particulier la proposition 7.1.3 nous dit qu'il existe une constante c telle que pour toute paire de tresses pseudo-Anosov à 4 brins conjuguées z_1 et z_2 , on peut trouver un élément w les conjugant satisfaisant $|w| \leq c \cdot (|z_1| + |z_2|)$.

Nous sommes maintenant prêts pour achever la preuve du théorème 8.1.2.

PROPOSITION 8.2.14. Soit $x \in BK L_4$ une tresse pseudo-Anosov rigide. Supposons que tous les éléments de $SC(x)$ ont au moins un facteur de leur forme normale égal à $(\overleftarrow{\cdot})$ ou $(\cdot \overrightarrow{\cdot})$. Alors, le graphe $\widetilde{SCG}(x)$ a au plus $16 \cdot c \cdot \ell(x)$ sommets. Ainsi, $\#SC(x) \leq 64 \cdot c \cdot \ell(x)^2$.

DÉMONSTRATION. D'abord, on peut supposer que $|x| \leq 2 \cdot \ell(x)$. En effet, quitte à multiplier x par une puissance de l'élément central δ^4 , on obtient des graphes isomorphes $\widetilde{SCG}(x)$ et $\widetilde{SCG}(\delta^{4m}x)$, pour tout entier m . De cette façon on peut supposer que $\inf(x) \in \{-3, -2, -1, 0\}$. Alors on a $|x| \leq 2 \cdot \ell(x)$ (rappelons que $\ell(x) > 1$, puisque x est pseudo-Anosov).

On observe que d'après le lemme 8.2.5, chaque sommet de $\widetilde{SCG}(x)$ est au plus bivalent donc topologiquement, $\widetilde{SCG}(x)$ est soit un segment de ligne, soit un cercle. Nous affirmons que deux sommets quelconques O_a, O_b distincts dans le graphe $\widetilde{SCG}(x)$ sont reliés dans $\widetilde{SCG}(x)$ par un chemin de longueur au plus $8 \cdot c \cdot \ell(x)$ et nous notons que cette affirmation (et le lemme 2.3.13 (iii)) impliquent la proposition (le facteur 2 vient de l'éventualité où $\widetilde{SCG}(x)$ forme un cercle).

Soient donc O_a et O_b deux sommets distincts de $\widetilde{SCG}(x)$ ainsi que z_a et z_b des représentants respectifs de ces orbites. En vertu de la proposition 7.1.3, il existe une tresse w satisfaisant $z_a^w = z_b$ et $|w| \leq 2 \cdot c \cdot |x| \leq 4 \cdot c \cdot \ell(x)$. On peut supposer que $\inf(w) = 0$, quitte à prendre un autre représentant z_a . Alors $\lambda(w) \leq 2 \cdot |w|$ (chaque facteur de la forme normale de w contribue au plus 2 au poids de w) et w est le produit d'au plus $2 \cdot |w|$ flèches minimales, ce qui donne un chemin de longueur au plus $2 \cdot |w|$ entre O_a et O_b dans le graphe $\widetilde{SCG}(x)$. \square

REMARQUE 8.2.15. La Question ouverte 2 dans [6] concerne l'existence d'une borne polynômiale en n et ℓ sur le cardinal du Ultra Summit Set d'une tresse rigide (pseudo-Anosov) avec n brins et de longueur au plus ℓ . Prasolov a donné une réponse négative en exhibant une famille de tresses pseudo-Anosov rigides dont la taille du Ultra Summit set croît exponentiellement en fonction de n (pour les deux structures, duale et classique). En revanche, si on fixe n , de tels contre-exemples ne sont pas connus. Le théorème 8.1.2 donne une réponse positive dans le cadre dual lorsque $n = 4$. Nous formulons donc la question suivante : étant fixé un entier naturel n , existe-t-il un polynôme P_n tel que le cardinal du USS (classique ou dual) d'une tresse rigide pseudo-Anosov à n brins est borné supérieurement par $P_n(\ell(x))$?

8.3. Validité des algorithmes

Dans cette section, nous prouvons les théorèmes 8.1.3 et 8.1.1. Le théorème 8.1.3 est prouvé dans un premier temps puis nous prouvons la validité de l'algorithme 8.1.4 et analysons sa complexité. Nous allons utiliser une deuxième fois la propriété de borne linéaire sur les éléments conjuguant deux pseudo-Anosov (voir proposition 7.1.3), cette fois via le théorème 7.1.1. C'est le point clé dans la démonstration du théorème 8.1.3.

DÉMONSTRATION. (Théorème 8.1.3). Notons $\beta(n)$ la borne supérieure pour m dans l'énoncé du théorème 7.2.2. Soient $x, y \in B_n$ deux tresses pseudo-Anosov. En vertu du théorème 7.2.2, il existe m_x et m_y des entiers tous deux bornés strictement par $\beta(n)$ tels que x^{m_x} et y^{m_y} sont conjugués à des tresses rigides. Pour tout $i = 1, \dots, \beta(n) - 1$, l'algorithme itère simultanément l'opération \mathfrak{s} sur x^i jusqu'à ce qu'une tresse rigide soit trouvée. La puissance i_x correspondante, ainsi qu'une tresse z_x tel que $(x^{i_x})^{z_x}$ est rigide sont alors mémorisées. Soit \tilde{x} le conjugué rigide de x^{i_x} obtenu ainsi. Le même processus appliqué à y fournit l'entier i_y , les tresses z_y et \tilde{y} avec les propriétés correspondantes. Notons que cette procédure est faisable en temps $O(l^2)$, où l est le maximum des longueurs de x et y . En effet, chacune des tresses $x^i, y^i, i = 1, \dots, \beta(n) - 1$ a sa longueur bornée par $\beta(n)\ell$. Le calcul de la forme normale est quadratique; puis chaque itération du glissement cyclique est linéaire. Enfin en vertu du théorème 2.3.7 et 7.1.1, le nombre d'itérations de l'opération \mathfrak{s} nécessaire avant de trouver \tilde{x} est linéairement borné par rapport à la longueur.

Les puissances d'une tresse rigide étant également rigides, l'entier $s = \text{ppcm}(i_x, i_y)$ satisfait x^s et y^s sont conjugués à des tresses rigides. Il suffit alors de prendre $\bar{x} = \tilde{x}^{\frac{s}{i_x}}, \bar{y} = \tilde{y}^{\frac{s}{i_y}}$ et $z_1 = z_x, z_2 = z_y$ pour satisfaire les contraintes du théorème 8.1.3. \square

DÉMONSTRATION. (Théorème 8.1.1). Nous devons prouver que l'algorithme 8.1.4 est valide et de complexité $O(l^3)$. Nous disposons déjà de tous les éléments nécessaires. Les étapes 1 et 3 sont de complexités respectives $O(l^2)$ et $O(l^3)$ en vertu des théorème 6.1.1 et corollaire 6.1.2. L'étape 2 est de complexité $O(l^2)$ (voir théorème 1 dans [7]). L'étape 4 est de complexité $O(l^2)$ en vertu du théorème 8.1.3. Finalement, le théorème 4.11 de [32] nous dit que l'algorithme 3 dans [32]) permet de résoudre DC et RC pour des tresses rigides de longueur canonique au plus l en temps $O(l \cdot \kappa)$, où κ désigne le cardinal du SC des entrées. Or, \bar{x} et \bar{y} fournis par le théorème 8.1.3 ont longueur canonique $O(l)$. En vertu du théorème 8.1.2, l'étape 5 de l'algorithme a donc complexité $O(l^3)$. De plus, en vertu de [38], la relation $\bar{x} = \bar{y}^c$ pour une tresse c (autrement dit $(x^s)^{z_1} = ((y^s)^{z_2})^c$) est équivalente à la relation $x^{z_1} = y^{z_2^c}$, soit x est conjugué à y par $z_2 c z_1^{-1}$. \square

Bibliographie

- [1] E. ARTIN, *Theorie der Zöpfe*, Abhandlungen Hamburg, 4 (1925), p. 47–72.
- [2] D. BENARDETE, M. GUTIÉRREZ ET Z. NITECKI, *Braids and the Nielsen-Thurston classification*, J. Knot Theory and Ramif., 4 (1995), p. 549–618.
- [3] M. BESTVINA ET M. HANDEL, *Train-tracks for surface homeomorphisms*, Topology, 34 (1995), p. 109–140.
- [4] J. BIRMAN, K. H. KO ET S. J. LEE, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math., 139 (1998), p. 322–353.
- [5] J. S. BIRMAN, *Braids, links, and mapping class groups*, Princeton University Press, Princeton, N.J., 1974. Annals of Mathematics Studies, No. 82.
- [6] J. S. BIRMAN, V. GEBHARDT ET J. GONZÁLEZ-MENESES, *Conjugacy in Garside groups. I. Cyclings, powers and rigidity*, Groups Geom. Dyn., 1 (2007), p. 221–279.
- [7] ———, *Conjugacy in Garside groups. III. Periodic braids*, J. Algebra, 316 (2007), p. 746–776.
- [8] ———, *Conjugacy in Garside groups. II. Structure of the ultra summit set*, Groups Geom. Dyn., 2 (2008), p. 13–61.
- [9] J. S. BIRMAN, K. H. KO ET S. J. LEE, *The infimum, supremum, and geodesic length of a braid conjugacy class*, Adv. Math., 164 (2001), p. 41–56.
- [10] J. S. BIRMAN, A. LUBOTZKY ET J. MCCARTHY, *Abelian and solvable subgroups of the mapping class group*, Duke Math. J., 50 (1983), p. 1107–1120.
- [11] E. BRIESKORN ET K. SAITO, *Artin-Gruppen und Coxeter-Gruppen.*, Invent. Math., 17 (1972), p. 245–271.
- [12] M. CALVEZ, *Fast Nielsen-Thurston classification of braids*, arXiv:1112.0165.
- [13] ———, *Dual Garside structure and reducibility of braids*, J. Algebra, 356 (2012), p. 355–373.
- [14] M. CALVEZ ET B. WIEST, *A fast solution to the conjugacy problem in the four-strand braid group*, arXiv:1204.6507.
- [15] ———, *Fast Nielsen-Thurston classification of four strand braids*, J. Knot Th. and Ramifications, 21 (2012).
- [16] A. J. CASSON ET S. A. BLEILER, *Automorphisms of surfaces after Nielsen and Thurston*, London Mathematical Society Student Texts, 9. Cambridge (UK) etc.: Cambridge University Press. 105 p. , 1988.
- [17] R. CHARNEY ET J. MEIER, *The language of geodesics for Garside groups*, Math. Z., 248 (2004), p. 495–509.
- [18] B. DE KERÉKJÁRTÓ, *Über die periodischen Transformationen der Kreisscheibe und der Kugelfläche*, Math. Ann., 80 (1919), p. 3–7.
- [19] P. DE LA HARPE, *An invitation to Coxeter groups*. Ghys, É. (ed.) et al., Group theory from a geometrical viewpoint. Proceedings of a workshop, held at the International Centre for Theoretical Physics in Trieste, Italy, 26 March to 6 April 1990. Singapore: World Scientific. 193-253 (1991)., 1991.
- [20] P. DEHORNOY, *Groupes de Garside*, Ann. Sci. Ecole Norm. Sup., 35 (2002), p. 267–306.
- [21] P. DEHORNOY, F. DIGNE, E. GODELLE, D. KRAMMER ET J. MICHEL, *Garside Theory*. In preparation.
- [22] P. DEHORNOY ET L. PARIS, *Gaussian groups and Garside groups, two generalisations of Artin groups*, Proc. Lond. Math. Soc., III. Ser., 79 (1999), p. 569–604.
- [23] S. EILENBERG, *Sur les transformations périodiques de la surface de sphère*, Fundam. Math., 22 (1934), p. 28–41.
- [24] E. A. ELRIFAI ET H. MORTON, *Algorithms for positive braids*, Q. J. Math., Oxf. II. Ser., 45 (1994), p. 479–497.
- [25] D. B. A. EPSTEIN, J. W. CANNON, D. F. HOLT, S. V. F. LEVY, M. S. PATERSON ET W. P. THURSTON, *Word processing in groups*, Jones and Bartlett Publishers, Boston, MA, 1992.
- [26] B. FARB ET D. MARGALIT, *A primer on mapping class groups*, vol. 49 de Princeton Mathematical Series, Princeton University Press, Princeton, NJ, 2012.
- [27] A. FATHI, F. LAUDENBACH ET V. POENARU, *Travaux de Thurston sur les surfaces*, vol. 66-67 de Astérisque, SMF, 1979.
- [28] R. FENN, M. GREENE, D. ROLFSEN, C. ROURKE ET B. WIEST, *Ordering the braid groups*, Pac. J. Math., 191 (1999), p. 49–74.

- [29] N. FRANCO ET J. GONZÁLEZ-MENESES, *Conjugacy problem for braid groups and Garside groups*, J. Algebra, 266 (2003), p. 112–132.
- [30] F. GARSIDE, *The braid group and other groups*, Q. J. Math., Oxf. II. Ser., 20 (1969), p. 235–254.
- [31] V. GEBHARDT, *A new approach to the conjugacy problem in Garside groups*, J. Algebra, 292 (2005), p. 282–302.
- [32] V. GEBHARDT ET J. GONZÁLEZ-MENESES, *Solving the conjugacy problem in Garside groups by cyclic sliding*, J. Symb. Comput., 45 (2010), p. 629–656.
- [33] ———, *The cyclic sliding operation in Garside groups*, Math. Z., 265 (2010), p. 85–114.
- [34] E. GODELLE, *Personal communication*.
- [35] ———, *Parabolic subgroups of Garside groups*, J. Algebra, 317 (2007), p. 1–16.
- [36] ———, *Parabolic subgroups of Garside groups. II: Ribbons*, J. Pure Appl. Algebra, 214 (2010), p. 2044–2062.
- [37] J. GONZÁLEZ-MENESES, *Logiciel Braiding*. <http://personal.us.es/meneses>.
- [38] ———, *The n th root of a braid is unique up to conjugacy*, Algebr. Geom. Topol., 3 (2003), p. 1103–1118.
- [39] J. GONZÁLEZ-MENESES, *On reduction curves and Garside properties of braids*. Cogolludo-Agustín, José Ignacio (ed.) et al., Topology of algebraic varieties and singularities. Invited papers of the conference in honor of Anatoly Libgober’s 60th birthday, Jaca, Spain, June 22–26, 2009. Providence, RI: American Mathematical Society (AMS); Madrid: Real Sociedad Matemática Española. Contemporary Mathematics 538, 227–244 (2011)., 2011.
- [40] J. GONZÁLEZ-MENESES ET B. WIEST, *Reducible braids and Garside theory*, Algebr. Geom. Topol., 11 (2011), p. 2971–3010.
- [41] T. HALL, *Logiciel “trains”*. http://www.liv.ac.uk/~tobyhall/T_Hall.html.
- [42] E.-K. LEE ET S.-J. LEE, *A Garside-theoretic approach to the reducibility problem in braid groups*, J. Algebra, 320 (2008), p. 783–820.
- [43] W. MAGNUS, *Über Automorphismen von Fundamentalgruppen berandeter Flächen*, Math. Ann, 109 (1934), p. 617–646.
- [44] H. MASUR ET Y. MINSKY, *Geometry of the complex of curves. II: Hierarchical structure*, Geom. Funct. Anal., 10 (2000), p. 902–974.
- [45] L. MOSHER, *Mapping class groups are automatic*, Ann. of Math., 142 (1995), p. 303–384.
- [46] M. PICANTIN, *Petits groupes gaussiens*, Thèse doctorat, Université de Caen, 2000.
- [47] M. SCHÖNERT ET AL. GAP-Groups, Algorithms, and Programming - version 3 release 4 patchlevel 4. Lehrstuhl D für Mathematik, Rheinische Westfälische Technische Hochschule, Aachen, Germany, 1997, package CHEVIE.
- [48] J. TAO, *Linearly bounded conjugator property for mapping class groups*. Preprint ArXiv:1106.2341.
- [49] W. P. THURSTON, *On the geometry and dynamics of diffeomorphisms of surfaces*, Bull. Amer. Math. Soc. (N.S.), 19 (1988), p. 417–431.

Problèmes algorithmiques dans les groupes de tresses

Cette thèse a pour objet de développer de nouveaux algorithmes pour les groupes de tresses. Un problème important en théorie mathématique des tresses est d'améliorer les algorithmes existants pour résoudre le problème de conjugaison. Nous résolvons complètement ce problème dans le cas du groupe des tresses à quatre brins, en exhibant un algorithme de complexité cubique en terme de la longueur des entrées. La démonstration s'appuie sur deux aspects fondamentaux des groupes de tresses : la structure de groupe de Garside et la structure de groupe de difféotopie.

Comme résultat préliminaire, nous développons un algorithme de complexité quadratique capable de classier les tresses à quatre brins selon leur type de Nielsen-Thurston. Plus généralement, nous étudions ce problème de classification pour un nombre arbitraire de brins. Nous donnons une adaptation des résultats connus de Benardete-Gutiérrez-Nitecki au cadre de la structure de Garside duale. Enfin, à l'aide d'un résultat profond (et non constructif) de Masur-Minsky, nous prouvons l'existence d'un algorithme de complexité polynômiale pour décider le type de Nielsen-Thurston d'une tresse avec un nombre de brins arbitraire.

Problemas algorítmicos en los grupos de trenzas

Esta tesis tiene por objeto desarrollar nuevos algoritmos para los grupos de trenzas. Un problema importante en la teoría matemática de las trenzas es mejorar los algoritmos existentes para resolver el problema de la conjugación. Resolvemos completamente este problema en el caso del grupo de trenzas con cuatro cuerdas, produciendo un algoritmo de complejidad cúbica en función de la longitud de las entradas. La demostración se apoya en dos aspectos fundamentales de los grupos de trenzas: la estructura de grupo de Garside y la estructura de grupo de difeotopía.

Como un resultado preliminar, desarrollamos un algoritmo de complejidad cuadrática capaz de clasificar las trenzas con cuatro cuerdas según su tipo de Nielsen-Thurston. Más generalmente, estudiamos este problema de clasificación para un número arbitrario de cuerdas. Damos una adaptación de los resultados conocidos de Benardete-Gutiérrez-Nitecki al caso de la estructura de Garside dual. Por fin, con la ayuda de un resultado profundo (y no constructivo) de Masur-Minsky, probamos la existencia de un algoritmo de complejidad polinomial para decidir el tipo de Nielsen-Thurston de una trenza con un número arbitrario de cuerdas.

Algorithmic problems in the braid groups

The aim of this thesis is to develop new algorithms for the braid groups. An important problem in the mathematical theory of braids is to improve the existing algorithms to solve the conjugacy problem. We completely solve this problem in the case of the four-strand braid group, by developing an algorithm of cubic complexity in term of the length of the input. The demonstration leans on two fundamental aspects of braid groups: the structure of Garside group and the structure of Mapping Class Group.

As a preliminary result, we develop an algorithm of quadratic complexity which classifies four-strand braids according to their Nielsen-Thurston type. More generally, we study this problem of classification for an arbitrary number of strands. We give an adaptation of known results by Benardete-Gutiérrez-Nitecki in the frame of the dual Garside structure. Finally, with the help of a deep (non-constructive) result by Masur-Minsky, we show the existence of a polynomial time algorithm for deciding the Nielsen-Thurston type of a given braid with arbitrarily many strands.