Patrick Dehornoy [1]

Le problème d'isotopie des tresses

Je vais vous parler du problème d'isotopie des tresses. Je crois que c'est un problème bien adapté à ces leçons car c'est un problème de difficulté moyenne. Cela veut dire qu'on ne connaît aucune solution qui soit triviale, mais, d'un autre côté, ce n'est pas un problème trop difficile : il existe des solutions qui peuvent être décrites et expliquées en un temps raisonnable — et c'est ce que je vais essayer de faire.

Une autre caractéristique du problème est qu'on peut l'aborder en partant de points de vue très variés. Peut-être que, du point de vue d'un spécialiste des équations différentielles, tout ce que je vais dire apparaîtra comme de l'algèbre, mais, à mon avis, ce sont vraiment des approches différentes : certaines sont purement algébriques, d'autres plus combinatoires, d'autres franchement topologiques ou géométriques.

Mon exposé aura deux parties, et son plan est simple :

- Première partie : *une* solution au problème d'isotopie des tresses,
- Deuxième partie : *des* solutions au problème d'isotopie des tresses.

Je vais essayer de vous expliquer une première solution lentement, pas à pas, pour vous convaincre que le problème est résoluble. La solution que j'ai choisie pour cela n'est pas la meilleure, loin de là, mais ses étapes successives devraient être faciles à suivre. J'irai ensuite beaucoup plus vite pour la deuxième partie, où je vous présenterai une sorte de panorama des solutions existantes pour vous donner une idée de la variété des approches possibles.

Première partie : *une* solution au problème d'isotopie des tresses

Je vais commencer par expliquer le problème, puis on va faire quelques essais pour le résoudre directement, je veux dire, sans mathématiques sophistiquées, et puis, ensuite, les tentatives naïves s'étant révélées infructueuses, on va voir comment construire pas à pas une solution en introduisant des outils convenables.

[1] rédigé avec l'aide de Marie Albenque

Le problème

Qu'est-ce qu'une tresse ? Eh bien, d'abord, c'est l'objet matériel qu'on voit sur la figure 1. Du point de vue mathématique, ce qu'on va prendre en compte dans la suite, ce ne sont pas du tout les aspects métriques, par exemple la longueur ou l'épaisseur des brins, mais seulement les croisements : quel brin croise quel autre, dans quel ordre, qui passe dessus et qui passe dessous. La théorie des tresses est avant tout un calcul des croisements.

Figure 1: Une tresse matérielle

Historiquement, on trouve des tresses dessinées dans des carnets de notes de Gauss à la fin du XVIIIe siècle, mais sans qu'aucune théorie en soit développée. C'est au tournant du XXe siecle que les tresses apparaissent comme objets proprement mathématiques dans les travaux de Hurwitz. Elles n'y sont pas vraiment considérées en tant que telles, mais seulement pour leur action par conjugaison sur les suites d'éléments d'un groupe, précisément connue depuis sous le nom d'action de Hurwitz. Par contre, les tresses et les groupes de tresses sont introduits formellement et étudiés pour eux-mêmes par Emil Artin dans un texte de 1925 [1], puis dans un article publié après la guerre aux USA où il avait émigré [2]. C'est donc à Artin qu'on fait en général remonter la théorie des tresses.

Le point de départ, ce sont les *diagrammes de tresse*. Un diagramme de tresse à trois brins est représenté dans la figure 2 : il est composé de trois brins qui relient en se croisant trois points sur une verticale à gauche à trois points sur une verticale à droite ; on exige que les brins gardent une orientation générale de gauche à droite, sans jamais revenir en arrière (si on autorise à revenir en arrière, c'est une autre théorie, celle des « stringlinks »).

Figure 2: Un diagramme de tresse à trois brins.

Ce qu'on appelle *problème d'isotopie des tresses* est le problème suivant :

> Etant donnés deux diagrammes de tresse, reconnaître si on peut *déformer* l'un en l'autre.

Pour que la question ait un sens, il faut préciser ce qu'on entend par déformer un diagramme. Ceci se fait en passant à l'espace $\mathbb{R}^3$ et en voyant un diagramme de tresses, qui au départ vit dans un plan, comme la projection d'un objet en trois dimensions, à savoir une collection de trois ficelles matérielles ininterrompues, ou encore une collection de trois courbes continues de $\mathbb{R}^3$ — ou plutôt de $\mathbb{R}^2 \times [0,1]$, en décidant que les extrémités gauches des brins se trouvent dans le plan $z = 0$, et les extrémités droites dans le plan $z = 1$. Il y a alors une notion naturelle de déformation continue de l'espace ambiant. On dit qu'une figure géométrique de $\mathbb{R}^2 \times [0,1]$ est *isotope* à cette autre s'il existe une déformation continue de l'espace faisant passer de l'une à l'autre, avec ici la règle supplémentaire que les points des deux plans du bord $z = 0$ et $z = 1$ sont laissés fixes. Un exemple d'isotopie est représenté dans la figure 3.

Figure 3: Isotopie transformant le diagramme de gauche en le diagramme de droite, les diagrammes étant vus comme la projection de figures en trois dimensions : le brin du devant, en pointillé, est déplacé vers la gauche, tandis que le croisement des deux brins de derrière est poussé vers la droite.

Le problème d'isotopie est donc le problème de reconnaître si deux diagrammes de tresse sont les projections de deux figures isotopes de $\mathbb{R}^2 \times [0,1]$, auquel cas on dira simplement que les diagrammes sont isotopes. Il est entendu que ce qu'on cherche est un algorithme général, c'est-à-dire une recette qui permette, quels que soient les diagrammes initiaux, de décider en un temps fini s'ils sont ou non isotopes — et pas seulement, bien sûr, de résoudre la question pour des diagrammes particuliers.

Dans l'exemple de la figure 3, où les diagrammes ont trois brins et trois croisements, on devine qu'il ne doit pas être très difficile de trouver une solution. Par contre, si on a des diagrammes à cent brins et dix mille croisements, le problème risque d'être plus difficile. Malgré tout, on va voir que c'est un problème qui peut tout à fait se résoudre, à la fois théoriquement et pratiquement, à l'aide de certains des algorithmes que je vais présenter.

A quoi bon résoudre ce problème ?

Si on s'intéresse aux tresses — ce n'est pas une évidence qu'il faille le faire ! — résoudre le problème d'isotopie est une question préliminaire à toute théorie, une sorte de problème numéro zéro. Ce qu'on appelle tresse en mathématiques, c'est une classe d'isotopie de diagrammes : on verra dans un petit moment que c'est la définition la plus naturelle pour obtenir une structure intéressante, à savoir une structure de groupe. A partir de là, reconnaître si des diagrammes sont isotopes, c'est reconnaître s'ils représentent la même tresse. Comme les tresses sont (presque) toujours spécifiées par le biais de diagrammes, on ne peut parler concrètement de tresses que si on sait reconnaître quand deux diagrammes représentent la même tresse, autrement dit que si on sait résoudre le problème d'isotopie.

La question est spécialement importante quand on veut utiliser des tresses dans des applications de nature algorithmique, par exemple pour faire de la cryptographie ainsi que cela a été proposé récemment [10] : de la même façon que, pour calculer avec des entiers, il faut être capable de reconnaître quand deux suites de chiffres représentent le même entier, pour calculer avec des tresses, il faut être capable de reconnaître quand deux diagrammes représentent la même tresse. Je ne sais pas si les tresses remplaceront un jour les nombres entiers dans les cartes à puce, mais, si elles le font, cela utilisera certainement, au départ, une solution efficace au problème d'isotopie.

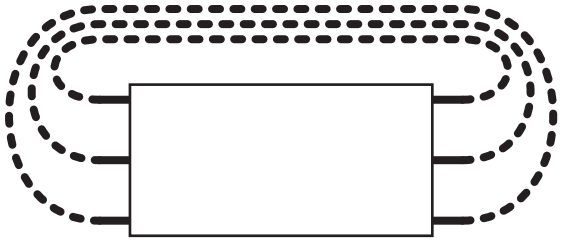

Figure 4: Clôture d'une tresse pour obtenir un nœud — ou plutôt un entrelacs en général.

Le problème d'isotopie des tresses est aussi lié à d'autres problèmes, par exemple le problème d'isotopie des nœuds, et résoudre le premier peut être vu comme une première étape vers la résolution du second. Un nœud, c'est la version fermée d'une tresse. Une tresse, ce sont des brins qui entrent et qui sortent et, entre les deux, une boîte avec des croisements. Un nœud c'est la même chose, mais où on a refermé les extrémités (voir Figure 4). Ainsi, à toute tresse, on associe un nœud, et, inversement on montre que tout nœud provient d'une tresse de cette façon-là. Il est clair que, si on fait une isotopie dans la boîte, on obtient une isotopie pour la clôture. Par contre, on peut appliquer à un diagramme fermé des quantités d'isotopies qui ne

proviennent pas d'une isotopie à l'intérieur de la boîte, c'est-à-dire d'une isotopie de la tresse : le problème d'isotopie des nœuds est un problème bien plus compliqué que celui de l'isotopie des tresses. Du reste, je vous ai bien dit que ce dernier est un problème de difficulté moyenne, alors que le problème d'isotopie des nœuds, lui, est un problème vraiment difficile.

Jacques Martinet — Tu n'as pas pris un nœud ici, tu as pris un entrelacs ?

P.D. — Oui, tu as raison.

Jacques Martinet — Est-ce que les entrelacs se ramènent d'une part aux nœuds et d'autre part aux tresses ?

P.D. — Un entrelacs, c'est comme un nœud, mais avec éventuellement plusieurs composantes. Quand j'ai parlé de nœud ci-dessus, j'aurais dû dire entrelacs partout, car la clôture d'une tresse n'a en général aucune raison de n'avoir qu'une composante. Mais le terme usuel est théorie des nœuds, et c'est pour cela que je l'ai employé. Cela dit, la théorie des entrelacs généraux n'est pas fondamentalement plus compliquée que la théorie des nœuds et, en particulier, tout entrelacs est clôture d'une tresse. Mais, à ma connaissance, non, il n'y a pas de moyen uniforme de ramener un entrelacs à un nœud et une tresse.

Si on revient aux applications des tresses, il y a des quantités de liens entre les tresses et la physique, par exemple les tresses décrivent, en un sens qui peut être rendu précis, les symétries des équations de Yang–Baxter. Il y a également des liens avec la chimie et la biologie : on imagine bien que les tresses peuvent être utilisées comme outil de modélisation pour l'ADN, ou pour des macromolécules comme le caoutchouc dont les propriétés d'élasticité sont directement liées aux phénomènes d'enroulement et de tressage. A proprement parler, ces aspects ne sont pas des applications du problème d'isotopie des tresses, mais ils sont quand même reliés.

Je vais donc m'arrêter là pour ce qui est des motivations, et tenir pour acquis que le problème d'isotopie est suffisamment intéressant pour qu'on ait envie de le résoudre.

Une première remarque

Je commence par une remarque générale. Le problème d'isotopie des tresses appartient à la famille générale des problèmes de décidabilité, et, à ce titre, il se décompose en deux demi-problèmes. Il y a un problème positif, à savoir prouver que deux diagrammes sont isotopes. Pour cela, il suffit de donner, d'une façon ou d'une autre, une déformation du premier diagramme sur le second, et on a alors prouvé qu'ils sont isotopes. En un sens, c'est la moitié facile, puisque, si on a deviné la bonne transformation, alors on a prouvé le résultat escompté.

Le deuxième demi-problème est le problème de prouver une non-isotopie. Il est d'une nature différente, et *a priori* plus difficile : ce n'est pas parce qu'on n'arrive pas à exhiber une isotopie entre deux diagrammes qu'on a pour autant prouvé qu'il n'en existe pas. Il faut donc trouver une autre approche. L'idée la plus naturelle, qui est tout à fait standard, est de trouver des invariants d'isotopie. Cela consiste à trouver une application I qui va des diagrammes de tresse vers un espace quelconque de sorte que, si des diagrammes sont isotopes, alors I prend la même valeur. Dans ces conditions, si I prend des valeurs différentes sur deux diagrammes D, D' — on dit alors que I *sépare* D et D' — on est assuré que ceux-ci ne sont pas isotopes. La question alors est de savoir si on peut trouver un invariant *complet*, c'est-à-dire un invariant qui sépare toute paire de diagrammes non isotopes.

Des invariants naïfs

Je vais commencer avec quelques tentatives à la main pour trouver des invariants d'isotopie. Un premier exemple est la permutation associée à une tresse. Quand vous avez deux diagrammes, vous pouvez numéroter les brins. Par exemple, dans la figure 5, on a numéroté les extrémités gauches des brins de chaque diagramme de bas en haut. On peut alors regarder les positions finales des brins, c'est-à-dire où finit à le brin qui part en position 1, puis de même pour les brins partant en position 2 et 3. Dans la figure 5, les brins partant en position 1 finissent respectivement en position 3 (diagramme de gauche) et en position 2 (diagramme de droite). La règle du jeu étant que l'isotopie fixe les extrémités, les diagrammes ne peuvent pas être isotopes, et on l'a ainsi démontré. Formellement, l'invariant utilisé ici est une permutation : tout diagramme de tresse à n brins définit une permutation des entiers $1, ..., n$, et, comme deux diagrammes isotopes donnent la même permutation, celle-ci est un invariant d'isotopie.

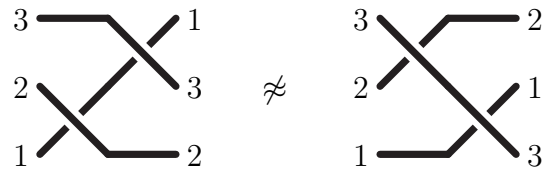

Figure 5: Deux diagrammes qui n'induisent pas la même permutation des brins ne peuvent pas être isotopes.

L'invariant précédent n'est pas complet — ainsi que le démontrent les résultats cité plus loin — et on cherche d'autres invariants. Une idée serait de compter les croisements, pour obtenir un invariant à valeurs dans les entiers naturels. Mais cela ne marche pas : on voit sur la figure 6 qu'on

Figure 6: Le nombre de croisements n'est pas un invariant d'isotopie : ici on déforme un diagramme à deux croisements en un diagramme sans croisement.

peut déformer un diagramme avec deux croisements en un autre avec zéro croisement : le nombre de croisements n'est donc *pas* un invariant. Par contre, on peut considérer le nombre de croisements modulo 2, ou encore regarder le nombre de croisements comptés avec un signe correspondant à l'orientation dessus–dessous. Cette fois, on obtient bien des invariants d'isotopie.

Une autre idée encore est de considérer le nombre d'enlacement de deux brins. Si, dans un diagramme de tresse, on isole deux brins en oubliant les autres, on obtient un diagramme de tresse à deux brins. Or un tel diagramme, c'est simplement une suite de demi-tours. Par conséquent, pour chaque paire de brins dans un diagramme de tresse, on peut compter les demi-tours formés par ces deux brins, et il n'est pas difficile de vérifier qu'on obtient ainsi un invariant d'isotopie, appelé nombre d'enlacement des deux brins.

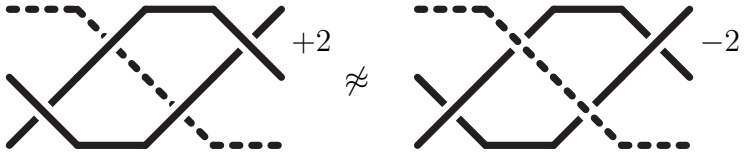

Figure 7: Le nombre d'enlacement des deux brins en traits pleins est $+2$ à gauche, et -2 à droite, donc les diagrammes ne sont pas isotopes.

Dans le dernier exemple, on a simplement isolé une tresse à deux brins au milieu d'une tresse à trois brins. D'une manière générale, quand on a deux diagrammes à n brins, on peut les projeter de manière naturelle en des diagrammes à p brins en oubliant $n-p$ brins. Si on trouve un invariant qui sépare les diagrammes projetés, il sépare a fortiori les diagrammes initiaux.

On a ainsi obtenu toute une collection d'invariants. La question est de savoir si cette collection est complète, c'est-à-dire si, étant donnés deux diagrammes non isotopes, il existe toujours au moins un invariant de la famille qui permet de les séparer. La réponse est négative — et vous pouvez vous en douter, puisque j'ai dit au début de la leçon que le problème d'isotopie est un problème de difficulté moyenne, pas un problème facile.

Par exemple, la figure 8 montre deux diagrammes qui ne sont pas isotopes — ce n'est pas encore prouvé, mais on le verra bientôt — et qui,

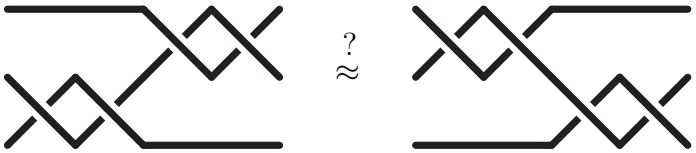

Figure 8: Deux diagrammes qui ne sont séparés par aucun des invariants décrits jusqu'à présent — et dont on verra pourtant plus loin qu'ils ne sont pas isotopes.

néanmoins, ont la même permutation, le même nombre de croisements dessus/dessous, et où chaque paire de brins a le même nombre d'enlacement. Autrement dit, aucun des invariants naïfs décrits jusqu'à présent ne sépare ces diagrammes.

Première étape : introduire une structure de groupe

Après ces tentatives peu concluantes, on va maintenant décrire une vraie solution au problème d'isotopie des tresses. Cette solution ne consiste pas à construire un invariant, mais repose sur le fait que les tresses ont une structure naturelle de groupe. La solution va nécessiter plusieurs étapes, cinq en tout, que je vais détailler successivement.

La première étape consiste à définir une structure de groupe qui va être fondamentale. C'est précisément cette structure, qui existe pour les tresses mais pas pour les nœuds ou les entrelacs, qui rend le problème d'isotopie des tresses (beaucoup) plus facile que celui des nœuds et des entrelacs.

Pour obtenir une structure de groupe, on commence par définir un produit sur les diagrammes de tresse. Etant donnés deux diagrammes D_1 et D_2 avec le même nombre de brins, on peut, comme dans la figure 9, les concaténer, c'est-à-dire les mettre l'un derrière l'autre en raccordant les extrémités droites de D_1 aux extrémités gauches de D_2. On obtient alors un troisième diagramme, qu'on appelle leur *produit* et qu'on note $D_1 D_2$.

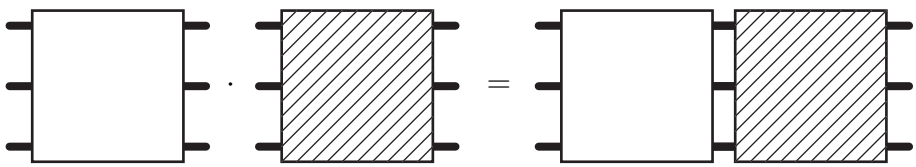

Figure 9: Produit de deux diagrammes de tresse.

Le produit des diagrammes de tresse est compatible avec l'isotopie : si D_1' est isotope à D_1, et si D_2' est isotope à D_2, alors $D_1' D_2'$ est isotope à $D_1 D_2$. Par conséquent, le produit des diagrammes induit un produit bien défini sur les classes d'isotopie, c'est-à-dire sur les tresses. Il n'est alors

pas difficile de vérifier que ce produit est associatif et admet pour élément neutre la tresse triviale qui est la classe d'un diagramme sans croisement.

Là où on voit l'intérêt de considérer les tresses plutôt que les diagrammes de tresse, c'est-à-dire de passer aux classes d'isotopie, c'est lorsqu'on cherche d'éventuels inverses pour le produit. Si un diagramme D a au moins un croisement, alors il en est de même de tout diagramme obtenu en multipliant D par un autre diagramme, et aucun diagramme, à part les diagrammes sans croisement, ne peut avoir d'inverse pour le produit. Par contre, lorsqu'on passe aux tresses, des croisements peuvent disparaître après isotopie. Et même, dans tous les cas, lorsqu'on considère le produit d'un diagramme quelconque D par son image $\widetilde{D}$ dans un miroir vertical — c'est-à-dire le diagramme obtenu en renversant l'ordre et l'orientation des croisements — alors chacun des deux diagrammes $D\widetilde{D}$ et $\widetilde{D}D$ est isotope à un diagramme sans croisement, les croisements se démêlant de proche en proche, comme on le voir dans un exemple sur la figure 10. Il en résulte que le produit des tresses donne une structure de groupe.

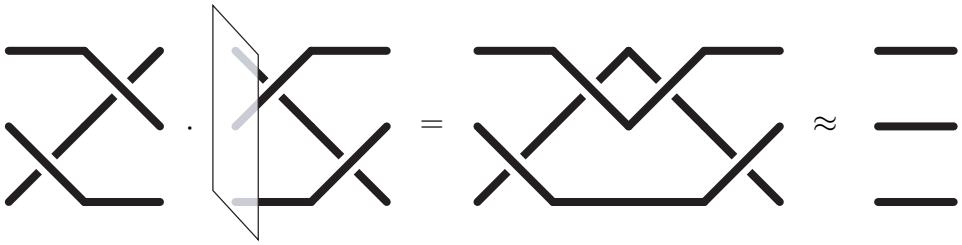

Figure 10: Le produit d'un diagramme et de son image dans un miroir vertical est isotope à un diagramme sans croisement.

Définition. Pour $n \geqslant 2$, on note B_n le groupe des tresses à n brins.

La lettre B de B_n vient ici de « braid », « tresse » en anglais.

Pour nous, maintenant, la question est de savoir ce qu'une structure de groupe fait gagner pour ce qui est de résoudre le problème d'isotopie. Il y a au moins un premier bénéfice, qui est de réduire le problème d'isotopie — déterminer si deux diagrammes D et D' sont isotopes — au problème de *trivialité* — déterminer si un diagramme D est isotope au diagramme trivial (c'est-à-dire sans croisement). En effet, deux diagrammes D et D' sont isotopes si et seulement si le diagramme $\widetilde{D}D'$ est isotope au diagramme trivial. Donc, si on sait résoudre le problème de trivialité, on sait *ipso facto* résoudre le problème d'isotopie. Il n'est pas évident que le problème de trivialité soit plus facile que le problème d'isotopie, mais on est au moins passé d'un problème à deux variables à un problème à une variable.

Deuxième étape : trouver une présentation

L'autre intérêt d'avoir obtenu une structure de groupe est de pouvoir utiliser des méthodes générales d'algèbre. Mais, pour cela, il faut d'abord spécifier le groupe B_n d'une manière ou d'une autre, de façon à pouvoir l'étudier concrètement. Or une façon usuelle de spécifier un groupe est d'en donner une présentation par générateurs et relations, et c'est ce qu'on va faire maintenant pour le groupe B_n.

Pour trouver des générateurs simples, on va commencer par se ramener à des diagrammes normalisés. D'abord, toute courbe peut être déformée de manière continue en une courbe affine par morceaux, c'est-à-dire composés de segments de droite : on ne perd donc rien en se restreignant à des diagrammes affines par morceaux. On peut ensuite redresser les segments, et se ramener à des diagrammes normalisés où les segments ont même longueur et où les pentes sont 0, +1, ou −1, comme dans la figure 11. De tels diagrammes peuvent alors être découpés en tranches de façon à ce que, dans chaque tranche, il n'y ait qu'un seul croisement de deux brins voisins. Mais alors, ceci signifie que toute tresse à n brins peut s'exprimer comme produit de diagrammes normalisés contenant un seul croisement. Autrement dit, les classes de ces diagrammes forment une famille génératrice du groupe B_n.

Figure 11: Normalisation d'un diagramme de tresse et expression comme produit de diagrammes élémentaires σ_i et σ_i^{-1}.

Il existe exactement $2(n-1)$ diagrammes à n brins du type ci-dessus, deux à deux inverses. Traditionnellement depuis Artin, on note σ_i la classe du diagramme dans lequel le brin $i+1$ passe au-dessus du brin i, et donc σ_i^{-1} son image-miroir. Notez bien que ce qu'on prend en compte ici, ce n'est pas le numéro des brins mais uniquement leur position (comme dans la présentation du groupe symétrique à partir des transpositions).

Les tresses $\sigma_1, ..., \sigma_{n-1}$ sont appelées les *générateurs d'Artin*. Remarquez qu'on se contente d'écrire σ_i et non pas $\sigma_{i,n}$: cela tient à ce qu'on suppose implicitement le nombre de brins fixé, mais aussi et surtout au fait qu'il n'y a aucun danger à identifier B_n à un sous-groupe de B_{n+1}, une tresse à n brins pouvant être considérée comme une tresse à $n+1$ brins où le dernier brin n'est pas tressé.

Il reste à étudier les relations entre les générateurs d'Artin, c'est-à-dire à traduire en termes algébriques la relation d'isotopie. La figure 3 montre que

les diagrammes correspondant aux produits $\sigma_1\sigma_2\sigma_1$ et $\sigma_2\sigma_1\sigma_2$ sont isotopes. Autrement dit, dans le groupe B_n, la relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ est satisfaite. Par ailleurs, il est à peu près évident que, dès que des croisements concernent des brins disjoints, l'ordre dans lequel ils sont effectués est indifférent (voir la figure 12). La relation $\sigma_3\sigma_1 = \sigma_1\sigma_3$, et toutes les relations similaires, sont donc vérifiées dans le groupe B_n.

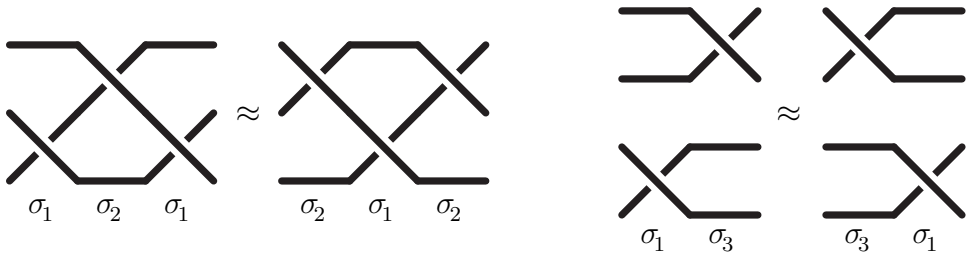

Figure 12: Deux types de relations entre les générateurs σ_i.

La question est de savoir s'il existe d'autres relations entre les tresses σ_i que celles devinées plus haut, et les relations $\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1$ qui sont vraies dans tout groupe. La réponse est qu'il n'en existe pas d'autre, et c'est précisément ce résultat d'Artin qui est le point de départ de la théorie moderne des tresses.

Théorème 1 (Artin, 1925). *Le groupe B_n admet la présentation*

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

La démonstration est assez simple. On appelle Δ-mouvement la transformation consistant à remplacer un segment d'un diagramme affine par morceaux de $\mathbb{R}^3$ par deux segments adjacents de mêmes extrémités sous réserve qu'aucun autre segment du diagramme n'intersecte le triangle formé par les trois segments, ou la transformation inverse (voir la figure 13). Il est facile de voir que deux diagrammes affines par morceaux sont isotopes si et seulement si on peut passer de l'un à l'autre par une suite de Δ-mouvements. Il reste alors à vérifier que, si w et w' sont les mots en les lettres σ_i qui codent les croisements de deux diagrammes obtenus l'un à partir de l'autre par Δ-mouvement, alors on passe de w à w' en appliquant une des relations de (*), ou une relation qui s'en déduit. Il n'y a qu'un nombre fini de cas à considérer, et c'est une vérification sans problème.

Le problème d'isotopie de tresses est donc ramené à ce qu'on appelle le *problème de mot* de la présentation de groupe (*) :

> Etant donné un mot de tresse, c'est-à-dire un mot sur les lettres σ_i et σ_i^{-1}, ce mot est-il équivalent au mot vide vis-à-vis des relations (*) ?

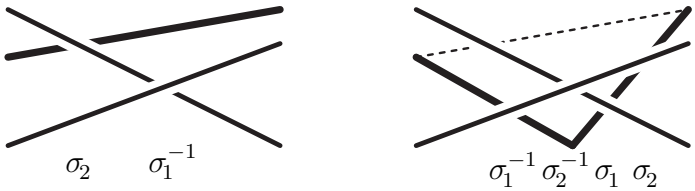

Figure 13: Δ-mouvement : quand on remplace le segment en gras à gauche par les deux segments en gras à droite, les croisements changent, donc aussi le codage par les σ_i, mais on constate qu'on passe de l'ancien au nouveau en appliquant une relation qui est conséquence des relations $(*)$, ici $\sigma_2\sigma_1^{-1} = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2$, qui est conséquence de $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ et des relations $\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1$ implicites dans tout groupe.

Soit encore, en notant ε le mot vide, et $\equiv$ la plus petite congruence sur les mots de tresse contenant les paires $(\sigma_i\sigma_j\sigma_i, \sigma_j\sigma_i\sigma_j)$ pour $|i-j| = 1$, $(\sigma_i\sigma_j, \sigma_j\sigma_i)$ pour $|i-j| \geqslant 2$, et $(\sigma_i\sigma_i^{-1}, \varepsilon)$ $(\varepsilon, \sigma_i\sigma_i^{-1})$ pour tout i, a-t-on $w \equiv \varepsilon$?

On a ainsi ramené le problème d'isotopie des tresses à un problème d'algèbre. A-t-on gagné pour autant ? Certainement pas... La faute en est à un théorème fameux :

Théorème 2 (Novikov, 1952). *Il existe une présentation finie de groupe dont le problème de mot est indécidable.*

Bien sûr, le théorème de Novikov ne dit rien de la présentation spécifique du théorème 1. Mais, puisqu'il existe des présentations de groupe finies telles qu'aucun algorithme ne puisse résoudre le problème du mot, il ne saurait exister une méthode uniforme pour résoudre tous les problèmes de mot associés à des présentations de groupe finies. Autrement dit, il n'y a rien à espérer de méthodes générales, et il va falloir trouver une solution *ad hoc* pour le cas des relations $(*)$.

Troisième étape : passer au monoïde

Pour résoudre le problème du mot dans le cas spécifique des groupes de tresses, on va utiliser ici la méthode développée par F.A. Garside à la fin des années 1960 dans [17] — son seul article de mathématiques publié. Ce n'est pas la méthode utilisée par Artin deux décennies plus tôt. Celle-ci sera mentionnée plus loin, mais, par bien des aspects, la méthode de Garside, qui consiste à introduire le monoïde associé à la présentation (*), est plus intéressante.

Un monoïde est une structure formée d'une opération associative et possédant un élément neutre, mais où on n'impose rien quant à l'existence d'inverses. Quand on a une présentation de groupe où les inverses des générateurs n'interviennent pas, comme c'est le cas pour (*), on peut tou-

jours considérer le monoïde qui, en tant que monoïde, a la même présentation que le groupe, c'est-à-dire les mêmes générateurs et les mêmes relations.

Définition. On appelle B_n^+ le monoïde défini par la présentation (*), c'est-à-dire, le monoïde qui, en tant que monoïde, admet les générateurs et les relations de (*).

Par définition, les éléments de B_n^+ sont des classes d'équivalence de mots formés sur les lettres σ_i — appelés mots (de tresse) *positifs* dans la suite — vis-à-vis de la plus petite congruence sur les mots de tresse positifs contenant les paires $(\sigma_i\sigma_j\sigma_i, \sigma_j\sigma_i\sigma_j)$ pour $|i-j|=1$ et $(\sigma_i\sigma_j, \sigma_j\sigma_i)$ pour $|i-j| \geqslant 2$. On notera $\equiv^+$ cette relation, et on dira que deux mots positifs w, w' sont *positivement équivalents* si on a $w \equiv^+ w'$. Par définition, résoudre le problème de mot de la présentation (*) du monoïde B_n^+ consiste à donner un algorithme décidant, pour deux mots positifs quelconques w, w', si on a $w \equiv^+ w'$.

On pourrait espérer que l'absence d'inverse rende le problème de mot des monoïdes plus facile que celui des groupes. Il n'en est rien, et c'est même le contraire.

Théorème 3 (Markov, Post, 1947). *Il existe une présentation de monoïde finie dont le problème de mot est indécidable.*

A nouveau donc, point d'espoir de méthode générale. Par contre, dans le cas qui nous intéresse, c'est-à-dire pour le monoïde B_n^+, il est très facile de résoudre le problème de mot. En effet, les relations entre les générateurs sont des relations qui préservent la longueur. Un mot positif ne peut donc être positivement équivalent à un autre mot positif que s'ils ont la même longueur. Comme il n'y a qu'un nombre fini de mots de longueur fixée, on peut énumérer tous les mots positivement équivalents à un mot donné, et on obtient la solution cherchée :

Algorithme 4. *Etant donnés deux mots de tresse positifs w, w' :*

- *Si w et w' ont des longueurs différentes, alors $w \equiv^+ w'$ est faux;*
- *Sinon, partir de w et énumérer de proche en proche tous les mots qui peuvent s'en déduire en appliquant les relations de (*) ; alors $w \equiv^+ w'$ est vrai si et seulement si w' apparaît dans la liste de mots ainsi construite.*

La méthode précédente ne saurait s'appliquer dans le cas du groupe B_n, puisque la relation $\sigma_i\sigma_i^{-1} = 1$, qui est vraie dans tout groupe, ne préserve pas la longueur : un mot de longueur 2 peut être équivalent à un mot de longueur 0.

On a donc résolu un problème de mot. En a-t-on pour autant terminé avec notre problème d'isotopie ? Toujours pas, car ce qui nous intéresse est le problème de mot du *groupe* B_n, et pas celui du *monoïde* B_n^+. Il reste donc à relier ces deux problèmes, si faire se peut.

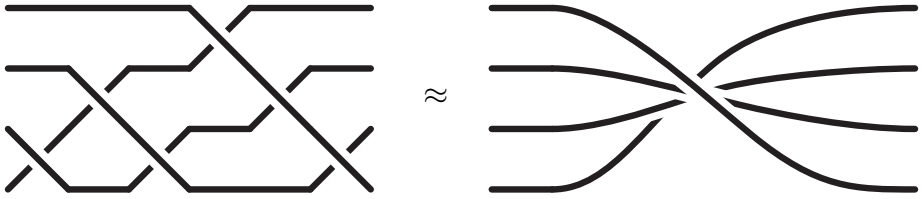

Figure 14: Deux diagrammes représentant la tresse Δ_4.

Quatrième étape : introduire la tresse Δ_n

Il y a deux différences entre le problème de mot de B_n et celui de B_n^+, à savoir que, dans le premier cas, on considère des mots quelconques et la relation $\equiv$, alors que, dans le second cas, on considère des mots positifs et la relation $\equiv^+$. Dans un premier temps, on va déjà se ramener à ne plus considérer que des mots positifs. Pour cela, on va se servir d'une tresse particulière, appelée *tresse de Garside*. Cette tresse est la tresse représentée par le mot (positif) Δ_n défini par la formule de récurrence

$$\Delta_1 = 1, \qquad \Delta_n = \Delta_{n-1} \cdot \sigma_{n-1} ... \sigma_2 \sigma_1.$$

Egalement noté (par abus) Δ_n, cette tresse correspond à un diagramme où une nappe de n brins fait un demi-tour (figure 14).

Il n'est pas difficile de montrer les propriétés suivantes.

Lemme 5. *Pour tout i entre 1 et $n-1$, on a $\sigma_i \Delta_n \equiv \Delta_n \sigma_{n-i}$, et, d'autre part, $\Delta_n \sigma_i^{-1}$ est équivalent à un mot positif.*

Ce lemme implique que, pour tout mot de tresse w contenant p lettres σ_i^{-1}, on peut trouver, de façon effective, un mot *positif* v vérifiant $\Delta_n^p w \equiv v$. Pour cela, on utilise la première relation du lemme pour faire migrer vers la droite les facteurs Δ_n de façon à en placer un à gauche de chaque lettre σ_i^{-1}, puis on utilise la seconde relation du lemme pour remplacer le facteur $\Delta_n \sigma_i^{-1}$ par un mot positif équivalent. Alors, par construction, on a

$$w \equiv \varepsilon \quad \Longleftrightarrow \quad v \equiv \Delta_n^p.$$

Par conséquent, on est ramené au problème de reconnaître si deux mots *positifs* sont équivalents pour $\equiv$.

Cette fois a-t-on terminé? Toujours pas car, même pour des mots positifs, il y a *a priori* une grande différence entre les relations $\equiv$ et $\equiv^+$. Il est clair que $w \equiv^+ w'$ entraîne $w \equiv w'$, toujours : si on sait passer de w à w' par des équivalences positives, on sait *a fortiori* le faire par des équivalences quelconques. Mais la réciproque n'a en général aucune raison d'être vraie : il se pourrait très bien qu'on puisse transformer w en w' en introduisant

des motifs intermédiaires $\sigma_i^{-1}\sigma_i$, mais pas en restant dans les mots positifs. Pensez par exemple à la présentation dont l'unique relation est $ab = ac$. Alors on a $b \not\equiv^+ c$, car aucune relation ne s'applique à b; par contre, on a $b \equiv c$, puisqu'on peut écrire $b \equiv a^{-1}ab \equiv a^{-1}ac \equiv c$. En d'autres termes, dans le monoïde présenté par $ab = ac$, on a $b \neq c$, alors que, dans le groupe de même présentation, on a $b = c$.

Par conséquent, le problème d'isotopie des tresses n'est pas résolu. Mais il ne reste plus qu'une étape.

Cinquième étape : utiliser le théorème de Ore

Il existe un cas où on est certain que l'équivalence positive et l'équivalence tout court coïncident sur les mots positifs, c'est celui des *groupes de fractions*, c'est-à-dire des groupes où tout élément peut s'écrire comme quotient de deux éléments du monoïde associé. Le critère précis est le suivant.

Théorème 6 (Ore, 1931). *Supposons que M est un monoïde simplifiable et admettant des multiples communs à droite. Alors, pour toute présentation de M, la relation $\equiv^+$ est la restriction aux mots positifs de la relation $\equiv$ associée.*

En termes équivalents, le monoïde M se plonge dans le groupe admettant, en tant que groupe, les mêmes présentations que M (lequel groupe ne dépend pas de la présentation choisie, et est un groupe de fractions de M). Le théorème de Ore est analogue à la construction des entiers relatifs à partir des entiers naturels, et à celle des nombres rationnels à partir des entiers relatifs. Il demande seulement un peu plus de soin parce qu'on ne suppose pas le monoïde de départ commutatif.

Il ne reste donc plus qu'à vérifier que le monoïde B_n^+ satisfait aux deux conditions du théorème de Ore. La première, la simplifiabilité, est la propriété que $abc = ab'c$ entraîne $b = b'$ quels que soient a et c. La seconde, l'existence de multiples communs à droite, est la propriété que, pour tous a, b, il existe c, d vérifiant $ad = bc$. C'est ce qui a été fait par Garside.

Théorème 7 (Garside, 1969). *Le monoïde B_n^+ est simplifiable et admet des multiples communs à droite.*

Le second point résulte facilement du lemme 5 : la tresse Δ_n^p est un multiple commun de toutes les tresses représentées par un mot positif de longueur p. Le premier point est plus délicat, et sa démonstration requiert des outils algébriques que je vais sauter ici — c'est essentiellement ma seule tricherie.

Alors on a gagné ! En effet, grâce au lemme 5, on peut transformer la question de décider $w \equiv \varepsilon$ en celle de décider $\Delta_n^p \equiv v$ où v est un mot positif,

donc, par le théorème de Ore, en celle de décider $\Delta_n^p \equiv^+ v$. Or ceci peut être fait grâce à l'algorithme 4. La méthode peut être récapitulée comme suit :

Algorithme 8. *Partant d'un mot de tresse à n brins w avec p lettres σ_i^{-1} :*
- *Appliquer le lemme* 5 *pour trouver un mot positif v vérifiant $\Delta_n^p\, w \equiv v$;*
- *Appliquer l'algorithme* 4 *pour décider si $v \equiv^+ \Delta_n^p$ est vérifié ; si oui, on a $w \equiv \varepsilon$, sinon, on a $w \not\equiv \varepsilon$.*

Exemple. Considérons les deux mots de tresse qui résistaient aux invariants naïfs, à savoir $\sigma_1^2\sigma_2^2$ et $\sigma_2^2\sigma_1^2$. La question est de décider si ces mots sont équivalents, donc, de façon équivalente, si le quotient $(\sigma_1^2\sigma_2^2)^{-1}(\sigma_2^2\sigma_1^2)$, c'est-à-dire $\sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$, est équivalent ou non au mot vide. Pour simplifier l'écriture, on pose $\mathtt{a} = \sigma_1$, $\mathtt{b} = \sigma_2$, ... et $\mathtt{A} = \sigma_1^{-1}$, $\mathtt{B} = \sigma_2^{-1}$, ... La question est donc de savoir si le mot $\mathtt{BBAAbbaa}$, qui comporte quatre lettres négatives, est ou non équivalent au mot vide. On utilise d'abord les relations du lemme 5 pour envoyer les facteurs Δ_3 neutraliser les lettres σ_i^{-1} :

$$\begin{aligned}
\Delta_3^4 w = \Delta_3^4.\mathtt{BBAAbbaa} &= \Delta_3.\Delta_3^3\mathtt{B}.\mathtt{BAAbbaa} \equiv \Delta_3.\mathtt{A}\Delta_3^3.\mathtt{BAAbbaa} \\
&= (\Delta_3\mathtt{A}).\Delta_3.\Delta_3^2\mathtt{B}.\mathtt{AAbbaa} \equiv (\Delta_3\mathtt{A}).\Delta_3.\mathtt{B}\Delta_3^2.\mathtt{AAbbaa} \\
&= (\Delta_3\mathtt{A}).(\Delta_3\mathtt{B}).\Delta_3.\Delta_3\mathtt{A}.\mathtt{Abbaa} \equiv (\Delta_3\mathtt{A}).(\Delta_3\mathtt{B}).\Delta_3.\mathtt{B}\Delta_3.\mathtt{Abbaa} \\
&= (\Delta_3\mathtt{A}).(\Delta_3\mathtt{B}).(\Delta_3\mathtt{B}).\Delta_3.\mathtt{Abbaa} \\
&= (\Delta_3\mathtt{A}).(\Delta_3\mathtt{B}).(\Delta_3\mathtt{B}).(\Delta_3\mathtt{A}).\mathtt{bbaa} \equiv (\mathtt{ab}).(\mathtt{ba}).(\mathtt{ba}).(\mathtt{ab}).\mathtt{bbaa}.
\end{aligned}$$

Il reste alors à voir si les mots Δ_3^4, c'est-à-dire $(\mathtt{aba})^4$, et $\mathtt{abbabaabbbaa}$ sont positivement équivalents. Pour ce faire, on peut appliquer systématiquement les relations de tresse, qui se réduisent ici à $\mathtt{aba} = \mathtt{bab}$, au mot $\mathtt{abbabaabbbaa}$, et voir si on finit par obtenir le mot Δ_3^4. Je ne vais pas le faire à la main, car ce serait fort pénible, même si, en théorie, c'est facile. Si on était courageux, ou qu'on programme un ordinateur, on constaterait, au bout d'un temps fini, qu'on n'obtient jamais Δ_3^4, et on aurait ainsi (enfin !) prouvé que les mots de tresse $\sigma_2^2\sigma_1^2$ et $\sigma_1^2\sigma_2^2$ ne sont pas équivalents, c'est-à-dire que les diagrammes qu'ils codent ne sont pas isotopes.

Remarque. Ci-dessus, on a appliqué à la lettre l'algorithme 8 pour montrer comment il fonctionne. En fait, dans le cas particulier qui nous intéressait, à savoir décider si les mots $\sigma_2^2\sigma_1^2$ et $\sigma_1^2\sigma_2^2$ sont équivalents, il n'était pas nécessaire de former le quotient, puis d'appliquer le lemme 5 : comme les deux mots considérés sont positifs, on peut directement observer qu'ils sont équivalents si et seulement ils sont positivement équivalents, et appliquer l'algorithme 4 pour le décider, ce qui est ici trivial car aucune relation de tresse ne peut s'appliquer ni à $\sigma_2^2\sigma_1^2$, ni à $\sigma_1^2\sigma_2^2$.

Deuxième partie : *des* solutions au problème d'isotopie des tresses

On vient d'obtenir une solution au problème d'isotopie des tresses. Conceptuellement, cette solution est simple, mais, en pratique, elle est franchement calamiteuse. Ce que je vais faire maintenant, c'est survoler d'autres solutions, certaines d'entre elles beaucoup plus efficaces algorithmiquement. Je vais certainement aller trop vite, mais mon espoir est que, même si vous ne suivez pas tous les détails, au moins vous ayez une petite idée de la variété des approches possibles. Cette variété est intéressante en soi parce qu'elle traduit la richesse des groupes de tresses et montre combien de jolies mathématiques y sont cachées — et, comme vous pouvez vous en douter, elle explique aussi que tout ce que je vais dire peut se généraliser dans des quantités de directions différentes.

La représentation d'Artin

Je vais commencer par une solution due à Emil Artin et qui, dans l'esprit de nos premières tentatives, repose sur la construction d'un invariant complet, c'est-à-dire associe à tout mot (ou diagramme) de tresse un certain objet — ici ce sera un automorphisme d'un groupe libre — de façon que deux mots sont équivalents si et seulement si les objets qu'on leur associe coïncident.

L'approche relève de la ***topologie algébrique***, et des mots clés sont ici ***homéomorphisme***, ***lacets***, ***groupe fondamental***.

Le point de départ est de considérer un diagramme de tresses à n brins comme le film du mouvement de n points dans un disque, comme suggéré dans la Figure 15.

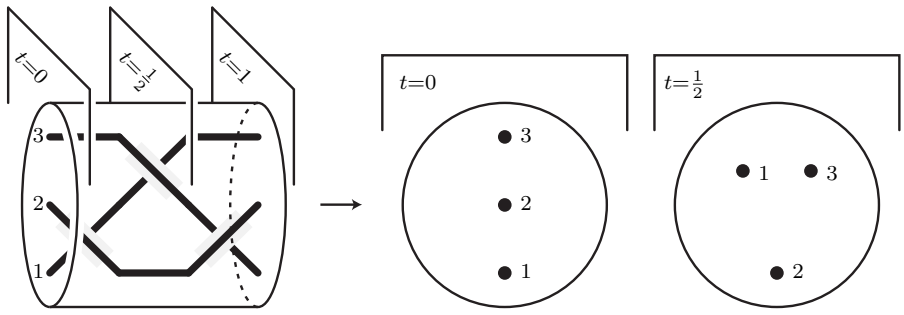

Figure 15: Tresse vue comme le film du mouvement de n points dans un disque (ici $n = 3$) : on coupe par des plans verticaux successifs, et les intersections avec les n brins donnent n points se déplaçant continûment dans le disque.

Ensuite, le mouvement de n points dans l'intérieur d'un disque peut être étendu en un homéomorphisme du disque entier : imaginez que le disque

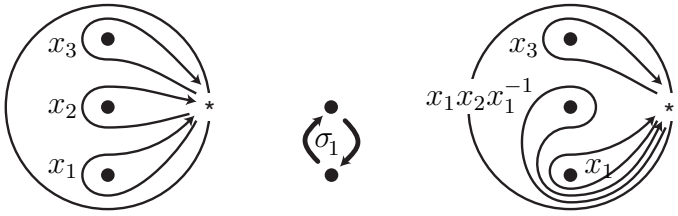

Figure 16: Générateurs standards du groupe fondamental d'un disque pointé, ici pour $n = 3$, et action de la tresse σ_1 sur ces générateurs.

est rempli de crème Mont-Blanc et que les n points sont des cuillères qu'on déplace. Comme la crème est visqueuse, les cuillères l'entraînent, et on obtient un homéomorphisme du disque dans lui-même. Cet homéomorphisme n'a aucune raison d'être unique. Par contre, si on impose qu'il soit l'identité sur le bord du disque, et qu'on le considère à isotopie près, alors il y a unicité. On obtient ainsi un isomorphisme du groupe de tresses B_n sur le groupe des classes d'isotopie d'homéomorphismes du disque à n points marqués D_n laissant ∂D_n fixe — usuellement appelé *mapping class group* de D_n.

Une tresse étant maintenant vue comme un homéomorphisme, elle agit naturellement sur les lacets de D_n, et de là sur son groupe fondamental $\pi_1(D_n)$, ensemble des classes d'isotopie de lacets de D_n (relativement à un point-base fixé) muni de la composition. En effet, soit γ un lacet de D_n et β une tresse. L'action de β sur γ est définie comme la classe d'isotopie de l'image de γ par un homéomorphisme ϕ quelconque associé à β. Cette action est bien définie : si γ et γ' sont deux lacets isotopes et si ϕ et ϕ' sont associés à la même tresse, alors $\phi(\gamma)$ et $\phi'(\gamma')$ sont isotopes.

Mais alors, ce qu'on a obtenu, c'est un homomorphisme ρ associant à toute tresse de B_n un automorphisme du groupe $\pi_1(D_n)$. Or il se trouve que le groupe fondamental de D_n est un groupe libre de rang n, dont une base est représentée dans la figure 16. Alors il suffit de lire sur la figure l'action de la tresse σ_1 sur les générateurs standards de $\pi_1(D_n)$ pour obtenir une définition explicite de ρ :

$$\rho(\sigma_i)(x_i) = x_i x_{i+1} x_i^{-1},\ \rho(\sigma_i)(x_{i+1}) = x_i,\ \rho(\sigma_i)(x_k) = x_k \text{ pour } k \neq i, i+1.$$

On a alors le résultat suivant — qui nécessite une démonstration et ne va pas de soi.

Théorème 9 (Artin, 1947). *L'homomorphisme ρ est injectif.*

Par conséquent, ρ est un invariant complet pour l'isotopie des tresses, et on en déduit une nouvelle solution au problème d'isotopie.

Algorithme 10. *Partant d'un mot de tresse à n brins w :*
- *Calculer l'image de x_i par $\rho(w)$ pour $i = 1, ..., n$;*
- *Alors $w \equiv \varepsilon$ est vrai si et seulement si on a $\rho(w)(x_i) = x_i$ pour tout i.*

Exemple. Pour $w = \sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$ comme dans l'exemple précédent, on calcule

$$\rho(w)(x_1) = x_1x_2x_1^{-1}x_3x_1x_2^{-1}x_1^{-1},$$

et on déduit immédiatement $w \not\equiv \varepsilon$, puisque le mot ci-dessus (qui est librement réduit) n'est pas x_1.

Tout comme l'algorithme 8, l'algorithme 10 est peu efficace en pratique : dans le pire cas, la longueur des mots $\rho(w)(x_i)$ est exponentielle en la longueur du mot de départ w, et l'algorithme est donc au moins de complexité exponentielle.

Les représentations linéaires

Je voudrais maintenant discuter une autre approche classique, à savoir étudier les représentations linéaires des groupes de tresses. C'est un moyen très naturel d'aborder le problème d'isotopie puisque, si on trouve une représentation fidèle (c'est-à-dire injective), alors, pour reconnaître si un mot est équivalent au mot vide, il suffit de calculer la matrice associée et de voir si c'est la matrice-identité.

Cette section relève donc d'une approche d'***algèbre linéaire***, et les mots clés sont ici ***matrice***, ***fidélité***, et également, dans le cas spécifique qu'on va développer, ***loi d'autodistributivité***.

Dans le cas des groupes de tresses, l'étude des représentations linéaires est un sujet ancien et difficile, et je vais me contenter ici introduire la plus ancienne et classique des représentations, à savoir la représentation de Burau. Pour ce faire, je vais utiliser le coloriage des tresses, une idée très simple et naturelle qui remonte au moins à Alexander au début du XXe siècle.

Le principe est le suivant. On attribue des couleurs aux extrémités gauches de chacun des brins d'un diagramme de tresse et on fixe des règles pour propager les couleurs vers la droite. Par exemple, si on décide que les couleurs sont propagées sans modification le long des brins, alors, sous réserve que les couleurs d'entrée soient deux à deux distinctes, on obtient en sortie une permutation des couleurs d'entrée. Cette permutation est la projection de la tresse considérée dans le groupe symétrique déjà considérée — et on a vu qu'elle ne résout le problème d'isotopie puisque des tresses distinctes, par exemple σ_1 et σ_1^{-1}, ont la même permutation.

Une autre règle, plus intéressante, consiste à décider que, lors des croisements, les couleurs des brins interagissent. On va considérer le cas le plus simple, celui où seulement une des deux couleurs, par exemple celle du brin

de devant, peut changer. Cela revient à dire que, si C est l'ensemble des couleurs, on a une opération binaire $\star$ sur C et que, quand un brin de couleur y passe devant un brin de couleur x, alors sa couleur devient $x \star y$.

Une telle règle permet de colorier n'importe quel diagramme de tresse — pour le moment, on ne considère que les croisements positifs. Mais ce qu'on souhaite, c'est colorier les tresses, et pas les diagrammes de tresses. Cela veut dire qu'on veut que, si on applique les mêmes couleurs en entrée à deux diagrammes isotopes, alors les couleurs de sortie soient également les mêmes. Or il est facile de voir quelles conditions doit vérifier l'opération sur les couleurs pour que ce soit le cas (voir la figure 17).

Lemme 11. *L'opération $\star$ donne un coloriage de B_n^+, c'est-à-dire, est compatible avec les relations de tresse, si et seulement si elle satisfait la loi (#) :* $x \star (y \star z) = (x \star y) \star (x \star z)$.

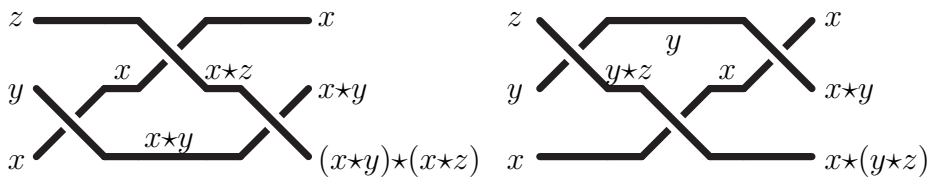

Figure 17: La loi (#) garantit la compatibilité avec $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$.

On est donc conduit à chercher des opérations satisfaisant la loi (#) (appelée *autodistributivité*). L'opération $x \star y = y$, qui correspond au cas où les couleurs ne changent pas, est un exemple trivial.

Un autre exemple est obtenu en prenant pour C un groupe et pour $\star$ la conjugaison, c'est-à-dire en posant $x \star y = xyx^{-1}$. En particulier, on peut prendre comme groupe un groupe libre à n générateurs $x_1, ..., x_n$. Alors, si on part des couleurs d'entrée $x_1, ..., x_n$, les couleurs de sortie sont exactement les images des x_i par l'automorphisme ρ de la section précédente. Autrement dit, on réobtient ainsi la représentation d'Artin, et donc une solution au problème d'isotopie des tresses.

Un nouvel exemple, qui va nous mener à une représentation linéaire de B_n, consiste à prendre pour C un $\mathbb{Z}[t]$-module et à poser

$$x \star y = (1 - t)x + ty.$$

On vérifie que l'opération $\star$ satisfait à la loi (#), et donc on obtient à nouveau un coloriage des tresses. Or, par construction, les couleurs de sortie sont ici des combinaisons linéaires des couleurs d'entrée. De la sorte, on associe à toute tresse (positive) une matrice, à savoir la matrice qui décrit les couleurs de sortie en termes des couleurs d'entrée. Passer aux tresses quelconques, c'est-à-dire traiter les croisements négatifs, est facile, pour

autant qu'on puisse inverser le paramètre formel t, et, finalement, on obtient ce qu'on appelle la *représentation de Burau* des tresses, un homomorphisme de B_n dans le groupe linéaire $\mathrm{GL}_n(\mathbb{Z}[t, t^{-1}])$.

La question pour nous ici est de savoir si cette représentation fournit une solution au problème d'isotopie, c'est-à-dire si la représentation de Burau est injective — pour les représentations linéaires, on emploie plutôt le terme synonyme « fidèle ». Autrement dit, est-ce que deux tresses distinctes sont toujours envoyées sur des matrices distinctes ? Dans le cas de tresses à trois brins, la réponse est positive. Au-delà, la question est restée ouverte pendant près de cinquante ans, jusqu'à ce que J. Moody montre, en 1991, que la représentation de Burau n'est *pas* fidèle pour B_{10}, résultat ultérieurement amélioré à B_5 (dans le cas de B_4, la question est toujours ouverte).

Par conséquent, la représentation de Burau ne fournit *pas* de solution au problème d'isotopie des tresses. Par contre, l'idée d'utiliser des représentations linéaires est valable, car on sait depuis quelques années qu'il existe d'autres représentations linéaires des groupes de tresses qui, elles, sont fidèles et donnent donc une solution au problème d'isotopie [19, 5, 20].

Théorème 12 (Krammer, Bigelow, 2000). *Il existe une représentation linéaire fidèle de B_n dans $\mathrm{GL}_{n(n-1)/2)}(\mathbb{Z}[t, t^{-1}, q, q^{-1}])$.*

On en déduit une nouvelle solution au problème d'isotopie des tresses : partant d'un mot de tresse w, on calcule la matrice qui est son image par la représentation de Krammer, et on conclut que w est équivalent au mot vide si et seulement si la matrice obtenue est la matrice identité.

Comme le groupe de matrices dans lequel on plonge les tresses est très gros, cette solution est peu efficace en pratique. Mais, d'un point de vue théorique, c'est un résultat majeur de savoir que les groupes de tresses peuvent être réalisés comme groupes de matrices.

La forme normale gloutonne

Je passe à une solution d'un type tout à fait différent, à savoir basée sur une forme normale : pour chaque tresse β, on va construire, de façon effective, un mot particulier qui la représente, appelé la *forme normale gloutonne* de β (« greedy normal form » en anglais). Ceci donne immédiatement une solution au problème d'isotopie : étant donné un mot de tresse w, on détermine l'unique mot normal w_0 équivalent à w, et on a alors $w \equiv \varepsilon$ si et seulement si w_0 est le mot normal représentant la tresse triviale, en l'occurrence le mot vide.

Cette approche relève principalement de la ***combinatoire du groupe symétrique*** et de la ***théorie des monoïdes***, avec des mots clés tels que ***permutation***, ***groupe symétrique***, ***descentes***, ainsi que ***divisibilité*** et ***pgcd***.

Elle est issue des travaux de Garside, mais sa forme actuelle a été redécouverte plusieurs fois et on peut citer les noms d'Adjan, Thurston, ElRifai et Morton, et peut-être d'autres encore [3, 14]. La toile de fond est la théorie des groupes automatiques développée par Cannon et Thurston vers la fin des années 1980, bâtie précisément à partir de l'exemple des groupes de tresses, voir [15].

Une conséquence des théorèmes 6 et 7 est que le monoïde B_n^+ s'identifie au sous-monoïde de B_n formé par les tresses qui ont au moins une expression où aucune lettre négative σ_i^{-1} n'apparaît. Ces tresses sont naturellement appelées tresses *positives*. Dans un premier temps, on va s'intéresser exclusivement aux tresses positives, et construire une forme normale pour celles-ci, c'est-à-dire une forme normale dans le monoïde B_n^+.

On a vu qu'on peut projeter B_n sur le groupe des permutations de $\{1, ..., n\}$. Cette projection n'est *pas* injective : une infinité de tresses réalisent chaque permutation. Néanmoins, on peut toujours choisir, pour chaque permutation π, une tresse particulière $[\pi]$ qui la réalise. De plus, on peut facilement s'arranger pour que les tresses ainsi obtenues soient positives, et que la longueur de $[\pi]$ (nombre de lettres σ_i dans une expression quelconque par un mot positif) soit exactement le nombre d'inversion de la permutation π. On vérifie alors qu'il n'y a qu'une façon de remplir ces conditions, et on obtient ainsi une famille bien définie de $n!$ tresses qui sont en bijection avec chacune des $n!$ permutations de $\{1, ..., n\}$, et qu'on appellera *tresses de permutation*.

Dans le monoïde B_n^+, on a une notion naturelle de divisibilité : on dit qu'une tresse positive β *divise* (à gauche) une tresse positive β' s'il existe une tresse positive γ vérifiant $\beta' = \beta\gamma$. On a alors une relation simple entre les tresses de permutation et la tresse Δ_n de la figure 14.

Lemme 13. *Les $n!$ tresses de permutation de B_n^+ sont les diviseurs de Δ_n dans B_n^+.*

En particulier, la tresse Δ_n est la tresse de permutation associé à la permutation demi-tour $(n, ..., 1)$. Le point crucial pour la construction d'une forme normale dans le monoïde B_n^+ et, de là, dans le groupe B_n, est le résultat suivant.

Théorème 14 (Garside, 1969). *Deux tresses positives quelconques admettent un unique pgcd dans B_n^+.*

(Garside montre aussi que deux tresses positives admettent un ppcm, de sorte que B_n^+ muni de la relation de divisibilité est, tout comme les nombres entiers, un treillis.)

Supposons alors que β est une tresse distincte de 1 dans B_n^+. Alors, par le théorème 14, β et Δ_n ont un pgcd qui, par construction, est un diviseur

de Δ_n. Donc, par le lemme 13, ce pgcd est une tresse de permutation. On obtient ainsi une décomposition distinguée $\beta = [\pi_1] \cdot \beta'$, où π_1 est une permutation. On procède de même avec β' s'il est non-trivial, obtenant $\beta' = [\pi_2] \cdot \beta''$, et ainsi de suite. Après un nombre fini d'étapes, on obtient une décomposition

$$\beta = [\pi_1] \cdot ... \cdot [\pi_d]$$

qui associe à chaque tresse positive une suite finie de tresses de permutations. Inversement, toute suite finie de tresses de permutations ne s'obtient pas ainsi, mais on a la caractérisation suivante :

Théorème 15 (Thurston, Morton-ElRifai, 1988). *Toute tresse de B_n admet une unique expression de la forme $\Delta_n^p \cdot [\pi_1] \cdot ... \cdot [\pi_d]$ telle que π_1 n'est pas la permutation $(n, ..., 1)$, π_d n'est pas l'identité, et, pour chaque r, on a $\pi_r(i) > \pi_r(i+1)$ dès qu'on a $\pi_{r+1}^{-1}(i) > \pi_{r+1}^{-1}(i+1)$ (« tout recul de π_{r+1} est une descente de π_r »).*

L'expression donnée par le théorème 15 est appelée la *forme normale gloutonne* de la tresse considérée. Le point fondamental est que la condition de normalité du théorème 15 est une condition locale et, à ce titre, elle est reconnaissable par un automate fini, et calculable par un transducteur : il existe un programme fini qui, à partir de la forme normale d'une tresse β et d'un générateur $\sigma_i^{\pm 1}$, fournit la forme normale de la tresse $\beta\sigma_i^{\pm 1}$. On déduit une nouvelle solution au problème d'isotopie des tresses :

Algorithme 16. *Partant d'un mot de tresse à n brins w :*

- *Calculer la forme normale de w incrémentalement ;*
- *Alors on a $w \equiv \varepsilon$ si et seulement si cette forme normale est Δ_n^0.*

Exemple. Reprenant l'exemple habituel $w = \sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$, on calcule de proche en proche la forme normale de σ_2^{-1}, qui est $\Delta_3^{-1}.[3,1,2]$ — en notant $[3,1,2]$ la tresse de permutation associée à la permutation $(3,1,2)$ — puis celle de σ_2^{-2}, etc., puis finalement celle de w, qui se trouve être

$$\Delta_3^{-3}.[3,1,2].[2,1,3].[2,3,1].[1,3,2].[3,1,2].[2,1,3].$$

Cette dernière n'est pas Δ_3^0, c'est-à-dire 1, et on a une nouvelle demonstration de la non-trivialité de w.

La mise en forme normale est une méthode très efficace d'un point de vue algorithmique, au moins pour les petites valeurs du nombre de brins n. En effet, comme il peut être effectué par un transducteur, l'ajout d'un générateur $\sigma_i^{\pm 1}$ a un coût linéaire et, par conséquent, le calcul de la forme normale d'une tresse représentée par un mot de longueur ℓ a un coût quadratique en ℓ, à n fixé. Par contre, il existe $n!$ tresses de permutation, et la complexité des automates mis en jeu augmente très vite avec n.

Le retournement de sous-mot

Je vais maintenant décrire une solution appartenant à une nouvelle famille, à savoir les systèmes de récriture et, plus précisément, les méthodes de *réduction*. Dans ce type d'algorithme, le principe n'est pas de construire une forme normale, mais simplement d'effectuer des transformations syntaxiques sur le mot de départ de façon à pouvoir conclure qu'il est équivalent au mot vide si et seulement si, à l'issue des transformations, on a obtenu le mot vide — en d'autres termes, on a réduit le mot initial au mot vide.

La méthode qu'on va décrire est typique d'une approche de ***système de réécriture***, tout en étant fondée sur des intuitions de ***théorie combinatoire des groupes*** ; des mots clés sont ici ***confluence***, ***terminaison***, et, à l'arrière plan, ***diagramme de van Kampen***.

Développée dans [8], cette solution très facile à implémenter sur un ordinateur est appelée *retournement de sous-mot* car elle consiste à prendre des sous-mots particuliers du mot de départ, et à les retourner en un certain sens qu'on va définir. La transformation est purement syntaxique, mais il est commode de la décrire en s'aidant de dessins. Pour cela, on associe à chaque lettre σ_i le motif $\xrightarrow{\sigma_i}$ et à chaque lettre σ_i^{-1} le motif $\downarrow_{\sigma_i}$. Puis, on associe à tout mot de tresse w le graphe en forme d'escalier obtenu en mettant bout à bout les motifs associés aux lettres successives de w, comme surligné en gris foncé dans la figure 19.

Partant d'un tel escalier, on complète ensuite le dessin, de proche en proche et autant que faire se peut, en appliquant les règles de la figure 18.

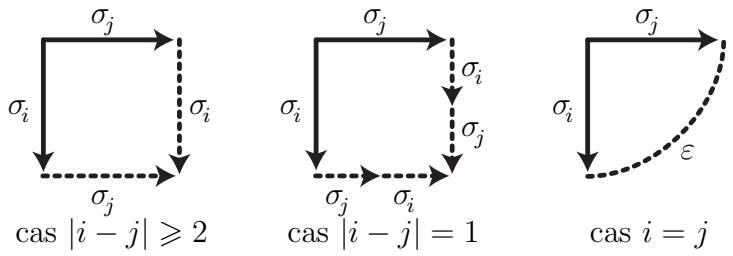

Figure 18: Règles du retournement : on complète les motifs ouverts (traits pleins) à l'aide des flèches en pointillé, en fonction des étiquettes ; les arcs étiquetés ε sont ignorés dans la suite.

La figure 19 donne un exemple. Lorsqu'on lit les étiquettes des escaliers successifs obtenus en partant en bas à gauche et en se dirigeantvers le haut et la droite, les mots obtenus sont ceux qui se dérivent à partir du mot initial w en appliquant les règles de réécriture

$$\sigma_i^{-1}\sigma_j \mapsto \begin{cases} \sigma_j\sigma_i^{-1} & \text{pour } |i-j| \geqslant 2, \\ \sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1} & \text{pour } |i-j| = 1, \\ \varepsilon & \text{pour } i = j. \end{cases}$$

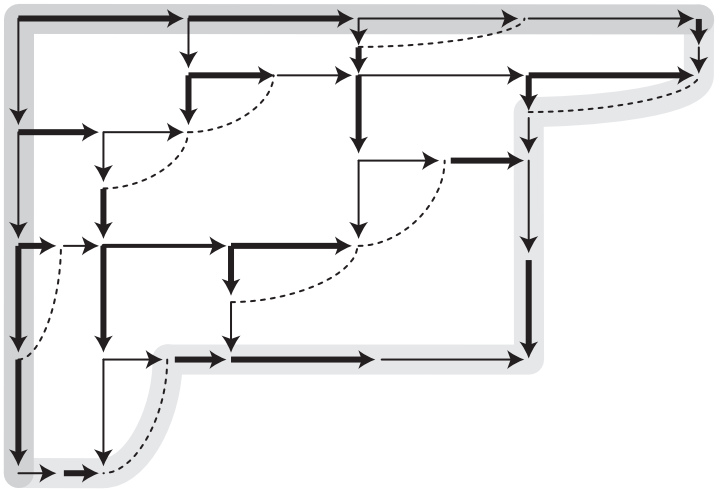

Figure 19: Retournement du mot $\sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$. Les flèches fines correspondent à σ_1, les flèches épaisses à σ_2. Les pointillés correspondent au mot vide ε, et ne sont pas pris en compte (leurs extrémités sont considérées comme identifiées). On part avec l'escalier, ici à une seule marche, associé au mot de départ, surligné en gris foncé, puis, de proche en proche, on complète le diagramme à l'aide des règles de la figure 18. On aboutit au chemin surligné en gris clair, qui ne peut plus être complété.

En d'autres termes, on transforme de proche en proche les sous-mots de w de type $-+$ (une lettre négative suivie par une lettre positive) pour les retourner en un mot de type $+-$ (des lettres positives suivies par des lettres négatives). On écrira $w \curvearrowright w'$ lorsque w' s'obtient ainsi à partir de w, et on dira que w *se retourne en* w'. Noter que $w \curvearrowright w'$ entraîne $w \equiv w'$: le retournement est une forme (très) particulière d'équivalence.

Les mots terminaux vis-à-vis du retournement sont les mots n'admettant pas de sous-mot de type $-+$, et ce sont donc les mots de la forme uv^{-1} avec u et v positifs. Le retournement a deux propriétés importantes. La première, qui résulte de l'unicité du diagramme de la figure 19, est la confluence : si un mot se retourne en un mot terminal, alors celui-ci est unique. Plus difficile est la question de la terminaison, c'est-à-dire la question de savoir si tout mot se réécrit en un mot terminal. Pour l'aborder, on montre d'abord le résultat d'invariance suivant, qui est lié à la théorie de Garside.

Lemme 17. *Supposons que u, u', v, v' sont des mots de tresse positifs vérifiant $u^{-1}v \curvearrowright v'u'^{-1}$. Alors, quels que soient les mots positifs u_*, v_* vérifiant $u_* \equiv^+ u$ et $v_* \equiv^+ v$, il existe des mots positifs u'_*, v'_* vérifiant $u'_* \equiv^+ u'$ et $v'_* \equiv^+ v'$, et $u_*^{-1}v_* \curvearrowright v'_*u'^{-1}_*$.*

A partir de là, on déduit facilement

Théorème 18. *Tout mot de tresse se retourne en un unique mot terminal.*

Le principe de la démonstration est le suivant. D'abord, on observe que, si u et v sont des mots positifs équivalents, alors on a $u^{-1}v \curvearrowright \varepsilon$. En effet, par construction, on a $v^{-1}v \curvearrowright \varepsilon$, c'est-à-dire $v^{-1}v \curvearrowright \varepsilon\varepsilon^{-1}$, et donc le lemme 17 entraîne qu'il existe u', v' vérifiant $u' \equiv^+ \varepsilon$, $v' \equiv^+ \varepsilon$, et $u^{-1}v \curvearrowright v'u'^{-1}$. Comme ε n'est équivalent à aucun mot positif autre que lui-même, on a nécessairement $u' = v' = \varepsilon$, ce qui est le résultat annoncé.

Ensuite, on considère le cas particulier où w est de la forme $u^{-1}v$ avec u et v positifs. Ainsi qu'on l'a déjà vu, il résulte du lemme 5 que deux éléments du monoïde B_n^+ admettent toujours un multiple à droite commun, donc il existe deux mots positifs u', v' vérifiant $uv' \equiv^+ vu'$. D'après ce qui précède, ceci entraîne que le retournement du mot $(uv')^{-1}(vu')$ doit se terminer avec le mot vide. Mais il est facile de voir que le retournement de $(uv')^{-1}(vu')$ ne peut se terminer que si le retournement de son sous-mot $u^{-1}v$, c'est-à-dire celui de w, se termine également.

Enfin, le cas d'un mot w quelconque se traite par une récurrence facile sur l'indice p tel que w s'écrive $u_1^{-1}v_1...u_p^{-1}v_p$, c'est-à-dire sur le nombre de marches de l'escalier associé à w.

Une fois le théorème 18 démontré, il est facile d'obtenir une solution au problème d'isotopie des tresses. En effet, soit w un mot de tresse quelconque, et soient u, v les (uniques) mots positifs tels que w se retourne en uv^{-1} — qui existent d'après le théorème 18. On a alors la chaîne d'équivalences

$$w \equiv \varepsilon \Leftrightarrow uv^{-1} \equiv \varepsilon \Leftrightarrow u \equiv v \Leftrightarrow u \equiv^+ v \Leftrightarrow v^{-1}u \curvearrowright \varepsilon,$$

et on en déduit l'algorithme suivant, qui consiste en un double retournement.

Algorithme 19. *Partant d'un mot de tresse w :*

- *Retourner w en uv^{-1} avec u, v positifs — c'est-à-dire appliquer les règles du retournement au mot w jusqu'à obtenir un mot de la forme « tout positif suivi de tout négatif » ;*
- *Retourner $v^{-1}u$ en $u'v'^{-1}$ avec u', v' positifs ;*
- *Alors on a $w \equiv \varepsilon$ si et seulement si le mot $u'v'^{-1}$ est le mot vide.*

Exemple. Pour notre exemple usuel, $w = \sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$, et avec les conventions $\mathtt{a} = \sigma_1$, $\mathtt{b} = \sigma_2$, $\mathtt{A} = \sigma_1^{-1}$, ... , on obtient (voir la figure 19)

`BBAAbbaa` $\curvearrowright$ `abbbaBAAAB`,

puis, après avoir permuté les facteurs positifs et négatifs,

`BAAABabbba` $\curvearrowright$ `BBAAbbaa`.

Le dernier mot (qui se trouve coïncider avec le mot initial w) n'est pas vide : on conclut que w n'est pas équivalent au mot vide.

Du point de vue algorithmique, la méthode a, tout comme la mise en forme normale, une complexité quadratique à n fixé. La complexité par rapport à n est inconnue à ce jour.

La réduction des poignées

Je vais maintenant mentionner brièvement une autre méthode de réduction, dite *réduction des poignées*. En un sens, cette méthode est assez analogue au retournement : on conclut qu'un mot de tresse est trivial si et seulement si, à l'issue de la réduction, on a obtenu le mot vide. La principale différence est que la méthode de réduction des poignées est *beaucoup* plus efficace en pratique. C'est même la solution la plus efficace à ce jour dans le cas de mots de tresse de très grande taille — et on peut la tester à l'adresse [21]. Le prix à payer pour cette efficacité est qu'il est beaucoup plus difficile de démontrer la terminaison de la réduction, et je n'essaierai pas de le faire ici. En sus de la théorie de Garside, on utilise un certain ordre sur les tresses qui pilote la réduction et permet d'arriver au plus vite à un mot terminal, ordre qui est issu, au terme d'un chemin fort tortueux, de travaux effectués il y a fort longtemps par l'auteur sur les grands cardinaux en théorie des ensembles [12]. Le cadre général ici est donc la ***théorie géométrique des groupes*** et la ***théorie des groupes ordonnés***, et des mots clés seraient ***graphe de Cayley*** et ***tresse σ-positive***.

Définition. (Figure 20) On dit qu'un mot de tresse v est une *σ_i-poignée* s'il est de la forme $\sigma_i^e u \sigma_i^{-e}$, où e est ± 1 et où u ne contient aucune lettre $\sigma_j^{\pm 1}$ avec $j \geqslant i$, et contient au plus une des deux lettres σ_{i-1} ou σ_{i-1}^{-1}. On définit alors la *réduction* de v comme le mot $\mathrm{red}(v)$ obtenu à partir de v en

- supprimant les lettres σ_i et σ_i^{-1}, et
- remplaçant chaque lettre $\sigma_{i-1}^{\pm 1}$ par $\sigma_{i-1}^{-e}\sigma_i^{\pm 1}\sigma_{i-1}^{e}$.

Si w, w' sont des mots de tresse, on dit que w' est obtenu par une réduction de poignée à partir de w s'il existe un sous-mot v de w qui est une poignée et que w' est obtenu à partir de w en remplaçant ce sous-mot par le mot $\mathrm{red}(v)$.

Il est clair que, si w' est obtenu à partir de w par (une ou plusieurs) réduction de poignée, alors w et w' sont équivalents. Par ailleurs, les mots de la forme $\sigma_i\sigma_i^{-1}$ ou $\sigma_i^{-1}\sigma_i$ sont des cas particuliers de poignée, dont la

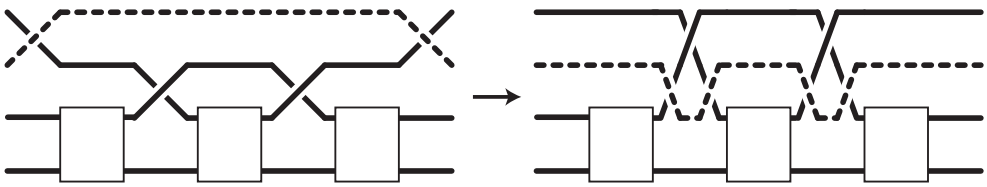

Figure 20: Une poignée, ici une σ_3-poignée, et sa réduction. Le brin en pointillé (celui qui a la forme de la poignée d'une valise) est poussé vers le bas pour contourner les croisements situés juste en-dessous.

réduction est le mot vide : la réduction de poignée est une généralisation de la réduction libre. Le résultat principal est le suivant.

Théorème 20 ([9]). • *Un mot de tresse ne contenant pas de poignée est équivalent au mot vide si et seulement si il est le mot vide.*

• *Toute suite de réductions de poignée aboutit en un nombre fini d'étapes à un mot ne contenant pas de poignée.*

Une solution au problème d'isotopie des tresses s'en déduit immédiatement.

Algorithme 21. *Partant d'un mot de tresse w :*

- *Réduire les poignées de w jusqu'à obtenir un mot w' sans poignée ;*
- *Alors on a $w \equiv \varepsilon$ si et seulement si w' est le mot vide.*

Exemple. Pour notre exemple usuel, $w = \sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$, et en choisissant de réduire la poignée la plus à gauche possible, on obtient la suite des mots suivants où, à chaque fois, on a souligné la poignée qui va être réduite :

BBAAbbaa, BaBAaBabaa, BaBBabaa, BaBaBAaa, BaBaBa.

Le dernier mot obtenu ne contient pas de poignée, et n'est pas vide, donc on conclut, une fois de plus, que w n'est pas équivalent au mot vide.

Les coordonnées de Dynnikov

Pour revenir vers la géométrie, je vais maintenant présenter une solution complètement différente de tout ce que on a vu jusqu'à présent. Cette solution, proposée par Ivan Dynnikov vers 2000, relève principalement de la ***théorie des surfaces***, et des mots clés sont ici ***lamination***, ***triangulation***, ***flip***, ainsi que — et c'est très inattendu — ***algèbre tropicale***.

L'approche repose sur l'étude des triangulations d'un espace topologique, et elle est liée à des résultats de Lee Mosher sur les mapping class groups. Le contexte est à nouveau celui des tresses vues comme homéomorphismes d'un disque pointé D_n, l'idée étant maintenant de faire agir la tresse sur une famille de courbes tracées dans D_n et de compter leurs intersections de ces courbes avec une triangulation fixée pour obtenir des sortes de coordonnées de la tresse.

Pour tout entier x, on pose $x^+ = \max(x, 0)$ et $x^- = \min(x, 0)$.

Définition. On introduit des fonctions F^+ et F^- de $\mathbb{Z}^4$ dans $\mathbb{Z}^4$ par $F^+ = (F_1^+, ..., F_4^+)$, $F^- = (F_1^-, ..., F_4^-)$ avec

$$
\begin{aligned}
F_1^+(x_1, y_1, x_2, y_2) &= x_1 + y_1^+ + (y_2^+ - z_1)^+, & F_2^+(x_1, y_1, x_2, y_2) &= y_2 - z_1^+,\\
F_3^+(x_1, y_1, x_2, y_2) &= x_2 + y_2^- + (y_1^- + z_1)^-, & F_4^+(x_1, y_1, x_2, y_2) &= y_1 + z_1^+,\\
F_1^-(x_1, y_1, x_2, y_2) &= x_1 - y_1^+ - (y_2^+ + z_2)^+, & F_2^-(x_1, y_1, x_2, y_2) &= y_2 + z_2^-,\\
F_3^-(x_1, y_1, x_2, y_2) &= x_2 - y_2^- - (y_1^- - z_2)^-, & F_4^-(x_1, y_1, x_2, y_2) &= y_1 - z_2^-,
\end{aligned}
$$

où on a posé $z_1 = x_1 - y_1^- - x_2 + y_2^+$ et $z_2 = x_1 + y_1^- - x_2 - y_2^+$.

Ensuite, on définit une action des mots de tresse à n brins sur $\mathbb{Z}^{2n}$ par

$$\sigma_i^e \cdot (a_1, b_1, ..., a_n, b_n) = (a'_1, b'_1, ..., a'_n, b'_n)$$

avec $a'_k = a_k$ et $b'_k = b_k$ pour $k \neq i, i+1$, et

$$(a'_i, b'_i, a'_{i+1}, b'_{i+1}) = \begin{cases} F^+(a_i, b_i, a_{i+1}, b_{i+1}) & \text{pour } e = +1, \\ F^-(a_i, b_i, a_{i+1}, b_{i+1}) & \text{pour } e = -1. \end{cases}$$

Finalement, on définit les *coordonnées* d'un mot de tresse à n brins w comme la suite $w \cdot (0, 1, 0, 1, ..., 0, 1)$.

Les formules ci-dessus paraissent effroyables — et on peut se demander quel extra-terrestre a pu les inventer. En fait, on peut noter que ces formules sont faciles à implémenter, ne mettant en jeu que les opérations max et + sur les entiers, et aucune multiplication ni *a fortiori* division. Le résultat fondamental est

Théorème 22 (Dynnikov, 2000). *Les coordonnées d'un mot de tresse ne dépendent que de la tresse qu'il représente, et elles caractérisent celle-ci.*

On obtient une nouvelle solution au problème d'isotopie.

Algorithme 23. *Partant d'un mot de tresse à n brins w :*
- *Calculer la suite des $2n$ coordonnées de w ;*
- *Alors on a $w \equiv \varepsilon$ si et seulement si cette suite est $(0, 1, 0, 1, ..., 0, 1)$.*

Exemple. Reprenant encore une fois l'exemple $w = \sigma_2^{-2}\sigma_1^{-2}\sigma_2^2\sigma_1^2$, on trouve que les coordonnées de w sont $(1, -19, -12, 9, 0, 13, 0, 1)$. Cette suite n'est pas $(0, 1, 0, 1, ..., 0, 1)$, donc w n'est pas trivial.

La méthode des coordonnées de Dynnikov est très efficace algorithmiquement : elle est à la fois quadratique en temps et linéaire en espace, et cela *indépendamment* de n à la différence de la forme normale ou du retournement.

Je ne vais pas démontrer les formules de Dynnikov, mais je voudrais expliquer d'où elles viennent. C'est ce point qui paraît mystérieux, et qui est le plus intéressant car, en fait, une fois les formules devinées, on peut toujours vérifier le théorème 22 par des calculs fastidieux mais élémentaires.

Comme pour la représentation d'Artin, on considère une tresse β comme un homéomorphisme du disque pointé D_n, mais, cette fois, on fait agir β sur la famille de courbes (ou lamination) L représentée sur la figure 21.

Ce faisant, on obtient une nouvelle lamination $\beta(L)$, et l'idée est de compter les intersections entre $\beta(L)$ et une triangulation fixée T de D_n —

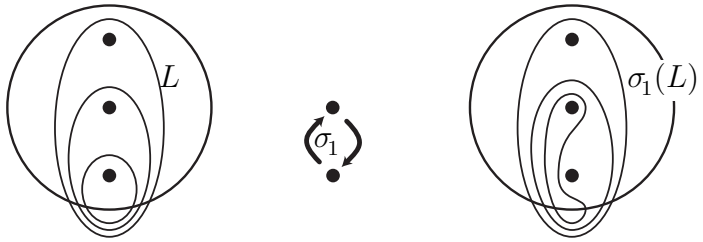

Figure 21: La lamination L, une collection de n courbes entourant les points marqués du disque points D_n (ici $n = 3$), et son image par la tresse σ_1.

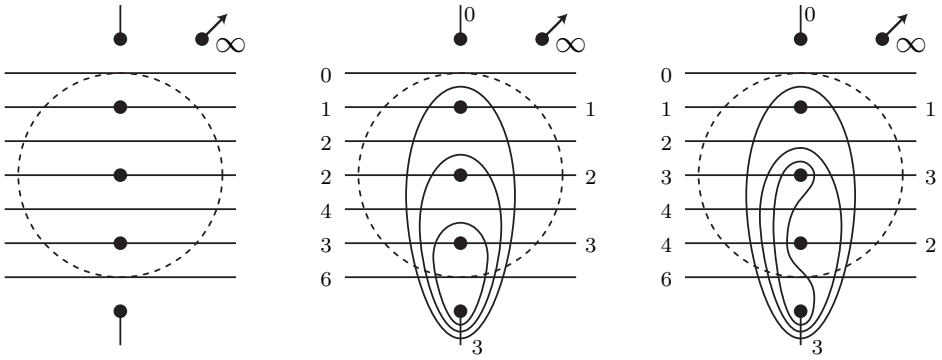

Figure 22: La triangulation T. Son allure est inhabituelle, car un des sommets est un point à l'infini, et certains des triangles ont deux sommets confondus ; au total, il y a $n + 1$ droites horizontales, $2n$ demi-droites horizontales, et 2 demi-droites verticales. Les nombres d'intersection respectifs des laminations L et $\sigma_1(L)$ avec les arêtes de T sont indiqués sur les figures de droite.

ou plutôt d'une sphère dans laquelle on plonge D_n — servant de repère de base et représentée sur la figure 22. La triangulation T possède $n + 3$ sommets, qui sont les n points marqués de D_n auxquels on rajoute deux points hors de D_n et un point à l'infini, et $3n + 3$ arêtes.

Dès qu'on a une famille de courbes tracées sur la sphère où D_n est plongé, on peut compter les intersections entre ces courbes et les $3n + 3$ arêtes de la triangulation T, obtenant ainsi $3n + 3$ entiers positifs ou nuls. Un résultat standard issu de la théorie des surfaces de Nielsen–Thurston garantit que, pourvu que les courbes soient convenablement disposées par rapport aux arêtes (pas de contact ou de digone), ces nombres déterminent la classe d'isotopie de la famille de courbes considérée. Le principe est alors d'utiliser les nombres d'intersection de la lamination $\beta(L)$ avec T comme des coordonnées pour la tresse β. En fait, en passant à des demi-différences convenables, on peut remplacer les $3n + 3$ entiers naturels précédents par $2n$ entiers relatifs. Donc, finalement, on a une méthode géométrique qui permet d'associer à toute tresse à n brins une suite de $2n$ entiers relatifs.

Pour en déduire une solution au problème d'isotopie, la question est

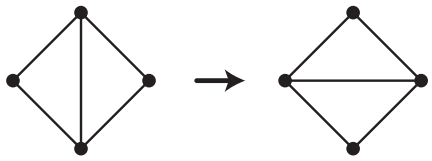

Figure 23: Un flip : l'échange des diagonales dans le quadrilatère formé par deux triangles adjacents.

d'être capable de calculer effectivement ces coordonnées — et c'est là que les choses sont jolies. En vue d'une récurrence, le problème de base est de calculer les coordonnées de $\beta\sigma_i$ à partir de celles de β. Ce problème est un cas particulier du problème général de calculer, pour n'importe quelle famille de courbes C, les coordonnées de $\sigma_i(C)$ à partir de celles de C, c'est-à-dire de comparer les intersections de $\sigma_i(C)$ et de C avec la triangulation de base T. Or σ_i est un homéomorphisme, donc, pour chaque arête e de T, on a

$$\#(\sigma_i(C) \cap e) = \#(C \cap \sigma_i^{-1}(e)).$$

Par conséquent, au lieu de comparer les intersections de C et $\sigma_i(C)$ avec T, il suffit de comparer les intersections de C avec les deux triangulations T et $\sigma_i^{-1}(T)$. Or ceci est facile. En effet, on sait qu'on peut toujours passer d'une triangulation à une autre par une suite finie de *flips*, définis comme l'opération de changer de diagonale dans le quadrilatère formé par deux triangles adjacents (figure 23). Donc on peut certainement passer de T à $\sigma_i^{-1}(T)$ par une suite finie de flips, et, de fait, on trouve facilement une suite de quatre flips qui effectue le passage souhaité (figure 24).

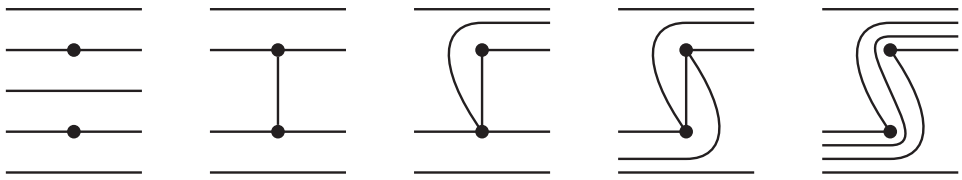

Figure 24: Passage de T à $\sigma_i^{-1}(T)$ par une suite de quatre flips ; à cause du point à l'infini et des sommets confondus, il faut un peu de temps pour se convaincre que chacune des opérations est bien un flip.

A ce point, il ne reste donc plus qu'à étudier comment les nombres d'intersection sont modifiés lorsqu'on effectue un flip, et c'est là que l'algèbre tropicale va faire son apparition.

Lemme 24. *Si C est une famille de courbes tracées sur une surface triangulée, et que $x_1, ..., x_4$, x, x' sont les nombres d'intersection de C avec les arêtes $e_1, ..., e_4, e, e'$ de la figure* 25*, alors on a*

$$x + x' = \max(x_1 + x_3, x_2 + x_4).$$

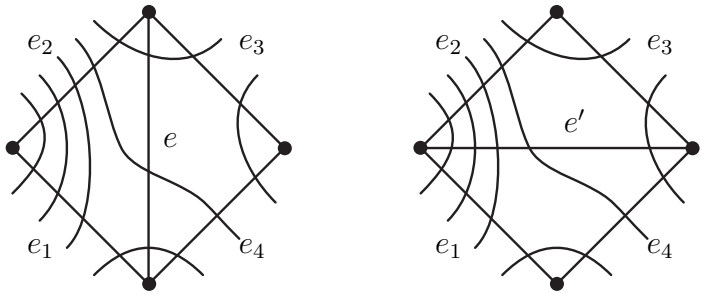

Figure 25: Relation entre les nombres d'intersection d'une famille de courbes avec les arêtes d'une triangulation lorsqu'un flip est opéré. Ici, on a $x_1 = 4$, $x_2 = 5$, $x_3 = 2$, $x_4 = 3$, $x = 3$, et $x' = 5$: on trouve bien $3+5 = \max(4+2, 5+3)$.

La vérification est aisée. Et on comprend maintenant d'où viennent les mystérieuses formules de Dynnikov, et en particulier le fait qu'elles mettent en jeu les opérations max et +. La formule du lemme 24 est simple, car un seul flip est considéré ; par contre, pour aller de T à $\sigma_i^{-1}(T)$, il faut quatre flips, et c'est l'empilement de quatre étages successifs qui aboutit aux étonnantes formules du début de la section.

La forme normale de Fromentin

Pour terminer, je vais encore mentionner brièvement deux autres solutions, histoire de citer des résultats très récents qui montrent que l'étude est loin d'être close. Je commence par des résultats algébriques de type forme normale. Les mots clés ici sont ***monoïde dual*** et ***conjugaison par l'élément de Garside***.

Tout à l'heure, on a obtenu une forme normale pour les tresses (positives) en utilisant le résultat de Garside qui affirme que toute tresse dans B_n^+ admet un unique diviseur maximal qui est une tresse de permutation, et en itérant. Une autre forme normale sur B_n^+ peut être obtenue en utilisant le fait que toute tresse dans B_n^+ admet également un unique diviseur maximal qui appartient à B_{n-1}^+, c'est-à-dire une tresse où le n-ème brin n'est pas tressé. L'itération directe ne donne rien, mais elle devient intéressante quand on intercale de façon convenable l'automorphisme Φ_n de conjugaison par Δ_n, ce qui correspond à échanger le haut et le bas dans les diagrammes de tresses. On obtient ainsi une nouvelle forme normale, dite *alternante* parce qu'on laisse alternativement le brin du haut et le brin du bas non tressés. Cette forme normale est liée à des résultats de S. Burckel obtenus dans les années 1990, et elle fournit elle aussi une solution au problème d'isotopie [11].

Si je mentionne ces résultats ici, ce n'est pas tant pour leur intérêt propre que pour servir d'introduction à d'autres résultats qui semblent plus

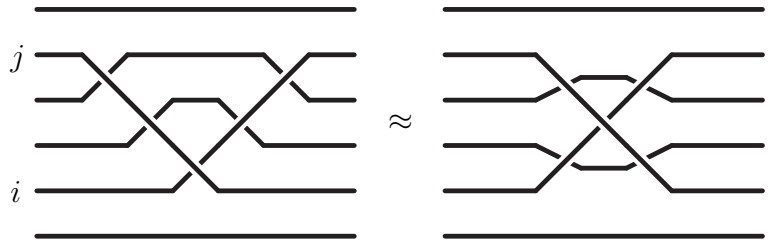

Figure 26: La tresse $a_{i,j}$: le brin j vient passer devant le brin i par devant tous les brins intermédiaires.

prometteurs. Pour expliquer cela, il faut que j'introduise ce qu'on appelle les générateurs de Birman–Ko–Lee du groupe B_n. Il s'agit de la famille des tresses $a_{i,j}$ définies pour $1 \leqslant i < j \leqslant n$ par $a_{i,j} = \sigma_{j-1}...\sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}...\sigma_{j-1}^{-1}$ (voir figure 26). Cette famille de générateurs est redondante : elle contient tous les σ_i (on a $\sigma_i = a_{i,i+1}$), mais, pour $n \geqslant 3$, elle contient en plus des conjugués tels que $a_{1,3}$, qui est $\sigma_2\sigma_1\sigma_2^{-1}$.

L'intérêt de considérer une famille de tresses autre que les générateurs d'Artin est de mener à un nouvel objet, à savoir le sous-monoïde B_n^{+*} engendré par tous les $a_{i,j}$. Comme chaque σ_i est un $a_{i,j}$, le monoïde B_n^{+*} inclut le monoïde B_n^+, et l'inclusion est stricte pour $n \geqslant 3$ car, par exemple, $a_{1,3}$ est dans B_n^{+*} mais pas dans B_n^+. Le monoïde B_n^{+*} est souvent appelé monoïde de tresses *dual*, à cause de symétries entre divers paramètres numériques associés à B_n^+ et à B_n^{+*}.

Un théorème de Birman, Ko, et Lee [6] affirme que le monoïde B_n^{+*} a une structure de Garside où le rôle de Δ_n est joué par $\delta_n = \sigma_{n-1}...\sigma_2\sigma_1$ et où les diviseurs de δ_n sont en bijection avec les partitions non croisées de $\{1, ..., n\}$. Comme je n'ai pas défini ce qu'on appelle une structure de Garside, cet énoncé ne vous dit pas grand chose. Essentiellement, ce qu'il signifie, c'est que les propriétés du monoïde B_n^{+*} sont similaires à celles du monoïde B_n^+. En particulier, comme pour B_n^+, on peut fabriquer une forme normale gloutonne sur B_n^{+*} — et de là une solution au problème d'isotopie — en termes non plus de permutations, mais de partitions non croisées. Il y a là-derrière toute une combinatoire à la fois profonde et élégante [4].

Le point où je veux en venir est ce qu'on obtient quand on marie l'idée de la forme normale alternante évoquée plus haut et le monoïde dual. C'est ce que fait J. Fromentin dans un travail tout récent [16], et cela semble très intéressant car cela a permis de débloquer plusieurs questions ouvertes depuis des années. L'idée est la suivante. Comme dans le cas de B_n^+, on montre que tout élément du monoïde B_n^{+*} a un diviseur maximal appartenant à B_{n-1}^{+*}. Pour pouvoir itérer et en déduire une forme normale, on intercale cette fois l'automorphisme ϕ_n de conjugaison par δ_n. Or celui-ci correspond non plus à une symétrie comme la conjugaison par Δ_n, mais à

une rotation d'ordre n. En effet, on montre facilement la relation

$$\phi_n(a_{i,j}) = a_{i+1\,(\mathrm{mod}\ n),\, j+1\,(\mathrm{mod}\ n)} \quad \text{pour } 1 \leqslant i < j \leqslant n.$$

Partant de là, on obtient une nouvelle forme normale sur B_n^{+*}, puis sur B_n. L'étape de base de la construction est illustrée dans la figure 27 où on a représenté les tresses sur un cylindre plutôt que sur un rectangle. La forme normale ainsi obtenue semble avoir des propriétés extrêmement intéressantes, mais je n'en dirai pas plus ici, et je vous renvoie à l'article de Fromentin [16].

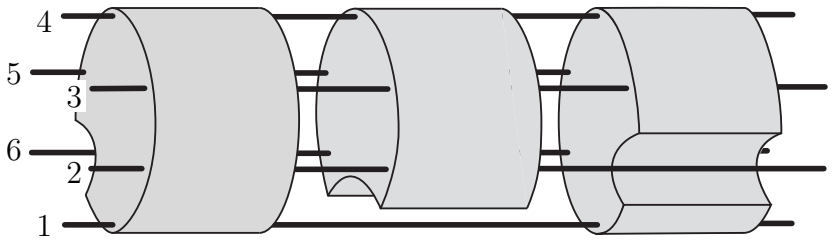

Figure 27: La forme normale cyclante de Fromentin, ici avec $n = 6$: on extrait le fragment maximal dans lequel le n-eme brin n'est pas tressé, puis le fragment maximal du reste dans lequel le premier brin n'est pas tressé, et ainsi de suite en tournant d'un sixième de tour à chaque fois.

La forme normale de Bressaud

Je ne peux pas terminer sans dire un mot des méthodes de relaxation. Il s'agit à nouveau de ***géométrie des surfaces*** dans une optique proche des ***systèmes dynamiques***, et le mot clé est ***relaxation***.

On considère une tresse β comme un homéomorphisme d'un disque pointé, et on fait agir β sur une courbe fixée C, par exemple le diamètre du disque, ou encore une collection fixée de segments. Après l'action de β, la courbe C est transformée en une nouvelle courbe $\beta(C)$, en général plus compliquée que C. Définir une méthode de relaxation, c'est fixer une stratégie qui, partant de la courbe compliquée $\beta(C)$, choisit un générateur $\sigma_i^{\pm 1}$ de sorte que la courbe $\sigma_i^{\pm 1}(\beta(C))$ soit plus simple que $\beta(C)$. Si cela peut être fait, alors, de proche en proche, on obtient des courbes de plus en plus simples, jusqu'à retomber sur la courbe initiale C, supposée de complexité minimale. Ce faisant, on a obtenu une suite de générateurs $\sigma_i^{\pm 1}$, c'est-à-dire un mot de tresse w, qui est une expression distinguée de la tresse β^{-1} puisque $w(\beta(C))$ est la courbe C (pourvu que la tresse triviale soit la seule qui fixe C à isotopie près). On a donc défini une forme normale sur le groupe B_n.

Cette idée est ancienne et elle a été utilisée en considérant différentes familles de courbes et différentes notions de complexité, par exemple dans les travaux de Wiest et Dynnikov [13]. Pour finir sur quelque chose de très récent, je vous renvoie à la nouvelle méthode de relaxation étudiée par Xavier Bressaud dans [7]. La stratégie consiste à minimiser les intersections entre les images des lacets standards de D_n et des demi-droites issues des points marqués. Un aspect spécialement intéressant est que la forme normale ainsi obtenue peut être calculée par un algorithme purement syntaxique très simple et étrangement réminiscent du jeu Tetris... Tout comme celle de Fromentin mentionnée dans la section précédente, la forme normale de Bressaud reste encore très mystérieuse, et elle montre qu'il reste encore beaucoup à découvrir sur les groupes de tresses.

Conclusion

J'espère vous avoir montré comment un même problème de départ pouvait mener à des développements variés mettant en jeu beaucoup de jolies mathématiques. Je suppose que vous en avez plus qu'assez des tresses et de leur problème d'isotopie pour aujourd'hui, et je vais m'arrêter. Pour autant, de nombreuses questions demeurent ouvertes, et ce que j'ai dit n'est que le début d'une longue histoire :

• *Quid* du problème de conjugaison, c'est-à-dire de la question de reconnaître si deux diagrammes de tresse représentent non pas la même tresse, mais des tresses conjugués ? C'est un problème plus difficile que le problème d'isotopie, il existe néanmoins des algorithmes le résolvant.

• *Quid* du problème de mot des groupes d'Artin–Tits ? Ce sont tous les groupes définis par des présentations analogues à celle du groupe B_n, mais avec des relations mettant en jeu des mots alternants de longueur quelconque, et pas seulement 2 ou 3. Certains résultats se généralisent, mais le problème général reste ouvert.

• *Quid* des groupes de tresses de surface ? Les groupes B_n correspondent aux tresses d'un disque ; on peut définir de même des groupes de tresses pour chaque surface (compacte).

• *Quid* des mapping class groups généraux ?

• *Quid* de l'isotopie des nœuds ?

etc. etc... la liste des questions est infinie !

Bibliographie

[1] E. Artin, *Theorie der Zöpfe*, Abh. Math. Sem. Univ. Hamburg **4** (1925) 47–72.

[2] E. Artin, *Theory of Braids*, Ann. of Math. **48** (1947) 101–126.

[3] S.I. Adyan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.

[4] D. Bessis, *The dual braid monoid*, An. Sci. Ec. Norm. Sup.; 36; 2003; 647–683.

[5] S. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14** (2001) 471–486.

[6] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.

[7] X. Bressaud, *A normal form for braid groups*, J. Knot Theory Ramifications; à paraître.

[8] P. Dehornoy, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997) 115–137.

[9] P. Dehornoy, *A fast method for comparing braids*, Advances in Math. **125** (1997) 200–235.

[10] P. Dehornoy, *Braid-based cryptography*, Contemp. Math. **360** (2004) 5–33.

[11] P. Dehornoy, *Alternating normal forms for braids and locally Garside monoids*, J. Pure Appl. Algebra **212-11** (2008) 2416–2439.

[12] P. Dehornoy, with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Mathematical Surveys and Monographs vol. 148, Amer. Math. Soc., (2008).

[13] I. Dynnikov and B. Wiest, *On the complexity of braids*, J. Europ. Math. Soc. **9** (2007) 801-840.

[14] E. A. ElRifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.

[15] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).

[16] J. Fromentin, *The cycling normal form on dual braid monoids*, Preprint (2007), arXiv : math.GR/0712.3836.

[17] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.

[18] C. Kassel & V. Turaev, *Braid groups*, Grad. Texts in Math., Springer (2008).

[19] D. Krammer, *The braid group B_4 is linear*, Invent. Math. **142** (2000) 451–486.

[20] D. Krammer, *Braid groups are linear*, Ann. Math. **151-1** (2002) 131–156.

[21] http://www.math.unicaen.fr/∼tressapp/index.html.