Tresses marines et problème du mot

Flore Le Roux

Année 2018-2019, Lycée Lakanal

Une corde tressée au bord de l'eau (Source : pixabay.com)

Abstract

In this text, I define the braids group which can be studied from both an algebraic and a geometric point of view. In fact, the geometric point of view matches the vision of a braid that people have in daily life. I also develop the word problem for this group, which consists in determining whether a word is equivalent to the neutral element of the group. Thus, I set out an algorithmic way to solve it. To do so, I define what a free group is, interpret it geometrically and use the action of the braid group by automorphisms of the free group.

Mots clés :

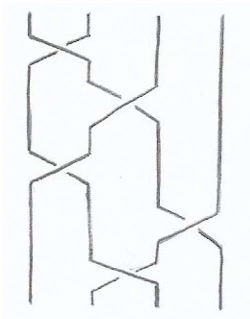
— Tresse, Groupe, Problème du mot, Groupe libre, Algorithme.

— Braid, Group, Word problem, Free group, Algorithm.

Table des matières

Introduction

En mer, sur leurs bateaux, les marins utilisent des cordes tressées. Ces tresses peuvent être modélisées de manière mathématique. Par exemple, géométriquement, le dessin suivant représente une tresse.



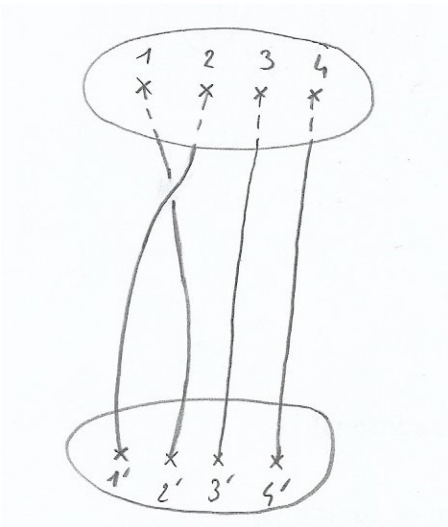
Un exemple de tresse géométrique

Les tresses constituent un intérêt certain puisque, si on munit leur ensemble d'un produit, elles forment une structure de groupe. Le but de cet exposé est de résoudre le problème du mot dans le groupe des tresses, c'est-à-dire d'obtenir un algorithme qui nous dit si une tresse est équivalente à une autre tresse. Nous étudierons ainsi ce groupe d'un point de vue à la fois géométrique et algébrique, puis nous proposerons un aglorithme de résolution codé en Python.

1 Présentation du groupe des tresses

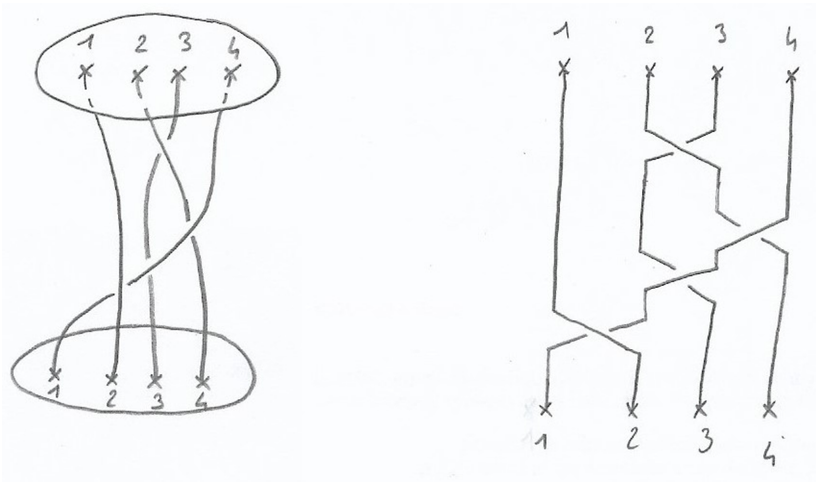
1.1 Modélisation géométrique et définition algébrique du groupe des tresses

Une tresse peut être représentée mathématiquement par l'union de n brins de l'espace joignant n points numérotés d'un plan à n autres points numérotés dans le même sens d'un autre plan sans intersection entre les brins. Par commodité, on donne un nom aux tresses en nommant les croisements entre leurs brins : pour tout i de $[\![1, n-1]\!]$, on note σ_i le croisement entre les brins i et $i+1$ lorsque le brin $i+1$ passe au-dessus du brin i et σ_i^{-1} le même croisement quand le brin i passe au-dessus du brin $i+1$.



Le croisement σ_1 pour une tresse à quatre brins

Pour faciliter la compréhension et la représentation des tresses géométriques, on utilise les diagrammes de tresses. Il s'agit de la projection dans le plan d'une tresse. Pour chaque croisement, on représente en trait continu le brin qui passe au-dessus et en trait discontinu celui du dessous.



Une tresse et son diagramme

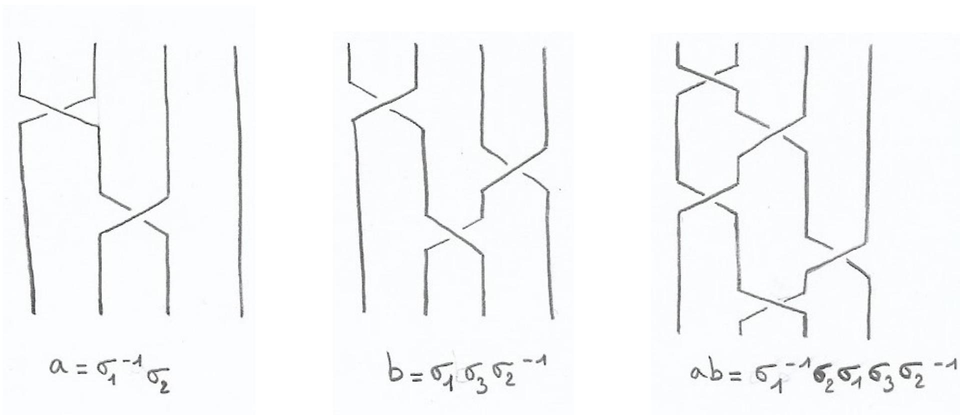
Par la suite, on représentera les tresses par leur diagramme.

Ensuite, on peut classifier les tresses grâce à la notion d'isotopie.

Définition. *Une tresse géométrique est isotope à une autre si on peut passer de la première à la deuxième par une déformation continue des brins de la première.*

On peut vérifier facilement qu'il s'agit d'une relation d'équivalence. On considère alors que deux tresses géométriques isotopes sont en fait la même tresse.

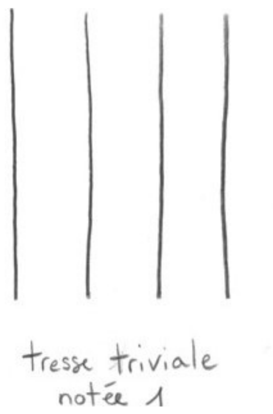
Par ailleurs, on peut concaténer les tresses.



Deux tresses et leur concaténation

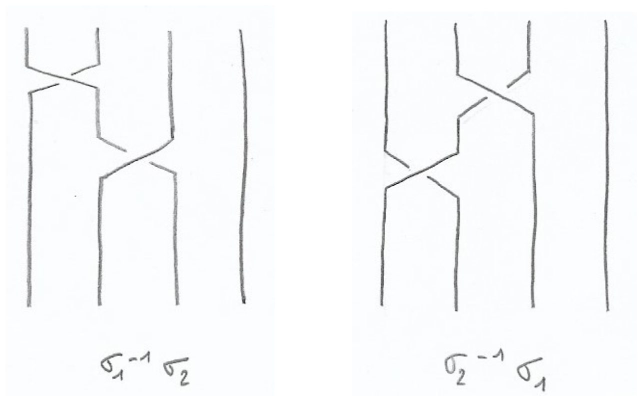
Cette concaténation permet de donner à l'ensemble des tresses une structure de groupe et l'on parle alors de produit.

La tresse triviale, c'est à dire l'élément neutre du groupe, est représentée par la tresse sans croisement entre les brins.



Représentation géométrique de l'élément neutre

Le symétrique d'un élément est représenté par son image dans un miroir et s'obtient donc en symétrisant la tresse par rapport au plan contenant les points d'arrivée de ses brins.



Une tresse et son symétrique

On peut à présent donner une définition algébrique du groupe des tresses. Chaque croisement entre deux brins d'une tresse géométrique représente un générateur du groupe des tresses algébriques. On obtient alors une définition de groupe par générateurs et relations :

Définition. *Le groupe des tresses, noté B_n, est le groupe engendré par $n-1$ générateurs $\sigma_1, \cdots, \sigma_{n-1}$ et les relations :*

$$(1)\ \sigma_i\ \sigma_j = \sigma_j\ \sigma_i\ \forall\ (i,j) \in [\![1, n-1]\!]^2 \textit{ tel que } |i-j| \geq 2$$

$$(2)\ \sigma_i\ \sigma_j\ \sigma_i = \sigma_j\ \sigma_i\ \sigma_j\ \forall\ (i,j) \in [\![1, n-1]\!]^2 \textit{ tel que } |i-j| = 1.$$

Cela signifie que l'on peut calculer dans le groupe des tresses uniquement avec ces deux relations et les relations normales entre un générateur et son inverse. Comme le groupe est noté de manière multiplicative, l'élément neutre est noté 1. Un produit de générateurs et d'inverses de générateurs est appelé un mot.

1.2 Explication des relations du groupe des tresses

Essayons de mieux comprendre les relations en voyant ce qu'elles donnent géométriquement.

La première relation

$$(1)\ \sigma_i\ \sigma_j = \sigma_j\ \sigma_i\ \forall\ (i,j) \in [\![1, n-1]\!]^2 \text{ tel que } |i-j| \geq 2$$

vient du fait que géométriquement, ces deux croisements n'impliquent pas les mêmes brins et donc n'ont pas d'impact l'un sur l'autre.

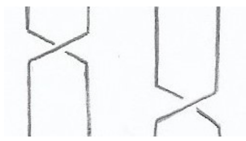


Illustration de la première relation

Comme on est passé d'une tresse à l'autre par déformation continue, les deux tresses sont isotopes.

La seconde relation s'illustre comme suit :

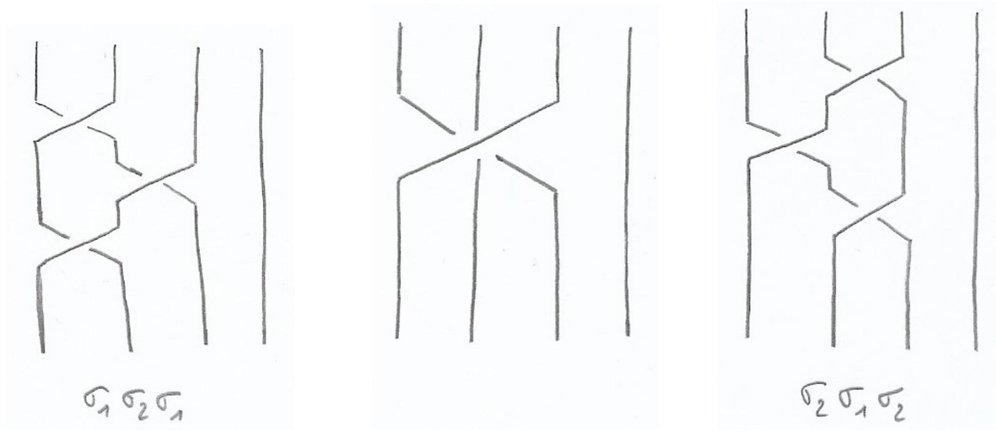


Illustration de la seconde relation

Le dessin du milieu représente la transition entre la tresse de gauche et celle de droite. Le brin du milieu passe entre les deux autres brins. C'est donc le brin de gauche qui est le plus en dessous. On voit qu'en décalant le brin du milieu vers la droite depuis sa position sur la tresse de gauche, on passe par l'état du milieu pour arriver finalement à la tresse de droite. Ces deux tresses sont isotopes, puisque l'on est passé de l'une à l'autre par une déformation continue des brins. En fait, on voit à travers ces deux exemples que l'égalité algébrique correspond à l'isotopie géométrique.

Voyons maintenant un exemple de calcul dans le groupe des tresses pour appréhender les différentes relations algébriquement.

Essayons de simplifier l'expression :

$$a = \sigma_3\ \sigma_1\ \sigma_2\ \sigma_3\ \sigma_2^{-1}\ \sigma_3^{-1}\ \sigma_2^{-1}\ \sigma_1^{-1}.$$

En utilisant la première relation, on obtient :

$$a = \sigma_1\ \sigma_3\ \sigma_2\ \sigma_3\ \sigma_2^{-1}\ \sigma_3^{-1}\ \sigma_2^{-1}\ \sigma_1^{-1}.$$

On peut alors utiliser la deuxième relation :

$$a = \sigma_1\ \sigma_2\ \sigma_3\ \sigma_2\ \sigma_2^{-1}\ \sigma_3^{-1}\ \sigma_2^{-1}\ \sigma_1^{-1}.$$

Tous les générateurs se simplifient alors avec leur inverse et on obtient :

$$a = 1.$$

Cet exemple illustre bien le fait que ce n'est pas évident algébriquement de savoir si une tresse est équivalente à la tresse triviale. Géométriquement, la notion d'isotopie n'est pas plus évidente, comme vu dans les exemples précédents.

1.3 Simplification du problème

Le fait de déterminer si deux tresses sont isotopes est équivalent au fait de déterminer si une tresse est triviale. En effet, si α est isotope à β, leurs expressions algébriques sont égales donc $\alpha\beta^{-1}$ est triviale.

Par ailleurs, déterminons si B_n est abélien ou non. Pour cela, on admet le lemme suivant.

Lemme. *Soient $s_1, \cdots, s_{n-1}$ des éléments d'un groupe G qui satisfont les relations précédentes :*

$$(1)\ s_i\ s_j = s_j\ s_i \text{ pour } |i-j| \geq 2$$

$$(2)\ s_i\ s_j\ s_i = s_j\ s_i\ s_j \text{ pour } |i-j| = 1.$$

Alors il existe un unique morphisme $f : B_n \longrightarrow G$ tel que :

$$s_1 = f(\sigma_1), \quad \cdots, \quad s_{n-1} = f(\sigma_{n-1}).$$

On applique ce lemme à certains éléments du groupe symétrique.
Soient $s_1 = (1\ \ 2), \cdots, s_{n-1} = (n-1\ \ n)$. Alors on a :

$$(1)\ s_i\ s_j = s_j\ s_i \text{ pour } |i-j| \geq 2.$$

En effet, deux transpositions à supports disjoints commutent. De plus, on a :

$$(2)\ s_i\ s_j\ s_i = (i\ \ i+2) = s_j\ s_i\ s_j \text{ pour } |i-j| = 1.$$

Corollaire. *Il existe un unique morphisme :*

$$\pi : B_n \longrightarrow S_n \quad \text{tel que} \quad \pi(\sigma_1) = s_1, \ \cdots, \ \pi(\sigma_{n-1}) = s_{n-1}.$$

Ce morphisme est surjectif car les transpositions $(i\ \ i+1)$ engendrent le groupe symétrique.

Corollaire. *Pour $n \geq 3$, B_n n'est pas abélien.*

Démonstration. *Pour $n \geq 3$, S_n n'est pas abélien car :*

$$s_1\ s_2 = (1\ \ 2) \circ (2\ \ 3) = (1\ \ 3\ \ 2) \neq (1\ \ 2\ \ 3) = (2\ \ 3) \circ (1\ \ 2) = s_2\ s_1.$$

Comme π est surjectif, $\exists\ (\sigma_i, \sigma_j) \in {B_n}^2$ tel que $s_1 = \pi(\sigma_i)$ et $s_2 = \pi(\sigma_j)$.
Ainsi $\pi(\sigma_i)\ \pi(\sigma_j) \neq \pi(\sigma_j)\ \pi(\sigma_i)$.
Donc $\pi(\sigma_i\ \sigma_j) \neq \pi(\sigma_j\ \sigma_i)$.
Et finalement $\sigma_i\ \sigma_j \neq \sigma_j\ \sigma_i$.

Savoir que B_n n'est pas abélien nous permet par exemple de dire qu'un commutateur, c'est-à-dire une tresse de la forme $\sigma_i \ \sigma_j \ \sigma_i^{-1} \ \sigma_j^{-1}$, n'est pas trivial.

Le problème du mot existe dans tous les groupes définis par générateurs et relations et est souvent non résoluble, ce qui signifie que l'on n'a pas d'algorithme capable de nous dire si un mot est trivial ou non. Dans le groupe des tresses, bien qu'il ne soit pas évident, il est résoluble.

2 Algorithme de résolution

2.1 Groupe libre et lien avec B_n

Pour comprendre comment fonctionne l'algorithme de résolution que nous allons étudier, il nous faut introduire la notion de groupe libre.

Définition. *Un groupe G est dit libre sur un sous-ensemble S de G si chaque élément de G s'écrit de façon unique comme produit réduit d'éléments de S et d'inverses d'éléments de S, c'est-à-dire sans occurence d'un générateur et de son inverse côte à côte. S est appelée partie génératrice de G et ses éléments, les générateurs de G.*

On remarque que le groupe des tresses n'est pas libre car par exemple le mot $\sigma_1\ \sigma_2\ \sigma_1$ est égal au mot $\sigma_2\ \sigma_1\ \sigma_2$ par la deuxième relation et qu'il s'agit de deux mots réduits.

Lemme. *Un groupe libre engendré par n générateurs est unique à isomorphisme près.*

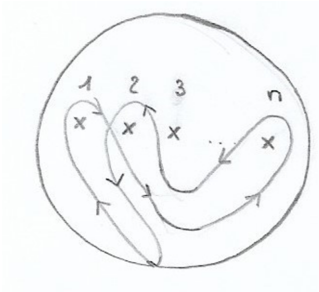
Démonstration. *Soient G le groupe libre engendré par les n générateurs $f_1, \cdots, f_n$ et G' celui engendrés par les n générateurs $f'_1, \cdots, f'_n$. Notons ϕ l'application de G dans G' qui, pour tout i de $[\![1, n]\!]$ associe s_i à s'_i. Montrons que cette application est un isomorphisme.*

— *Soit $(a, b) \in G^2$. Par définition, ils admettent chacun un mot réduit. Comme G est un groupe, $ab \in G$ donc ab admet lui aussi un mot réduit. ϕ envoie chaque générateur de G présent dans ce mot réduit sur un générateur de G' pour former un mot réduit de G'. De plus, ϕ envoie également a et b sur un mot réduit de G' et le produit de $\phi(a)$ et $\phi(b)$ appartient à G' donc a également un mot réduit. Or, on peut facilement vérifier que les opérations de réduction effectuées sur ab et sur $\phi(a)\phi(b)$ sont effectuées sur les générateurs de même indice. Ainsi, $\phi(ab) = \phi(a)\phi(b)$ donc ϕ est un morphisme.*

— *La bijectivité de ϕ est donnée par l'existence et l'unicité du mot réduit d'un élément de G et de G' par définition de G et G'.*

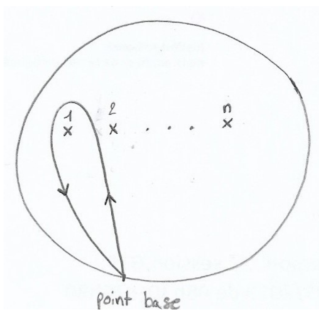
Par la suite, on notera F_n le groupe libre engendré par n générateurs $f_1, \cdots, f_n$.

F_n s'interprète aussi de manière géométrique comme le groupe fondamental du disque privé de n points, c'est-à-dire l'ensemble des courbes continues, considérées à déformation près, partant d'un point fixe du bord du disque appelé point base et revenant à ce point base sans passer par un des n points.



Un exemple d'élément du groupe libre

Les générateurs sont alors représentés par les lacets faisant le tour d'un seul de ces n points dans le sens trigonométrique. Ainsi, pour tout i de $[\![1, n]\!]$, le générateur s_i part du point base, fait le tour du ième point et revient au point base. L'inverse de chaque générateur est le même lacet parcouru dans l'autre sens.

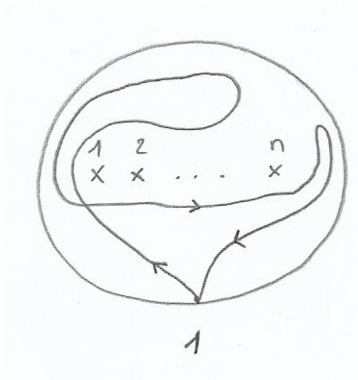


Le générateur f_1 de F_n

Le produit de deux éléments correspond à parcourir d'abord le premier puis le deuxième. On peut ainsi reprendre le premier exemple et l'écrire au moyen de générateurs et d'inverses.

Un exemple de produit

L'élément neutre est représenté par la courbe qui ne fait le tour d'aucun point et peut donc être assimilé au point base puisque les courbes sont considérées à déformations près.

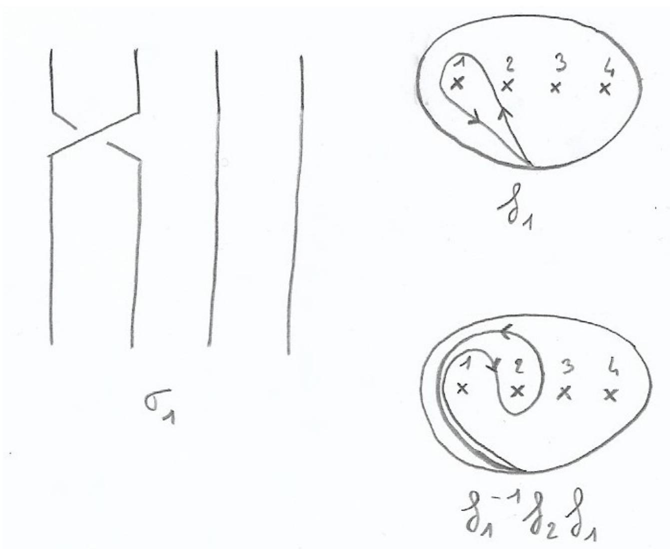


L'élément neutre du groupe libre

On établit un lien entre B_n et F_n avec la notion d'action de groupe.

Définition. *Une action d'un groupe G sur un groupe G' est un morphisme de G dans le groupe $Aut(G')$ des automorphismes de G'.*

On va par la suite considérer l'action de B_n sur F_n qui correspond géométriquement à faire glisser le long d'une tresse de B_n une courbe du groupe fondamental. Voici un exemple :



Action de σ_1 sur f_1

Les points numérotés dans la représentation du groupe libre correspondent aux brins de la tresse vus du dessus. Le dessin montre l'état du générateur f_1 avant et après avoir glisser le long de σ_1.

On admet le fait que cette action soit injective, bien que l'on puisse peut-être le comprendre géométriquement en remarquant par exemple que seule la tresse triviale envoie chaque générateur du groupe libre sur lui même. Ceci nous permet donc de considérer une tresse par son action sur un élément du groupe fondamental, ce qui nous facilite la tâche puisque les seules relations de simplification dans le groupe libre sont celles entre un générateur et son inverse.

2.2 Principe de fonctionnement de l'algorithme

L'algorithme considéré appliqué sur une tresse à quatre brins procède comme suit :

— On prend une tresse sous la forme d'un mot ;

— On la fait agir sur les générateurs du groupe libre et on obtient ainsi quatre mots qui correspondent à ce que sont devenus les quatre générateurs du groupe libre lors de leur passage autour des brins de la tresse ;

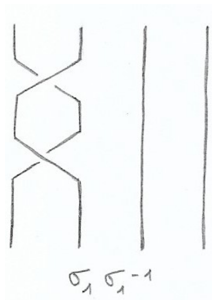
— On réduit ces mots ;

— Si chaque générateur du groupe libre est inchangé, la tresse est triviale, sinon elle ne l'est pas.

L'algorithme a été codé en Python et figure en annexe.

On peut appliquer cet algorithme à différentes tresses pour tester son efficacité. Lors du codage, chaque générateur est représenté par son indice et son inverse, par le même indice avec un "moins" devant. Commençons par une tresse qui est evidemment triviale, la tresse $\sigma_1\ \sigma_1^{-1}$.

```
>>> (executing line 79 of "PythonTIPE.py")
La tresse : [1, -1]
L'action sur le 1 e générateur du groupe libre : [-2, 2, 1, -2, 2]
Le mot réduit : [1]
L'action sur le 2 e générateur du groupe libre : [2]
Le mot réduit : [2]
L'action sur le 3 e générateur du groupe libre : [3]
Le mot réduit : [3]
L'action sur le 4 e générateur du groupe libre : [4]
Le mot réduit : [4]
La tresse est triviale
```

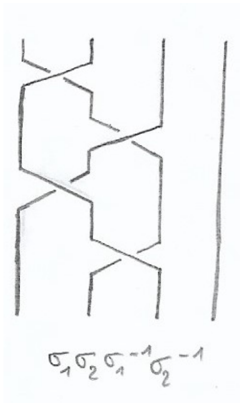


Un premier exemple et la tresse associée

L'algorithme affiche successivement ce que devient chaque générateur après son passage autour des brins de la tresse et s'arrête dès qu'un des générateurs n'est pas envoyé sur lui-même. Ici, la tresse étant triviale, l'algorithme teste tous les générateurs du groupe libre avant de conclure dans ce sens.

Essayons avec un deuxième exemple : le commutateur $\sigma_1\ \sigma_2\ \sigma_1^{-1}\ \sigma_2^{-1}$ que l'on sait ne pas être trivial puisque B_n n'est pas abélien.

```
>>> (executing line 80 of "PythonTIPE.py")
La tresse : [1, 2, -1, -2]
L'action sur le 1 e générateur du groupe libre : [-3, 3, -1, -3, 3, 2, -3, 3, 1, -3, 3]
Le mot réduit : [-1, 2, 1]
La tresse n'est pas triviale
```

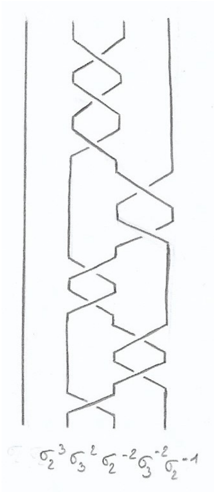


Un deuxième exemple et la tresse associée

Ici, l'algorithme s'arrête dès le premier générateur puisque ce dernier n'est pas envoyé sur lui-même. La tresse est bien dite non triviale par l'algorithme.

Voyons maintenant un exemple plus complexe.

```
>>> (executing line 85 of "PythonTIPE.py")
La tresse : [2, 2, 2, 3, 3, -2, -2, -3, -3, -2]
L'action sur le 1 e générateur du groupe libre :
[1]
Le mot réduit : [1]
L'action sur le 2 e générateur du groupe libre :
trop long !!, de longueur 917
Le mot réduit : [-3, -4, 3, 4, 3, -2, -3, -4, -3,
4, 3, 4, 3, 2, -3, -4, -3, 4, 3, -2, -3, -4, -3,
-4, 3, 4, 3, 2, -3, -4, -3, 4, 3, 4, 3, 2, -3, -4
, 3, 4, 3, -2, -3, -4, -3, -4, 3, 4, 3, 2, -3, -4
, -3, 4, 3]
La tresse n'est pas triviale
```



Un exemple plus complexe et la tresse associée

Bien que non triviale, cette tresse présente un interêt car elle verifie deux conditions nécessaires à la trivialité : l'ordre des brins est le même au départ et à l'arrivée et les enlacements des brins deux à deux sont nuls.

On remarque ici que l'image non réduite du second générateur n'a pas été affichée par l'algorithme car son expression est trop longue. C'est une des limites de cette méthode : comme chaque générateur du groupe libre peut être envoyé sur un produit de trois générateurs et inverses, la croissance de la longueur des mots lors du passage dans le groupe libre peut être assez importante.

Conclusion

Le problème du mot dans le groupe des tresses est donc résoluble. Cependant, on a pu voir que la complexité de l'algorithme n'est pas très bonne puisque la croissance des mots dans le goupe libre peut être assez importante. Sur le plan personnel, je trouve difficile le fait de devoir rédiger des maths toute seule et réussir à avoir un rendu structuré n'est pas chose facile.

Références

[1] C. Kassel, V. Turaev, *Braid Groups*, Springer, 2008.

[2] J. Riou, X. Caruso, *Groupe des tresses d'Artin*, Mémoire de magistère, `https://www.math.u-psud.fr/~riou/doc/tresses.pdf`.

[3] C. Milliet, *Groupe de tresses et cryptographie*, Rapport de stage, `http://math.univ-lyon1.fr/~milliet/rapportstagetresses.pdf`.

[4] Divers articles *Wikipédia*, notamment : Groupe libre, Groupe fondamental.

[5] T. Aubriot, E. Wagner, *L'ouvert*, numéro 113, 1–16, Des tresses et des noeuds en mathématiques.

[6] P. Dehornoy, *Bulletin de l'APMEP*, numéro 465, 465–476, Le calcul des tresses.