La combinatoire des tresses

Charles-Antoine Louët

12 juin 2002

Résumé

Mon sujet de recherche concerne le groupe des tresses, plus particulièrement d'un point de vue combinatoire. Après avoir introduit ce groupe et en avoir donné une présentation, j'expliquerai certaines techniques permettant de résoudre le problème des mots : le *retournement*, et la *réduction des poignées*. On démontre que la réduction des poignées s'arrête grâce à des résultats profonds sur le groupe des tresses, notamment qu'il est ordonnable. Malheureusement, la meilleure borne de complexité connue à ce jour pour cet algorithme est exponentielle, et il semble que la complexité soit quadratique.

La première partie de cette introduction donne les définitions de groupe des tresses, qu'on pourra trouver par exemple dans [Bir74]. Les deuxième et troisième parties abordent le retournement des mots et la réduction des poignées en suivant les chapitres II et III de [Deh00].

1 Définitions

1.1 Approche géométrique

Afin de reproduire en mathématiques l'idée que nous avons d'une tresse, il convient d'abord d'en donner une définition géométrique.

Définition 1.1.1 — *Soit n un entier. On pose*

$$\mathfrak{T}_n = \left\{ f \in \mathcal{C}^0(I, \mathbb{C}^n)\,;\ \left[\begin{array}{l} \forall t \in I\ (i \neq j \implies f_i(t) \neq f_j(t)) \\ \exists \pi \in \mathfrak{S}_n \text{ t.q. } \forall i\ f_i(0) = i \text{ et } f_i(1) = \pi^{-1}(i) \end{array} \right. \right\}$$

On dit que π est la permutation associée *à $f \in \mathfrak{T}_n$, et on la note π_f.*

Un élément $f \in \mathfrak{T}_n$ est un n-uplet de fonctions de I dans le plan $\mathbb{C}$. Si on en considère le graphe, on obtient n courbes dans $I \times \mathbb{C}$, ne se coupant pas, et ayant chacune un unique point d'intersection avec le plan $\{t\} \times \mathbb{C}$, pour tout $t \in I$. Si on considère que I est vertical, et les plans $\{t\} \times \mathbb{C}$ horizontaux, on a bien une tresse, au sens capillaire du terme. Les conditions $f_i(0) = i$ et $f_i(1) = \pi^{-1}(i)$ imposent que la tresse parte et arrive aux mêmes n points, et que les brins réalisent une permutation de ces points, selon la permutation π, qui peut se lire en remontant le long des brins.

Bien sûr, on considérera toutes les tresses uniquement à homotopie fixant les extrémités près. Si on note $\mathcal{H}$ cette relation d'homotopie, l'ensemble des tresses à n brins est $B_n = \mathfrak{T}_n/\mathcal{H}$. C'est un groupe pour la loi de concaténation : si deux tresses sont représentées par f et $g \in \mathfrak{T}_n$ alors leur produit fg est la classe modulo $\mathcal{H}$ de h dont le graphe dans $I \times \mathbb{C}$ est obtenu en dessinant le graphe de $f(2t)$ dans $\left[0, \frac{1}{2}\right] \times \mathbb{C}$ et celui de $g(2t-1)$ dans $\left[\frac{1}{2}, 1\right] \times \mathbb{C}$.

On peut donner une autre définition, bien plus courte, du groupe des tresses en tant que groupe fondamental.

Définition 1.1.2 — *Soit $Y_n = \{(z_1, \ldots, z_n) \in \mathbb{C}^n\ ;\ i \neq j \implies z_i \neq z_j\}$, et $X_n = {}^{Y_n}\!/_{\mathfrak{S}_n}$, pour l'action du groupe symétrique sur Y_n par permutation des coordonnées. On pose $B_n = \pi_1(X_n)$.*

Ces deux définitions du groupe B_n des tresses à n brins coïncident de façon élémentaire.

1.2 Approche algébrique

Le groupe des tresses possède également une définition algébrique.

Théorème 1.2.1 (Artin) — *B_n est donné par la présentation suivante :*

$$\left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{rcll} \sigma_i\sigma_j & = & \sigma_j\sigma_i & si \quad |i-j|>1 \\ \sigma_i\sigma_j\sigma_i & = & \sigma_j\sigma_i\sigma_j & si \quad |i-j|=1 \end{array} \right\rangle$$

Si on appelle G ce groupe, on a morphisme $G \to B_n$ défini en envoyant σ_i sur la tresse géométrique obtenue en faisant passer le brin $i+1$ au-dessus du brin i, et en laissant les autres brins descendre tout droit.

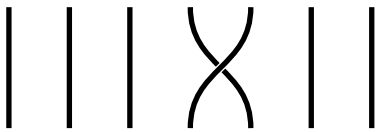


Fig. 1 – La tresse géométrique à 7 brins associée à σ_4

Afin d'avoir un morphisme, il faut vérifier que les tresses géométriques correspondant aux σ_i vérifient bien les relations définissant le groupe G. Ceci se vérifie grâce aux dessins, ou à l'aide de morceaux de ficelle...

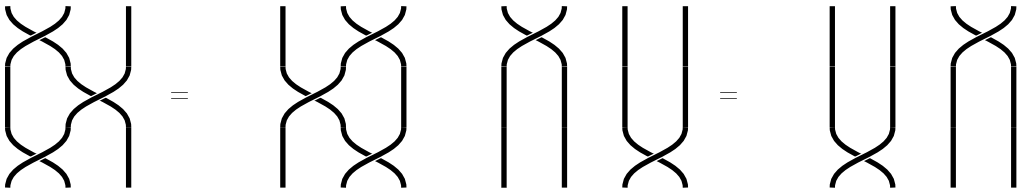


Fig. 2 – Les relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ et $\sigma_i\sigma_j = \sigma_j\sigma_i$ dans $\mathcal{B}_n$

On a donc bien un morphisme de G vers B_n. Il n'est pas difficile de montrer que ce morphisme est surjectif : on peut toujours représenter une tresse par des brins affines par morceaux (car Y_n est un ouvert de $\mathbb{C}^n$), et on peut ensuite repérer les croisements dans une tresse géométrique, et en déduire une expression en les σ_i qui la représente. L'injectivité est en revanche plus difficile, et je ne la démontrerai pas ici.

Définition 1.2.1 — *On appelle* mot de tresse *une expression de la forme $\sigma_{i_1}^{\varepsilon_1} \ldots \sigma_{i_l}^{\varepsilon_l}$, avec $\epsilon_i = \pm 1$, et sa* longueur *est l'entier l. Un mot de tresse est dit* positif *si tous les ε_i sont égaux à 1.*

On a vu que le groupe B_n était de présentation finie, c'est-à-dire donné par un nombre fini de générateurs soumis à un nombre fini de relations. Ces relations sont appelées *relations de tresses*. On remarque que ces relations sont *positives*, c'est-à-dire qu'elles ne font intervenir que des mots de tresses positifs. On peut donc donner la définition suivante.

Définition 1.2.2 — *On appelle* monoïde de tresses *et on note B_n^+ le monoïde donné par la même présentation que le groupe des tresses.*

Ainsi, tout élément du monoïde des tresses peut être représenté par un mot de tresse positif. Deux mots de tresses positifs représentent le même élément du monoïde si et seulement si on peut passer de l'un à l'autre en n'utilisant que les relations de tresses. Ils représentent alors le même élément du groupe des tresses. On a donc un morphisme de monoïdes $B_n^+ \to B_n$, qui envoie σ_i sur σ_i. Si deux mots de tresses positifs représentent le même élément de B_n, alors on peut passer de l'un à l'autre en utilisant les relations de tresses, ainsi que toutes les relations conjuguées, et les relations $\sigma_i\sigma_i^{-1} = e$. Il n'est donc pas évident que ces deux mots représentent le même élément de B_n^+. En d'autres termes, il n'est pas évident que le morphisme naturel $B_n^+ \to B_n$ soit injectif. Nous verrons que c'est tout de même le cas, ce qui justifie l'emploi des mêmes lettres pour les générateurs de B_n^+ et de B_n.

1.3 Le problème des mots

Définition 1.3.1 — *On appelle* problème des mots *pour un groupe donné par une présentation, le problème de la décision effective de l'égalité dans le groupe de deux expressions en ses générateurs.*

En d'autres termes, le problème des mots est résolu lorsqu'on sait dire si deux expressions sont égales dans le groupe, ou encore si on peut passer d'une expression à l'autre en utilisant les relations données dans la présentation du groupe. Dans le groupe des tresses avec la présentation donnée plus haut, par exemple, les mots $\sigma_1\sigma_2^{-1}\sigma_3\sigma_3\sigma_2\sigma_1\sigma_3\sigma_3\sigma_3$ et $\sigma_1\sigma_3\sigma_2\sigma_2\sigma_1\sigma_3\sigma_3$ représentent-ils le même élément ? Les tresses correspondantes sont-elles homotopes ? Le théorème d'Artin nous dit que c'est le cas si et seulement si on peut passer d'une expression à l'autre en n'utilisant que les relations de tresses et leurs conséquences dans un groupe. Or on a successivement, en appliquant une relation au sous-mot souligné :

$$\begin{array}{lll} \sigma_1\sigma_2^{-1}\sigma_3\sigma_3\sigma_2\underline{\sigma_1\sigma_3}\sigma_3\sigma_3 & = & \sigma_1\sigma_2^{-1}\sigma_3\underline{\sigma_3\sigma_2\sigma_3}\sigma_1\sigma_3\sigma_3 \quad = \\ \sigma_1\sigma_2^{-1}\underline{\sigma_3\sigma_2\sigma_3}\sigma_2\sigma_1\sigma_3\sigma_3 & = & \sigma_1\underline{\sigma_2^{-1}\sigma_2}\sigma_3\sigma_2\sigma_2\sigma_1\sigma_3\sigma_3 \quad = \\ \sigma_1\sigma_3\sigma_2\sigma_2\sigma_1\sigma_3\sigma_3 & & \end{array}$$

Les deux mots représentent donc la même tresse. Le problème des mots pour le groupe des tresses n'est pas pour autant résolu, car il s'agit d'être certain de pouvoir repérer les égalités pour tout couple de mots, c'est-à-dire qu'il nous faut un algorithme permettant de tester l'égalité entre deux expressions. Nous allons tout de suite en voir un.

2 Le retournement des mots

2.1 Idée de base

Définition 2.1.1 — *Soit A un alphabet et f une fonction partielle de $A\times A$ dans $A^\star$, l'ensemble des mots sur A, telle que $f(x,y)$ existe si et seulement si $f(y,x)$ existe, et telle que $f(x,x)=\epsilon$, le mot vide. On dit que f est un* complément. *La présentation de monoïde ou de groupe* associée à ce complément *est :*

$$\langle x\in A \quad | \quad xf(x,y)=yf(y,x), \quad (x,y)\in dom(f)\rangle.$$

Dorénavant, dans cette partie, on travaillera avec un alphabet A, un complément f sur cet alphabet, et la présentation donnée ci-dessus. L'intérêt des présentations complémentées est qu'elles entraînent pour tous x et y tels que $f(x,y)$ soit défini la relation $x^{-1}y=f(x,y)f(y,x)^{-1}$, vraie dans le groupe défini par f, et grâce à laquelle on peut transformer une fraction à gauche en une fraction à droite. Cette opération, qu'on appellera retournement, a lieu dans l'ensemble des mots sur $A^\pm=A\cup A^{-1}$.

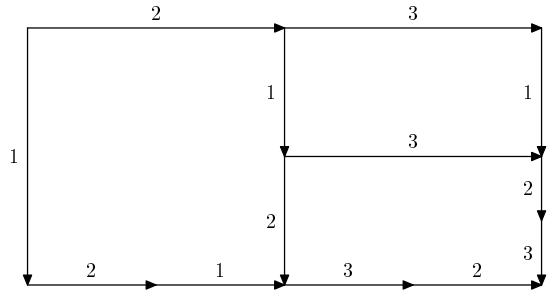
Définition 2.1.2 — *Soient w et w' des mots sur $A^\pm$. On dit que w se* retourne à droite *en w* en une étape *s'il existe des mots u et v sur $A^\pm$ ainsi que des lettres x et y dans A tels que l'on ait $w=ux^{-1}yv$ et $w'=uf(x,y)f(y,x)^{-1}v$. On note $w\curvearrowright^{(1)}w'$. On définit par récurrence la relation $\curvearrowright^{(n)}$, en posant pour $n>1$, $w\curvearrowright^{(n)}w'$ si et seulement si il existe w'' tel que $w\curvearrowright^{(n-1)}w''\curvearrowright^{(1)}w'$. La relation $\curvearrowright^{(0)}$ est par convention égale à l'égalité sur $A^{\pm\star}$. On dit que w se* retourne à droite *en w' s'il existe n tel que $w\curvearrowright^{(n)}w'$.*

Il nous faudra sans cesse distinguer entre les mots, les éléments du groupe, et les éléments du monoïde. Pour cela, on dira pour deux mots u et v sur $A^\pm$ qu'ils sont *égaux* s'ils sont égaux lettre par lettre (noté $u=v$), qu'ils sont *égaux dans le groupe* ou *équivalents* s'ils représentent le même élément du groupe (noté $u\equiv v$), et, s'ils sont positifs, qu'ils sont *égaux dans le monoïde* ou *positivement équivalents* s'ils représentent le même élément du monoïde (noté $u\equiv^+ v$). Pour un mot u (positif ou non), on notera $\overline{u}$ son image (dans le monoïde ou dans le groupe).

Le groupe et le monoïde des tresses sont tous les deux associés à un complément, défini par

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_j & \text{si} \quad |i-j| > 1 \\ \sigma_j \sigma_i & \text{si} \quad |i-j| = 1 \\ \epsilon & \text{si} \quad i = j. \end{cases}$$

On peut donc faire des retournements de mots en utilisant ce complément, par exemple, le diagramme suivant représente le retournement à droite du mot $\sigma_1^{-1}\sigma_2\sigma_3$.



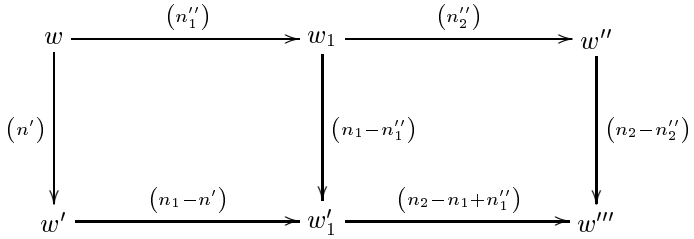
En partant du coin inférieur gauche, et en rejoignant le coin supérieur droit, en ne faisant que monter ou aller à droite, on lit les lettres successives le long des arêtes que l'on traverse, étant entendu qu'une arête traversée contre son orientation contribue pour l'inverse d'un générateur. Ainsi, on a $\sigma_1^{-1}\sigma_2\sigma_3 \curvearrowright \sigma_2\sigma_1\sigma_3\sigma_2\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}$. Ce dernier mot est terminal pour le retournement à droite, car il ne contient aucun motif $x^{-1}y$ avec x et y dans A. Notre but va maintenant être de démontrer que le retournement de mots converge toujours vers un mot terminal dans le cas du groupe des tresses.

2.2 Cohérence et arithmétique

Proposition 2.2.1 — *Le retournement des mots est confluent : si* $w \curvearrowright^{(n')} w'$ *et* $w \curvearrowright^{(n'')} w''$, *alors il existe* n *et* w''' *tels que* $\sup(n', n'') \leqslant n \leqslant n' + n''$, $w' \curvearrowright^{(n-n')} w'''$ *et* $w'' \curvearrowright^{(n-n'')}$.

Démonstration — Lorsque n' ou n'' sont nuls, le résultat est immédiat. Supposons que $n' = n'' = 1$. Cela signifie que pour passer de w à w' on a retourné un sous-mot de la forme $x^{-1}y$, de même pour passer de w à w''. Si le sous-mot retourné dans chacun des cas est le même, alors $w' = w''$, et on peut prendre $n = 1$, $w''' = w'$. Sinon, les deux sous-mots de w retournés pour passer à w' et à w'' sont disjoints. On prend alors $n = 2$ et w''' est obtenu en retournant ces deux sous-mots.

Pour terminer, on utilise la récurrence sur $n' + n''$. Le résultat est établi pour $n' + n'' \leqslant 2$. Supposons que $n' + n'' \geqslant 3$, et, pour fixer les idées, que $n'' \geqslant 2$. On peut considérer un mot intermédiaire w_1 tel que $w \curvearrowright^{(n_1'')} w_1 \curvearrowright^{(n_2'')} w''$, avec n_1'' et n_2'' strictement inférieurs à n'', et conclure grâce à l'hypothèse de récurrence.



On a $w \curvearrowright w_1$ et $w \curvearrowright w'$, donc on peut dire que w_1 et w' se retournent tous les deux en w_1', en $n_1 - n_1''$ et $n_1 - n'$ étapes respectivement, avec $\sup(n', n_1'') \leqslant n_1 \leqslant n' + n_1''$. Cette dernière inégalité donne $n_1 - n_1'' < n' + n_1''$ soit $(n_1 - n_1'') + n_2'' < n' + n''$ et on peut donc à nouveau utiliser l'hypothèse de récurrence pour trouver w''' et n_2 qui complètent le schéma.

En posant $n = n_2 + n_1''$, on a bien $w' \curvearrowright^{(n-n')} w'''$ et $w'' \curvearrowright^{(n-n'')} w'''$. Il en découle que n' et n'' sont tous les deux inférieurs à n, et il reste à vérifier que $n \leqslant n' + n''$, ce qui est équivalent à

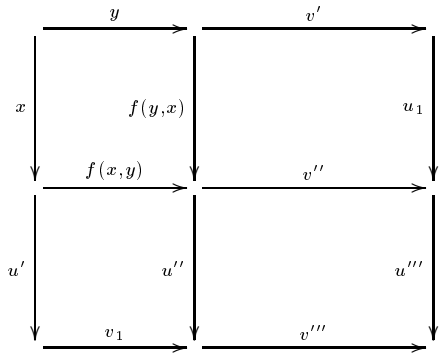
$n_2 \leqslant n' + n''_2$. Mais on a $n_1 \leqslant n' + n''_1$, d'où $n_1 - n''_1 + n''_2 \leqslant n' + n''_2$. Or $n_2 \leqslant (n_1 - n''_1) + n''_2$, par hypothèse de récurrence, et on a fini. ✓

Cette proposition montre en particulier que le nombre d'étapes nécessaires pour effectuer un retournement est bien défini.

Définition 2.2.1 — *Soient u et v des mots sur l'alphabet A. Si le mot $u^{-1}v$ se retourne en $v'u'^{-1}$, avec v' et u' des mots positifs, on pose $u\backslash v = v'$. Cette opération est bien définie d'après la confluence du retournement.*

Par construction, $u\backslash v$ existe si et seulement si $v\backslash u$ existe. On peut aussi remarquer que $\backslash$ est un prolongement de f car $x\backslash y = f(x, y)$.

Proposition 2.2.2 — *Soient u et v deux mots sur A. On a $u\,(u\backslash v) \equiv^+ v\,(v\backslash u)$.*
Démonstration — On a vu que les deux membres de l'égalité sont définis en même temps. La démonstration se fait par récurrence sur le nombre n d'étapes dans le retournement $u^{-1}v \curvearrowright (u\backslash v)\,(v\backslash u)^{-1}$. Si $n = 0$, alors u ou v était le mot vide, et on conclut. Sinon, on pose $u = xu'$ et $v = yv'$ et on lit le résultat sur un diagramme de retournement :



On a successivement : $u\,(u\backslash v) = xu'v_1v''' \equiv^+ xf(x,y)u''v''' \equiv^+ yf(y,x)v''u''' \equiv^+ yv'u_1u''' = v\,(v\backslash u)$. ✓

On déduit de cette proposition que si u et v sont deux mots positifs, alors $u^{-1}v \curvearrowright \epsilon$ entraîne $u \equiv^+ v$. Posons $u \equiv^{++} v$ si $u^{-1}v \curvearrowright \epsilon$. On a $\equiv^{++} \subseteq \equiv^+$.

Définition 2.2.2 — *On dit que le complément f est* complet *si $\equiv^+ \subseteq \equiv^{++}$. On dit qu'il est* cohérent *si pour tous mots positifs u, v et w, $(u\backslash v)\setminus(u\backslash w)$ et $(v\backslash u)\setminus(v\backslash w)$ existent en même temps, et si $((u\backslash v)\setminus(u\backslash w))\setminus((v\backslash u)\setminus(v\backslash w)) = \epsilon$ lorsque c'est le cas.*

Proposition 2.2.3 — *Si le complément f est complet, le monoïde M associé est simplifiable à gauche.*
Démonstration — Supposons que $uv \equiv^+ u'v$. Par complétude, on peut dire que $uv \equiv^{++} u'v$, soit $u'^{-1}v^{-1}vu \curvearrowright \epsilon$. Mais comme $v^{-1}v \curvearrowright \epsilon$ la confluence donne $u'^{-1}u \curvearrowright \epsilon$ d'où $u \equiv^{++} u'$, ce qui entraîne $u \equiv^+ u'$. ✓

La propriété de cohérence peut se résumer par un dessin dans lequel les trois mots u, v et w sont représentés par les trois arêtes partant du même sommet d'un cube. En "refermant" par retournements les trois faces définies par ces arêtes, on obtient plusieurs façons de construire le sommet diamétralement opposé, mais on voudrait qu'il représente toujours le même élément du monoïde, autrement dit que $(u\backslash v)\setminus(u\backslash w) \equiv^+ (v\backslash u)\setminus(v\backslash w)$. La cohérence demande en plus que cette congruence puisse être testée par retournement, ce qui équivaut à demander que $(u\backslash v)\setminus(u\backslash w) \equiv^{++} (v\backslash u)\setminus(v\backslash w)$.

Proposition 2.2.4 — *On a équivalence des trois propriétés suivantes :*

(i) Le complément f est complet (i.e. $\equiv^{++}$ et $\equiv^+$ coïncident).

(ii) L'opération $\backslash$ est compatible avec $\equiv^+$.

(iii) Le complément f est cohérent.

DÉMONSTRATION — Montrons que *(i)* implique *(ii)*. Bornons-nous à montrer que si $v \equiv^+ v'$ alors $v'\backslash u \equiv^+ v\backslash u$. Comme on sait que $u\,(u\backslash v) \equiv^+ v\,(v\backslash u)$, on a $u\,(u\backslash v) \equiv^+ v'\,(v\backslash u)$. Mais l'hypothèse entraîne alors que $u\,(u\backslash v) \equiv^{++} v'\,(v\backslash u)$. En ne conservant qu'une partie du retournement qui démontre cette congruence, on trouve $(v\backslash u) \setminus (v'\backslash u) = \epsilon$. Ceci montre en particulier que $v'\backslash u$ et par conséquent $u\backslash v'$ existent, et on peut échanger les rôles de v et v' pour trouver $(v'\backslash u) \setminus (v\backslash u) = \epsilon$. On a donc $v'\backslash u \equiv^{++} v\backslash u$, et ces deux mots sont positivement équivalents. Que *(ii)* implique *(i)* est immédiat. Si $\backslash$ est compatible avec $\equiv^+$, alors deux mots u et v positivement équivalents seront tels que $u\backslash v \equiv^+ u\backslash u = \epsilon$; maintenant, dans une présentation donnée par un complément, le seul mot qui soit positivement équivalent au mot vide est le mot vide, et on obtient $u\backslash v = \epsilon$ et de même $v\backslash u = \epsilon$, ce qui entraîne $u \equiv^{++} v$. Ainsi, les deux premières propriétés sont équivalentes.

Démontrons à présent que *(ii)* implique *(iii)*. On peut supposer à la fois *(i)* et *(ii)*. Soient u, v et w trois mots positifs. On sait déjà que $u\backslash v$ et $v\backslash u$ existent en même temps. Si ce n'est pas le cas, ni $(u\backslash v) \setminus (u\backslash w)$ ni $(v\backslash u) \setminus (v\backslash w)$ ne sont définis. Supposons donc que $u\backslash v$ existe. En écrivant le retournement de $a^{-1}bc$ on trouve facilement que $(bc)\setminus a = c\setminus (b\backslash a)$, l'égalité signifiant aussi que les deux termes existent en même temps. On en déduit que $(u\backslash v) \setminus (u\backslash w) = (u\,(u\backslash v))\setminus w$. Comme $u\,(u\backslash v) \equiv^+ v\,(v\backslash u)$, en utilisant *(ii)* on obtient $(u\backslash v) \setminus (u\backslash w) \equiv^+ (v\,(v\backslash u))\setminus w = (v\backslash u) \setminus (v\backslash w)$. D'après *(i)*, on peut maintenant dire que $(u\backslash v) \setminus (u\backslash w) \equiv^{++} (v\backslash u) \setminus (v\backslash w)$.

Supposons à présent *(iii)* et montrons que $\equiv^+ \subseteq \equiv^{++}$. L'équivalence positive est la relation d'équivalence sur $A^\star$ engendrée par les paires $(uxf(x,y)v, uyf(y,x)v)$, pour u et v dans $A^\star$ et x et y dans A. Il suffit donc de montrer que $uxf(x,y)v \equiv^{++} uyf(y,x)v$, ce qui est immédiat, et que $\equiv^{++}$ est une relation d'équivalence. Elle est clairement symétrique et réflexive. Il nous reste à démontrer qu'elle est transitive. Soient u, v et w trois mots sur A, et supposons que $u \equiv^{++} v$ et $v \equiv^{++} w$. Cela entraîne que $(v\backslash u) \setminus (v\backslash w) = \epsilon$, et il résulte de la cohérence que $(u\backslash v) \setminus (u\backslash w) = \epsilon$ aussi. Comme $u\backslash v = \epsilon$, on a $(u\backslash v) \setminus (u\backslash w) = u\backslash w = \epsilon$. Par symétrie, on obtient aussi $w\backslash u = \epsilon$ et finalement $u \equiv^{++} w$. ✓

D'après la proposition précédente, la cohérence d'un complément permet d'affirmer que le retournement détecte les couples des mots positifs positivement équivalents. Mais la cohérence telle qu'elle a été définie semble bien difficile à vérifier. Heureusement, lorsque le complément est *normé*, il suffit de vérifier la cohérence sur les triplets de générateurs, ce qu'on appelle la *cohérence locale*.

DÉFINITION 2.2.3 — *On dit que le complément f est* normé *(à droite) s'il existe une fonction $\nu : A^\star \mapsto \mathbb{N}$ qui vérifie, pour tous u et v dans $A^\star$ et tous x et y dans A, $\nu(xu) > \nu(u)$, $\nu(ux) > \nu(u)$ et $\nu(uxf(x,y)v) = \nu(uyf(y,x)v)$.*

Par exemple, le complément qui donne la présentation d'Artin du groupe des tresses est normée. C'est le cas pour tout complément tel que $f(x,y)$ et $f(y,x)$ soient de même longueur. La longueur des mots est alors compatible avec $\equiv^+$ et elle définit une norme ν. L'intérêt de la norme vient de la proposition suivante, dont la démonstration est essentiellement technique, et que je ne reproduirai pas.

PROPOSITION 2.2.5 — *Soit f un complément normé. Alors f est cohérent si et seulement si f est localement cohérent.*

2.3 Convergence

On s'intéresse maintenant au problème de la convergence du retournement des mots associé à un complément f. On sait par exemple que si u et v sont deux mots positifs positivement équivalents et que f est normé et localement cohérent, alors $u^{-1}v \curvearrowright \epsilon$, mot terminal pour le retournement. Mais on peut avoir mieux.

DÉFINITION 2.3.1 — *Soient a et b deux élément d'un monoïde M. On dit que a* divise *b (à gauche) s'il existe c tel que $ac = b$. On dit aussi que b est un* multiple *de a (à droite). On note $a \preccurlyeq b$. On dit que m est le* plus petit multiple commun *de a et b si les multiples communs de a et b sont les multiples de m. On note $m = a \vee b$. De même, on dit que d est le* plus grand commun diviseur *de a et b si les diviseurs communs de a et b sont les diviseurs de d. On note $d = a \wedge b$.*

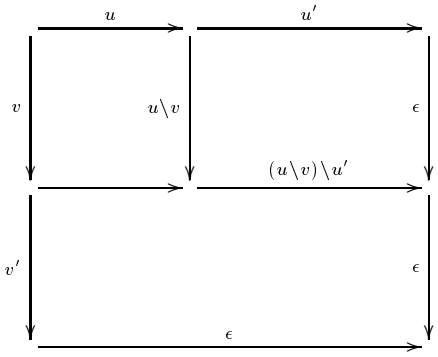
PROPOSITION 2.3.1 — *Soient u et v deux mots positifs sur A, et a et b les éléments correspondants dans le monoïde M défini par f. On suppose que f est cohérent. On a l'équivalence des assertions suivantes.*

(i) Le mot $u\backslash v$ existe.

(ii) Les éléments a et b ont un multiple commun dans M.

Dans ce cas, a et b ont un plus petit multiple commun, représenté par les mots positivement équivalents $u\,(u\backslash v)$ et $v\,(v\backslash u)$.

DÉMONSTRATION — Il est évident que *(i)* implique *(ii)*, car si $u\backslash v$ existe, il en va de même pour $v\backslash u$, et on a $u\,(u\backslash v) \equiv^{+} v\,(v\backslash u)$. Supposons *(ii)*. On peut trouver des mots u' et v' tels que $uu' \equiv^{+} vv'$. Comme f est cohérent, il est complet, et on a $uu' \equiv^{++} vv'$, soit ${v'}^{-1}v^{-1}uu' \curvearrowright \epsilon$.



Par confluence, on en déduit que le retournement de $v^{-1}u$ converge, et que $u\backslash v$ et $v\backslash u$ existent. On peut aussi dire que $(uu')\backslash v = \epsilon$, et on en déduit que $u\,(u\backslash v)\,((u\backslash v)\backslash u') \equiv^{+} uu'$, ce qui montre que $u\,(u\backslash v)$ représente bien le plus petit commun multiple de a et de b. ✓

COROLLAIRE 2.3.1 — *Si f est cohérent et normé, alors tout sous-ensemble non vide de M admet un plus grand commun diviseur (à gauche).*

DÉMONSTRATION — Soit $\emptyset \subsetneq S \subseteq M$, et D l'ensemble des diviseurs de S. La norme ν associée à f est compatible à l'équivalence positive, elle définit donc une application $\overline{\nu}$ sur M. Si $ac = b$, on a $\overline{\nu}(a) \leqslant \overline{\nu}(b)$. Les valeurs de $\overline{\nu}$ sur D sont donc bornées par ses valeurs sur S, et on peut choisir $d \in D$ tel que $\overline{\nu}(d)$ soit maximal. Soit $b \in D$. Comme S et non vide, b et d ont un multiple commun. On en déduit qu'ils ont un plus petit multiple commun $b \vee d$. Mais celui-ci est encore dans D. Si on écrit $b \vee d = db'$, on trouve $\overline{\nu}(db') \leqslant \overline{\nu}(d)$, et on en déduit que b' est représenté par le mot vide, et que d est un multiple de b. ✓

DÉFINITION 2.3.2 — *On dit que le complément f est convergent si pour tous mots positifs u et v, $u\backslash v$ existe.*

D'après ce qui précède, une condition nécessaire et suffisante pour que f soit convergent est que tout couple d'éléments de M ait un multiple commun.

DÉFINITION 2.3.3 — *Soit M un monoïde, et Δ un élément de M. On dit que Δ est un* élément de Garside *s'il a les même diviseurs à gauche et à droite, et que leur ensemble est fini et engendre M.*

THÉORÈME 2.3.1 — *Si f est un complément normé et localement cohérent, tel que le monoïde M associé possède un élément de Garside, alors f est convergent.*

DÉMONSTRATION — Il suffit de montrer que si deux éléments a et b de M ont un multiple commun. Soit Δ un élément de Garside pour M, et soit S l'ensemble de ses diviseurs. Pour tout x dans S, on peut écrire $xx' = \Delta$. Comme f est cohérent, M est simplifiable à gauche, et l'application $x \mapsto x'$ est bien définie. On en déduit une application $\sigma : S \mapsto S$ définie par $\sigma(x) = (x')'$. On a $xx'\sigma(x) = x\Delta = \Delta\sigma(x)$.

Par hypothèse, S engendre M. On peut dont écrire a comme produit de l éléments de S. Montrons par récurrence sur l qu'un produit de l éléments de S est un diviseur (à gauche) de Δ^l. C'est vrai pour $l = 0$. Supposons que ce soit vrai pour l, et soit $a = sb$ avec $s \in S$ et $b \in M$ un produit de l éléments de S. D'après l'hypothèse de récurrence, on peut écrire $bc = \Delta^l$, et on obtient $ac = s\Delta^l$, d'où $ac\sigma^l(s') = s\Delta^l\sigma^l(s') = ss'\Delta^l = \Delta^{l+1}$. ✓

Dans ce cas, on obtient une solution au problème des mots. Si f est convergent, le retournement de n'importe quel mot $w \in A^{\pm\star}$ converge vers uv^{-1} avec u et v positifs. On a alors $w \equiv uv^{-1}$, il

suffit alors d'effectuer le retournement de $v^{-1}u$, et w représente la tresse triviale si et seulement si $v^{-1}u \curvearrowright \epsilon$. On résout donc le problème des mots avec deux retournements. Un examen plus attentif montre que cette solution est quadratique en la longueur initiale de w.

Pour le groupe des tresses B_n, on n'a aucune peine, comme je l'ai déjà indiqué, à trouver une norme pour le complément f. On vérifie ensuite qu'il est localement cohérent, en vérifiant la condition du cube pour tous les triplets de générateurs, ce qui ne pose pas de problème. Il reste à construire un élément de Garside. Une étude combinatoire élémentaire (faite par exemple dans mon mémoire de D.E.A.) montre que si $\Pi_k = \sigma_1 \dots \sigma_k$ l'élément défini par $\Delta = \Pi_{n-1} \dots \Pi_1$ convient. Le retournement des mots converge donc dans le groupe des tresses. À cause de la symétrie des relations de tresses, on peut aussi définir le retournement à gauche, et en déduire le calcul de ppcm à gauche et obtenir la simplifiabilité à droite. Le monoïde B_n^+ vérifie donc les conditions de Öre et se plonge dans son groupe de fractions B_n.

Définition 2.3.4 — *Soit w un mot de tresse. On définit les mots positifs $N_r(w)$ et $D_r(w)$ par $w \curvearrowright N_r(w)D_r(w)^{-1}$. On définit de même les mots positifs $N_l(w)$ et $D_l(w)$ par le retournement à gauche : $w \curvearrowright_g D_l(w)^{-1}N_l(w)$. On appelle* valeur absolue *de w et on note $|w|$ la tresse positive représentée par $D_l(w)N_r(w)$ ou $N_l(w)D_r(w)$.*

3 La réduction des poignées

Le retournement des poignées est un autre algorithme de résolution du problème des mots dans le groupe des tresses. Il repose sur l'ordre de Dehornoy sur le groupe des tresses : si e est la tresse triviale, pour toute tresse t, on est dans l'un des trois cas $t = e$, $t > e$, $t < e$, ces trois cas s'excluant mutuellement. La réduction des poignées est une méthode pour mettre un mot de tresse sous une forme permettant de décider dans quel cas on se trouve.

3.1 L'ordre de Dehornoy

Définition 3.1.1 — *Soit $w = \sigma_{i_1}^{\varepsilon_1} \dots \sigma_{i_l}^{\varepsilon_l}$ un mot de tresse. Soit $k = \min\{i_1, \dots, i_l\}$. On appelle σ_k le* générateur principal *de w.*

On dit que w est σ-positif *(respectivement* σ-négatif*) s'il est non trivial et si son générateur principal n'apparaît qu'avec des puissances positives (respectivement* négatives*) dans w. Si le mot w est trivial, σ-positif, ou σ-négatif, on dit qu'il est* σ-défini*. On dit qu'il est* σ-indéfini *sinon.*

Soit $a \in B_n$. On dit que a est σ-positive (respectivement σ-négative) si elle admet un représentant σ-positif (respectivement σ-négatif).

Théorème 3.1.1 — *Une tresse σ-positive est nécessairement non-triviale. Une tresse non triviale est soit σ-positive, soit σ-négative, mais jamais les deux à la fois. On définit un ordre total invariant par multiplication à gauche sur B_n par*

$$a < b \iff a^{-1}b \text{ est } \sigma\text{-positive.}$$

Ce théorème est difficile ; l'une de ses démonstrations repose notamment sur le retournement des mots, et sur l'étude des lois de composition auto-distributives (i.e. qui vérifient l'identité $x(yz) = (xy)(xz)$), et en particulier de celle définie sur $B_\infty = \varinjlim B_n$ par $a \bullet b = a\mathrm{sh}(b)\sigma_1\mathrm{sh}(a^{-1})$, où $\mathrm{sh}(\sigma_i) = \sigma_{i+1}$. Remarquons que ce théorème montre que si un mot ne contient que des puissances positives de son générateur principal, alors il ne peut représenter la tresse triviale. Ce résultat admet la généralisation suivante, qu'on ne démontrera pas non plus.

Proposition 3.1.1 — *Soit $w = \sigma_{i_1}^{\varepsilon_1} \dots \sigma_{i_l}^{\varepsilon_l}$ un mot de tresse. On suppose que le générateur σ_i n'apparaît qu'avec des puissances positives dans w, et au moins une fois. Alors w ne peut représenter la tresse triviale.*

Voici un exemple qui illustre le théorème. Le mot $\sigma_1^{-1}\sigma_2\sigma_1$ est σ-indéfini. Mais il est équivalent au mot $\sigma_2\sigma_1\sigma_2^{-1}$ qui est σ-positif. On en déduit que $\sigma_1^{-1}\sigma_2\sigma_1 > e$, et par conséquent que cette tresse est non triviale. Il n'est pas toujours facile de déterminer si une tresse est σ-positive, σ-négative, ou triviale. Par exemple, qu'en est-il de $\sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_3\sigma_1\sigma_2^{-1}\sigma_1^{-1}$? Le retournement des poignées est un algorithme permettant de résoudre ce problème.

3.2 L'algorithme

Lorsqu'un mot de tresse est σ-indéfini, cela signifie qu'il est non trivial et que son générateur principal apparaît à la fois négativement et positivement.

Définition 3.2.1 — *Soit w un mot de tresse. On dit que w est une* σ_i-poignée *(ou une* i-poignée*) s'il est de la forme $\sigma_i^e u \sigma_i^{-e}$, avec $e = \pm 1$, et où le mot u ne contient que des lettres σ_j avec $j > i$.*

Le nom de poignée vient de l'interprétation géométrique d'un tel mot de tresse. En effet, dans une i-poignée, le i-ème brin forme bien une "poignée" sur la gauche de la tresse. L'idée de la réduction des poignées peut être résumée sur le dessin suivant.

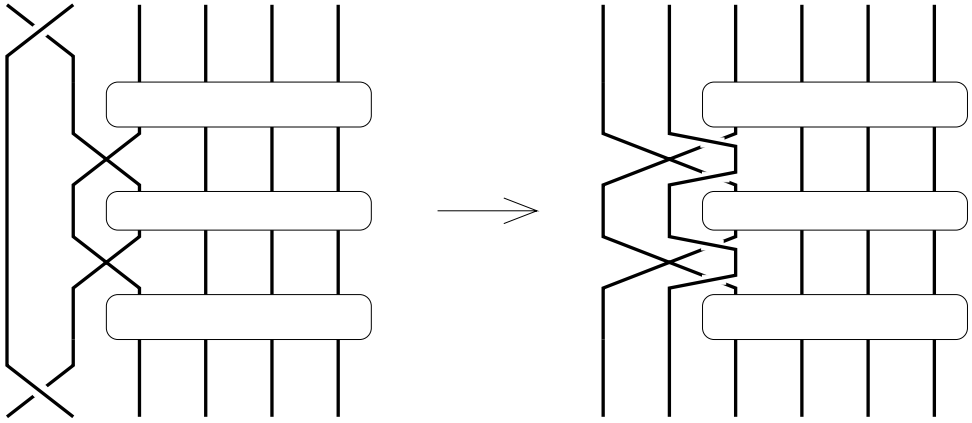


Fig. 3 – Réduction d'une poignée

L'expérience montre qui si l'on se borne à réduire les poignées dans n'importe quel ordre, sans contraintes, il existe des suites infinies de réductions de poignées. L'algorithme final ne réduira qu'un certain type de poignées, qu'on définit à présent.

Définition 3.2.2 — *On dit qu'une i-poignée est* admissible *si elle ne contient pas de $i+1$-poignée. Soient w et w' deux mots de tresse. On dit que w' est obtenu à partir de w par* réduction d'une poignée *s'il existe une i-poignée admissible $v = \sigma_i^e u \sigma_i^{-e}$ dans w, telle que w' s'obtienne en remplaçant dans w les lettres du sous-mot v suivant le schéma :*

$$\sigma_k^d \longmapsto \begin{cases} \sigma_k^d & si \quad k \neq i, i+1 \\ \epsilon & si \quad k = i \\ \sigma_{i+1}^{-e} \sigma_i^d \sigma_{i+1}^e & si \quad k = i+1 \end{cases}$$

On note $w \looparrowright^{(1)} w'$. De même que pour $\curvearrowright^{(n)}$, on définit $\looparrowright^{(n)}$ par récurrence, et on dit que w' s'obtient à partir de w par réduction de poignées *s'il existe n tel que $w \looparrowright^{(n)} w'$, ce qu'on note $w \looparrowright w'$.*

Ceci n'est pas un algorithme à proprement parler, car il se peut que dans un mot donné, il y ait plusieurs poignées admissibles parmi lesquelles choisir. Mais il n'est pas besoin de préciser davantage, car on va montrer que sous la seule contrainte de ne réduire que des poignées admissibles, toute suite de réduction de poignées est finie.

3.3 Terminaison de la réduction des poignées

Il y a deux arguments à donner. Tout d'abord un argument de finitude, par lequel on établira que l'ensemble des mots qu'on peut atteindre à partir d'un mot donné en n'utilisant que la réduction des poignées est en un certain sens fini, ensuite un argument d'acyclicité, qui nous permettra d'affirmer que la réduction des poignées ne peut donner de boucle.

Définition 3.3.1 — *Soit G un groupe, et S un système de générateurs pour ce groupe. Le* graphe de Cayley *de G relativement à S a pour sommets l'ensemble des éléments de G, et comporte pour tout s une arête orientée de g à gs. On définit de même le graphe de Cayley d'un monoïde.*

Soit b une tresse positive. Le graphe de Cayley *de b est le sous-graphe de celui de B_n ayant pour sommets les diviseurs de b dans B_n^+, et pour arêtes toutes les arêtes entre diviseurs de b.*

Définition 3.3.2 — *Soit Γ un graphe dont les arêtes orientées sont indexées par un alphabet A, soit s l'un de ses sommets, et soit w un mot sur $A^{\pm}$. On dit que w est* tracé dans Γ à partir de *s si w est le mot vide, ou bien s'il est de la forme xv (respectivement $x^{-1}v$), avec $x \in A$ et $v \in A^{\pm\star}$, et s'il existe un sommet t de Γ et une arête indexée par x de s vers t (respectivement de t vers s), tels que v soit tracé dans Γ à partir de t.*

Par exemple, il est clair que tout mot positif représentant b est tracé dans le graphe de Cayley de b à partir de e. Pour toute tresse positive b, le graphe de Cayley de b est fini. Nous allons montrer qu'un mot de tresse w étant donné, il existe une tresse positive b telle que w soit tracé dans le graphe de Cayley de b, ainsi que tout mot w' tel que $w \looparrowright w'$.

Lemme 3.3.1 — *Soit b une tresse positive. L'ensemble des mots tracés dans le graphe de Cayley de b à partir d'un point donné est stable par retournement à droite et à gauche.*
Démonstration — Supposons que $w = v\sigma_i^{-1}\sigma_j v'$ soit tracé dans Γ, le graphe de Cayley de b, à partir de a. Il faut montrer qu'il en va de même pour $w = vf(\sigma_i,\sigma_j)f(\sigma_j,\sigma_i)^{-1}v'$. On peut supposer que $v = \epsilon$ quitte à changer a en $a\overline{v}$, et il s'agit de montrer que si $\sigma_i^{-1}\sigma_j$ est tracé dans Γ à partir de a alors $f(\sigma_i,\sigma_j)f(\sigma_j,\sigma_i)^{-1}$ aussi. L'hypothèse est qu'il existe a' positive telle que $a'\sigma_i$ et $a'\sigma_j$ soient des diviseurs de b. Mais alors $a'\sigma_i f(\sigma_i,\sigma_j) = a'\sigma_j f(\sigma_j,\sigma_i)$ est un diviseur de b, car $\sigma_i f(\sigma_i,\sigma_j) = \sigma_i \vee \sigma_j$, ce qui montre que $f(\sigma_i,\sigma_j)f(\sigma_j,\sigma_i)^{-1}$ est tracé dans Γ à partir de $a = a'\sigma_i$. On démontre de façon analogue la propriété de stabilité par retournement à gauche. ✓

Définition 3.3.3 — *On appelle* équivalence positive *(respectivement* équivalence négative*) la relation d'équivalence sur $A^{\pm\star}$ compatible à la concaténation engendrée par les couples (u,v) (respectivement (u^{-1},v^{-1}) avec u et v positifs et positivement équivalents.*

Ainsi, on passe d'un mot à l'autre par équivalence positive en remplaçant un sous-mot positif par un mot positif qui lui est équivalent, et on passe d'un mot à l'autre par équivalence négative en remplaçant un sous-mot négatif par un mot négatif qui lui est équivalent. On obtient sans difficulté le lemme suivant.

Lemme 3.3.2 — *Soit b une tresse positive. L'ensemble des mots tracés dans le graphe de Cayley de b à partir d'un point donné est stable par équivalences positive et négative.*

Proposition 3.3.1 — *Soient w et w' deux mots de tresse, tels que $w \looparrowright w'$. Alors ils sont tous les deux tracés dans le graphe de Cayley de $|w|$ à partir de $\overline{D_l(w)}$.*
Démonstration — On montre par récurrence sur la longueur de w qu'il est tracé dans le graphe de Cayley de $|w|$ à partir de $\overline{D_l(w)}$. Il nous suffit ensuite, en vertu des deux lemmes précédents, de montrer que si $w \looparrowright^{(1)} w'$, alors w' s'obtient à partir de w par équivalences positive et négative, et par retournements à gauche et à droite. Mais la réduction de la poignée admissible $\sigma_i^e u_0 \sigma_{i+1}^d u_1 \dots u_{k-1}\sigma_{i+1}^d u_k \sigma_i^{-e}$ (avec u_j ne contenant pas les lettres σ_h avec $h < i+2$) peut se décomposer en plusieurs étapes. Si $e = d$, on imagine que la dernière lettre $x = \sigma_i^{-e}$ est poussée vers le début : elle commute avec les lettres des u_j grâce au retournement dans le cas de signes contraires et grâce à l'équivalence (positive ou négative selon le signe de e) dans le cas de signes égaux, et par retournement $\sigma_{i+1}^d x$ devient $x\sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e$. Si $e = -d$ c'est la première lettre qui doit atteindre la fin du mot. ✓

Maintenant qu'on a ce résultat de finitude, on va pouvoir donner une borne sur la longueur d'une suite de réductions de poignées.

Définition 3.3.4 — *Soit w un mot de tresse. Si i est l'indice minimal d'un générateur apparaissant dans w et j l'indice maximal, l'entier $n = j - i + 2$ est par définition la* largeur *de w. C'est le nombre de brins qui interviennent effectivement dans w. La* hauteur *de w est le nombre maximal de σ_i apparaissant dans un mot ne contenant aucun σ_i^{-1} et tracé dans le graphe de Cayley de $|w|$, pour i variant.*

Proposition 3.3.2 — *Soit w un mot de tresse de longueur l et de largeur n. Alors sa hauteur h est inférieure à $(n-1)^{ln(n-1)/2}$.*

Démonstration — Si un mot de tresse tracé dans un graphe de Cayley ne contient que des puissances positives de σ_i, alors chaque occurrence de cette lettre correspond à une arête différente, car dans le cas contraire, on aurait une boucle qui croiserait toujours dans le sens positif les arêtes indexées par σ_i, ce qu'exclut la proposition 3.1.1. La hauteur de w est donc majorée par le nombre d'arêtes dans le graphe de Cayley de $|w|$. Mais on montre que celui-ci est moindre que $(n-1)^{ln(n-1)/2}$. ✓

Nous nous attaquons maintenant au problème de la réduction des poignées à proprement parler. Soient w et w' deux mots de tresse tels que $w \twoheadrightarrow^{(1)} w'$. Supposons de plus que $w = v\sigma_1^e u_0 \sigma_2^d u_1 \dots u_{k-1}\sigma_2^d u_k \sigma_1^{-e} v'$, avec les notations de la proposition 3.3.1, et que c'est la 1-poignée qui a été réduite. Il est possible que cette réduction entraîne l'apparition d'une nouvelle 1-poignée, car les σ_2^d vont être transformés en $\sigma_2^{-e}\sigma_1^d\sigma_2^e$, faisant ainsi apparaître de nouvelles lettres σ_1^d.

Appelons $\mathrm{pref}_p(w)$ le préfixe de w allant jusqu'à (et incluant) la première lettre de la p-ème poignée. On constate que si la réduction de la p-ème poignée en fait apparaître une nouvelle, elle peut être considérée comme l'héritière de celle qui a été réduite, au sens où pour tout i, $\mathrm{pref}_i(w) \equiv \mathrm{pref}_i(w')$ sauf pour $i = p$. On démontre au cas par cas qu'il existe u tracé de $\mathrm{pref}_p(w)$ à $\mathrm{pref}_p(w')$ dans le graphe de Cayley de $|w|$, contenant une lettre σ_1^{-1} et pas de lettre σ_1 : si par exemple $e = d = 1$ et la nouvelle poignée se termine à droite de l'ancienne (i.e. la première occurrence de σ_1 dans v' est négative), on prend $u = mm'$ où $m = u_0\sigma_2 u_1 \dots u_{k-1}\sigma_2 u_k \sigma_1^{-1}$, sous-mot de w, et m' est le sous-mot de w' commençant là où l'ancienne poignée s'achève, et reculant jusqu'au début de la nouvelle poignée (w' est $\sigma_1\sigma_2 u_k$ à l'envers).

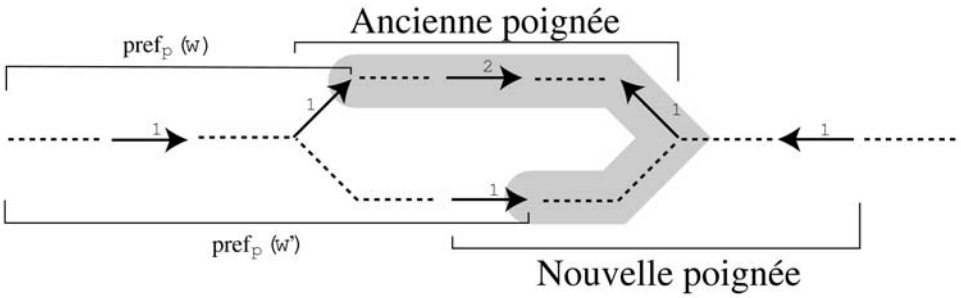


Fig. 4 – Cas σ_2-positif

Lemme 3.3.3 — *Soit une suite $w = w_0 \twoheadrightarrow^{(1)} \dots \twoheadrightarrow^{(1)} w_k$ de réductions de 1-poignées, où w est un mot de longueur l et de hauteur h. Alors $k \leqslant lh$. Plus généralement, si w est de largeur n, de longueur l, et de hauteur h, alors toute suite de réduction de poignées commençant en w est de longueur majorée par $l(2h)^{2n-1}$.*

Démonstration — Considérons les héritiers successifs de la p-ème 1-poignée de w, qui apparaissent dans les mots $w_1, \dots, w_{k_p}$. L'argument précédent nous donne des mots $u_{p,i}$ tracés dans le graphe de Cayley de $|w|$, ne contenant qu'une fois la lettre σ_1^{-1}, et pas de σ_1, et tels que $u_{p,1} \dots u_{p,p_k}$ soit aussi tracé dans ce graphe de Cayley. Par définition de la hauteur, on a donc $p_k \leqslant h$. Les héritiers de chaque 1-poignée sont donc réduits au plus h fois. Comme il y a moins de l 1-poignées dans w, on obtient $k \leqslant lh$.

Nous n'avons considéré que des réductions de 1-poignées. Or il se peut que pour rendre une 1-poignée admissible, il faille réduire des 2 poignées, et ainsi de suite. Mais on peut généraliser la technique précédente pour majorer le nombre de réductions de $i+1$-poignées entre deux réductions de i-poignées, et en majorant brutalement les longueurs des mots obtenus on trouve la borne générale annoncée. ✓

Proposition 3.3.3 — *Soit w un mot de tresse de largeur n et de longueur l. Toute suite de réductions de poignées commençant en w converge en au plus $2^{n^4 l}$ étapes.*

Démonstration — Il suffit d'inclure la borne sur la hauteur d'un mot au résultat précédent. ✓

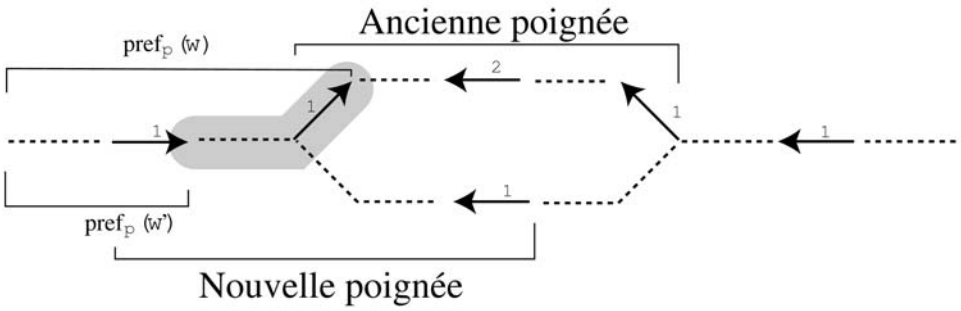


FIG. 5 – Cas σ_2-négatif

Références

[Bir74] Joan S. Birman, *Braids, links, and mapping class groups*, Princeton University Press, Princeton, N.J., 1974, Annals of Mathematics Studies, No. 82. MR 51 #11477

[Deh00] Patrick Dehornoy, *Braids and self-distributivity*, Birkhäuser Verlag, Basel, 2000. MR 2001j :20057