Aspects algorithmiques du retournement de mot

Marc Autord

Université de Caen Basse-Normandie
U.F.R. de Sciences
École doctorale SIMEM

T H È S E

présentée par

M. **Marc AUTORD**

et soutenue le 7 mai 2009

en vue de l'obtention du

DOCTORAT de l'UNIVERSITÉ de CAEN

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

Aspects algorithmiques du retournement de mot

MEMBRES du JURY

M. Martin ANDLER, professeur à l'Université de Versailles
M. Patrick DEHORNOY, professeur à l'Université de Caen *(directeur)*
M. Bernard LECLERC, professeur à l'Université de Caen
M. Géraud SÉNIZERGUES, professeur à l'Université de Bordeaux *(rapporteur)*
M. Victor UFNAROVSKI, professeur à l'Université de Lund (Suède) *(rapporteur)*

SOMMAIRE

SOMMAIRE

REMERCIEMENTS

Merci à Patrick Dehornoy, mon efficace et sage guide.

Merci à Géraud Sénizergues pour son rapport et son apport.

Хотелось бы особо и от всей души поблагодарить Виктора Анатольевича Уфнаровского. Он не только подсказал один из вопросов, которые я рассмотрел в своей работе, но и согласился написать рецензию на мою диссертацию (а ведь она на французском языке !), за что я ему очень признателен

Merci à Martin Andler et Bernard Leclerc. Dans mon jury de Licence (de DEUG à l'époque), dans mon jury de Master et maintenant dans mon jury de Doctorat. LMD. La der des ders ?

Merci à Guillermo Moreno-Socías pour sa présence. Et pas seulement dans mon jury.

Merci à Camille, miroir de ma fragilité.

Merci à Chloé pour son recul et sa délicatesse. Et pour ses remerciements.

Merci à Corentin, gentleman au grand cœur du bureau 108.

Merci à Émeline, ma sœur d'armes. Quel obstacle n'avons-nous pas vaincu ?

Merci à Emmanuel, perspicace et joueur.

Merci à Erwan pour cette discussion sous un porche dont l'écho résonne encore souvent.

Merci à Jean-Michel de ne freiner que rarement. Juste quand il faut.

Merci à Pierre pour l'élan avant le saut.

Merci à Filippo, Ion et Mathieu d'être restés une fois les jeux terminés.

Merci aux membres du bureau 108 — Benjamin, Pierre et Philippe — pour leur accueil quand je passe les voir.

Merci aux jeunes du labo pour l'ambiance si sympathique.

Merci à ma famille. Toujours là. Passé, présent et futur. Réciproquer est un défi agréable.

Merci à Lucie, le centre de mes émotions.

Enfin, merci à toi aimable lecteur de faire en sorte que la phrase suivante se réalise :

« Tu es en train de lire ces mots. »

REMERCIEMENTS

INTRODUCTION
DANS LA LANGUE DE DESPROGES

LE CONTEXTE GÉNÉRAL

Le sujet de cette thèse est le retournement de mot, une méthode combinatoire permettant d'étudier certains monoïdes spécifiés par une présentation et, typiquement, de résoudre le problème de mot associé.

PRÉSENTATIONS DE SEMIGROUPE ET DIAGRAMMES DE VAN KAMPEN

Les présentations auxquelles la méthode du retournement peut s'appliquer sont des présentations de semigroupe, c'est-à-dire les présentations du type $(\mathcal{S}, \mathcal{R})$, où $\mathcal{S}$ est un ensemble non vide de générateurs (ou lettres) et où $\mathcal{R}$ est une famille de relations de semigroupe sur $\mathcal{S}$, c'est-à-dire une famille de relations du type $u = v$ où u et v sont des mots *non vides* sur l'alphabet $\mathcal{S}$. Un exemple typique de présentation de semigroupe est la présentation standard du monoïde de tresses positives B_n^+, pour laquelle l'alphabet est $\{\sigma_1, ..., \sigma_{n-1}\}$ et les relations sont

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \qquad \text{pour } |i-j| = 1, \tag{1}$$

$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{pour } |i-j| \geq 2. \tag{2}$$

D'une façon générale, on notera $\langle \mathcal{S}; \mathcal{R} \rangle^+$ le monoïde associé à une présentation $(\mathcal{S}, \mathcal{R})$.

Par définition, si un monoïde M est engendré par une famille $\mathcal{S}$, alors tout élément de M peut s'exprimer comme un produit (éventuellement vide) d'éléments de $\mathcal{S}$, c'est-à-dire qu'il est l'évaluation dans M d'un *mot* sur l'alphabet $\mathcal{S}$. On notera $\mathcal{S}^*$ l'ensemble des mots sur l'alphabet $\mathcal{S}$ et, dans le contexte précédent, si w est un mot de $\mathcal{S}$, on note $\overline{w}$ l'élément de M représenté par w.

Dire alors que le monoïde M admet la présentation $(\mathcal{S}, \mathcal{R})$ signifie, par définition, que deux mots w, w' de $\mathcal{S}^*$ représentent le même élément de M, c'est-à-dire vérifient $\overline{w} = \overline{w}'$, si et seulement si il existe une *$\mathcal{R}$-dérivation de w à w'*, définie comme une suite finie de mots $w_0, ..., w_N$ de $\mathcal{S}^*$ vérifiant $w_0 = w$, $w_N = w'$, et telle que, pour tout k, le mot w_k s'obtient à partir de w_{k-1} en appliquant une relation de $\mathcal{R}$, c'est-à-dire qu'il existe une

relation $u = v$ dans $\mathcal{R}$ et des mots u', u'' vérifiant

$$w_{k-1} = u'uu'' \text{ et } w_k = u'vu'', \quad \text{ou} \quad w_{k-1} = u'vu'' \text{ et } w_k = u'uu''.$$

Par exemple, les mots de tresse $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ et $\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$ représentent le même élément du monoïde B_4^+ puisqu'il existe une dérivation de l'un à l'autre à l'aide des relations de tresse (1) et (2), par exemple la suite de longueur 9 (huit relations appliquées)

$$\begin{aligned}(3)\quad &\sigma_1\sigma_2[\sigma_1\sigma_3]\sigma_2\sigma_1, \qquad \sigma_1\sigma_2\sigma_3[\sigma_1\sigma_2\sigma_1], \qquad \sigma_1[\sigma_2\sigma_3\sigma_2]\sigma_1\sigma_2,\\ &[\sigma_1\sigma_3]\sigma_2\sigma_3\sigma_1\sigma_2, \qquad \sigma_3\sigma_1\sigma_2[\sigma_3\sigma_1]\sigma_2, \qquad \sigma_3[\sigma_1\sigma_2\sigma_1]\sigma_3\sigma_2,\\ &\sigma_3\sigma_2\sigma_1[\sigma_2\sigma_3\sigma_2], \qquad \sigma_3\sigma_2[\sigma_1\sigma_3]\sigma_2\sigma_3, \qquad \sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3,\end{aligned}$$

où, à chaque étape, on a indiqué en gras le sous-mot auquel une relation va être appliquée.

Une façon équivalente de dire qu'il existe une $\mathcal{R}$-dérivation d'un mot w en un mot w' est de dire qu'il existe un *diagramme de van Kampen* dont le bord est étiqueté (w, w'). Un tel diagramme est un graphe planaire orienté dont les arêtes sont étiquetées par les lettres de $\mathcal{S}$, dont les faces sont étiquetées par des paires de mots (u, v) telles que $u{=}v$ est une relation de $\mathcal{R}$, et dont le bord consiste en deux chemins respectivement étiquetés w et w', voir la figure 1. Si $(w_0, ..., w_N)$ est une $\mathcal{R}$-dérivation de w à w', alors on obtient un diagramme de van Kampen pour (w, w') en partant d'un chemin étiqueté w et en juxtaposant dans une direction orthogonale des pavés correspondant aux relations successivement appliquées. Inversement, si $\mathcal{K}$ est un diagramme de van Kampen pour (w, w'), on obtient une $\mathcal{R}$-dérivation de w à w' en partant de w et en lisant les étiquettes d'une suite de chemins obtenus en franchissant un à un les pavés qui composent $\mathcal{K}$.

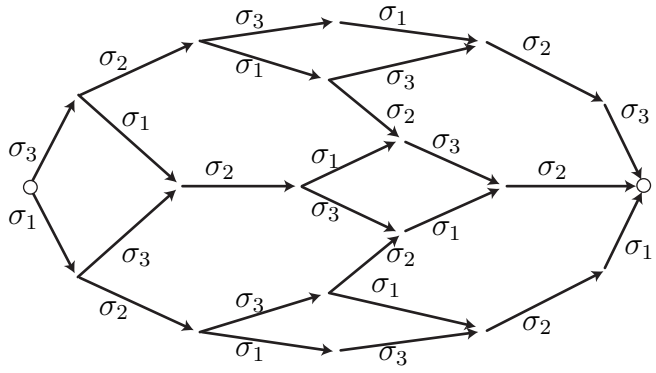
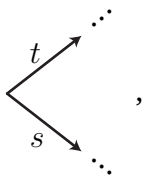


FIGURE 1 – Diagramme de van Kampen associé à la dérivation (3).

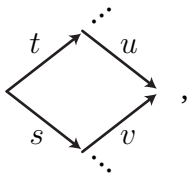
RETOURNEMENT DE MOT : LE PRINCIPE

Apparemment introduite pour la première fois par P. Dehornoy dans [11] afin d'étudier un certain monoïde lié à la loi d'autodistributivité [13], la méthode du retournement de mot apparaît indépendamment chez K. Tatsuoka dans [26] et, sous une forme un peu différente mais essentiellement équivalente chez R. Corran dans [10] et chez S. Hermiller et J. Meier dans [19]. La méthode a ensuite été étudiée de façon plus systématique dans [12], pour les groupes de tresses, puis dans [14] et [16] pour des cas plus généraux.

Le retournement de mot est une stratégie pour tenter de construire des $\mathcal{R}$-dérivations ou, de façon équivalente, des diagrammes de van Kampen. Partant de deux mots w, w' de $\mathcal{S}^*$, cette stratégie cherche à obtenir une $\mathcal{R}$-dérivation de w à w' en considérant à chaque fois le premier désaccord entre les mots de la dérivation en cours de construction ou, si on préfère, le motif ouvert le plus à gauche dans le diagramme de van Kampen en cours de construction. Un tel motif a la forme générale



où s et t sont deux lettres de $\mathcal{S}$, et la stratégie retenue consiste à fermer un tel motif en adjoignant à droite des mots u, v tels que $sv = tu$ est une des relations de $\mathcal{R}$:

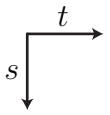


et à itérer la construction. Ainsi, il s'agit simplement de tenter de construire un diagramme de van Kampen en partant toujours de la gauche. On voit par exemple que le diagramme de la figure 1 peut s'obtenir de la sorte.

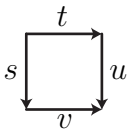
À ce stade, il n'est pas clair que le retournement de mot doive réussir, au sens où, même si on part de mots initiaux w, w' qui sont $\mathcal{R}$-équivalents, donc tels qu'il existe un diagramme de van Kampen pour (w, w'), rien ne prouve en général que la stratégie de retournement doive fournir un tel diagramme : il se peut que le retournement bloque (pas de relation $s... = t...$ permettant de continuer), ou encore qu'il ne termine jamais. Notons aussi que la stratégie de retournement ne fournit un algorithme que si la présentation considérée a la propriété que, pour chaque paire de lettres s, t, il existe au plus une relation de la forme $s... = t...$.

RETOURNEMENT DE MOT : FORMALISATION

Pour décrire précisément le retournement de mot, il est d'abord commode de dessiner les diagrammes de van Kampen associés d'une façon un peu différente, de sorte qu'ils soient inscrits sur une grille rectangulaire et que les arêtes soient exclusivement verticales orientées vers le bas ou horizontales orientées vers la droite. De la sorte, l'étape de base du retournement illustrée ci-dessus correspond à

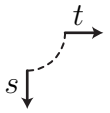


complété en

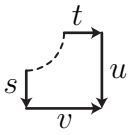


pour $sv = tu$ dans $\mathcal{R}$.

Pour pouvoir maintenir cette convention (qui jouera un rôle mathématique, et pas seulement notationnel, dans les chapitres 4 et 5), on doit introduire un troisième type d'arêtes, étiquetées par le mot vide ε, reliant des sommets qui doivent être identifiés. En pratique, ces ε-arêtes seront représentées comme des arcs en pointillé, de sorte que le schéma général correspondant à l'étape de base devient



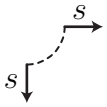
complété en



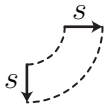
pour $sv = tu$ dans $\mathcal{R}$,

y compris le cas de lettres coïncidentes

(*)



complété en



,

qui entre dans le cas général si on considère $s = s$ comme une relation par défaut.

De la sorte, on obtient ce qu'on appellera un *diagramme de retournement*, voir la figure 2. Celui-ci n'est pas un diagramme de van Kampen, mais il le devient lorsqu'on contracte sur un point les ε-arêtes.

Il est alors facile de traduire en termes purement syntaxiques le retournement de mot. Pour ce faire, on introduit une copie notée $\mathcal{S}^{-1}$ de l'alphabet $\mathcal{S}$, contenant une lettre s^{-1} pour chaque lettre s de $\mathcal{S}$, et on code les chemins dans un diagramme de retournement par la suite des étiquettes des arêtes parcourues, avec la convention que la contribution d'une arête étiquetée s parcourue dans le sens opposé à son orientation est s^{-1}.

Si alors on parcourt du coin inférieur gauche au coin supérieur droite les chemins successifs obtenus lors de la construction d'un diagramme de retournement contenant N étapes élémentaires, on obtient $N + 1$ mots $w_0, ..., w_N$ sur l'alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$, dont le premier est $w^{-1}w'$ et le dernier est le mot vide ε. Chaque étape élémentaire correspond alors à remplacer un sous-mot du type $s^{-1}t$ par un mot vu^{-1} où $sv = tu$ est une relation de $\mathcal{R}$, y

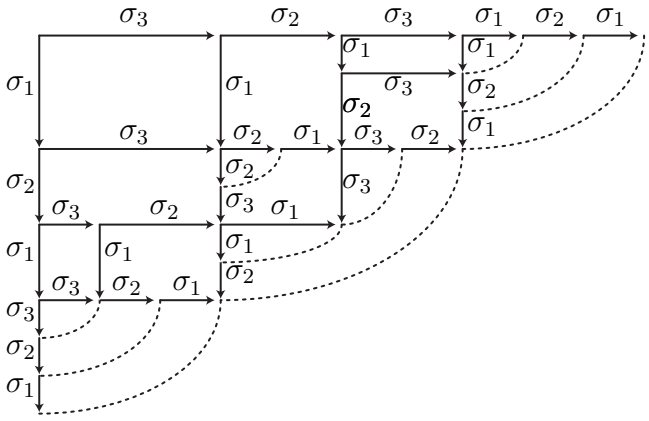


FIGURE 2 – Diagramme de retournement correspondant au diagramme de van Kampen de la figure 1 : les arêtes sont toutes verticales orientées vers le bas ou horizontales orientées vers la droite ; lorsqu'on contracte les arêtes en pointillé sur un point, on obtient le diagramme de van Kampen de la figure 1.

compris le cas particulier où on remplace $s^{-1}s$ par le mot vide, qui correspond à la relation implicite $s = s$. On voit que cette étape de base consiste à remplacer un motif dont les signes sont $-+$ par un nouveau motif dont les signes sont $+-$, et c'est ce qui explique la dénomination "retournement".

Dans le contexte ci-dessus, c'est-à-dire dès que $(\mathcal{S}, \mathcal{R})$ est une présentation de semi-groupe, on peut donc introduire une règle de réécriture $\curvearrowright_{\mathcal{R}}$ sur les mots de $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ en déclarant que $w \curvearrowright^1_{\mathcal{R}} w'$ est vrai si w' s'obtient à partir de w en remplaçant un sous-mot de la forme $s^{-1}t$ par vu^{-1} tel que $sv = tu$ est une relation de $\mathcal{R}$, et en appelant $\curvearrowright_{\mathcal{R}}$ la clôture réflexive–transitive de $\curvearrowright^1_{\mathcal{R}}$.

LES RÉSULTATS PRÉCÉDEMMENT CONNUS

On déclare qu'une présentation $(\mathcal{S}, \mathcal{R})$ est *complète* (pour le retournement) si la stratégie de retournement réussit toutes les fois que cela est possible, c'est-à-dire si, toutes les fois que w, w' sont des mots $\mathcal{R}$-équivalents de $\mathcal{S}^*$, alors le retournement fournit un diagramme de van Kampen pour (w, w'), soit encore, en termes de mots, si le mot $w^{-1}w'$ de $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ se retourne en le mot vide.

Le principal résultat de [12] et (dans un cadre plus général) de [16] est qu'il existe un critère effectif pour reconnaître la complétude d'une présentation. On en déduit par exemple que la présentation d'Artin des monoïdes de tresses donnée ci-dessus est complète et, de là, on obtient grâce au retournement une solution algorithmiquement efficace au problème de mot du monoïde B_n^+. On peut également utiliser le retournement pour reconnaître des

propriétés du monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ ou du groupe $\langle \mathcal{S}; \mathcal{R} \rangle$, typiquement pour établir que $\langle \mathcal{S}; \mathcal{R} \rangle^+$ est un monoïde de Garside.

LES RÉSULTATS DE CE TRAVAIL

Dans ce travail, nous approfondissons l'étude du retournement de mot à la fois comme outil général et dans des cas particuliers intéressants, principalement ceux du monoïde d'Heisenberg et des monoïdes de tresses d'Artin. Nous décrivons ci-dessous les principaux résultats nouveaux obtenus.

COMPARAISON AVEC LES BASES DE GRÖBNER–SHIRSHOV

Les résultats de [16] donnent davantage qu'un critère permettant — dans les bons cas — de reconnaître l'éventuelle complétude d'une présentation vis-à-vis du retournement. Dans le cas où le critère n'est pas satisfait, et où donc la présentation initiale $(\mathcal{S}, \mathcal{R})$ n'est pas complète, le critère fournit une nouvelle relation $u = v$, qui est conséquence des relations de $\mathcal{R}$, et dont l'ajout à $\mathcal{R}$ lève l'obstruction particulière constatée à la satisfaction du critère. Notant $\mathcal{R}'$ l'ensemble $\mathcal{R} \cup \{u{=}v\}$, on peut alors rappliquer le critère à la présentation $(\mathcal{S}, \mathcal{R}')$, qui définit le même monoïde que $(\mathcal{S}, \mathcal{R})$. La procédure peut ou bien s'arrêter, c'est-à-dire qu'on a obtenu une présentation complète, ou bien se poursuivre. Dans tous les cas, on a un processus de *complétion* qui, à partir d'une présentation initiale incomplète, mène, en un nombre fini ou infini d'étapes, à une présentation complète.

Formellement, cette procédure de complétion est analogue à la construction d'une base de Gröbner-Shirshov. D'abord introduite par Buchberger dans un contexte d'algèbre commutative pour étudier les idéaux d'une algèbres, la méthode des bases de Gröbner a été étendue par Shirshov et ses successeurs au cas des semigroupes et des groupes [5, 18, 22, 24]. Comme dans le cas du retournement, la construction d'une base de Gröbner-Shirshov consiste à partir d'une présentation $(\mathcal{S}, \mathcal{R})$ et à ajouter des relations redondantes conséquences de $\mathcal{R}$ jusqu'à ce qu'un certain critère de complétion soit satisfait.

Le point de départ de notre travail a été l'observation du fait que, sur certaines présentations simples, les complétions liées au retournement et aux bases de Gröbner-Shirshov coïncident, rendant très naturelle la comparaison des deux méthodes et rendant même une conjecture de coïncidence plausible.

Nous réfutons complètement cette conjecture : les deux types de complétion, à savoir la complétion pour le retournement, dite *R-complétion* ci-dessous, et la complétion de Gröbner-Shirshov, dite *G-complétion* ci-dessous, divergent en général. Le résultat que nous démontrons est le suivant (proposition II.4.1) :

> **Proposition :** *Chacune des situations suivantes est possible : il existe des présentations de semigroupe $(\mathcal{S}, \mathcal{R})$ telles que*

(i) *la R-complétion et la G-complétion coïncident,*

(ii) *la R-complétion est strictement incluse dans la G-complétion,*

(iii) *la G-complétion est strictement incluse dans la R-complétion,*

(iv) *la R-complétion et la G-complétion ne sont pas comparables pour l'inclusion.*

La démonstration se fait en construisant des exemples effectifs pour chacun des types — en fait des familles d'exemples pour lesquels on peut montrer des comportements uniformes. Par ailleurs, les résultats de divergence peuvent être affinés pour prendre en compte d'autres propriétés comme la finitude éventuelle de la complétion. Dans tous les cas, on conclut à des comportements non corrélés en général.

Les résultats de cette partie ont fait l'objet d'une publication, à paraître dans *European-Asian Journal of Mathematics* [2].

RETOURNEMENT ITÉRÉ

Soit $(\mathcal{S},\mathcal{R})$ une présentation de semigroupe. Pour w,w' dans $(\mathcal{S}\cup\mathcal{S}^{-1})^*$, déclarons que $w \curvearrowright_{\mathcal{R}}^{\boxed{2}} w'$ est vrai s'il existe deux mots u,v de $\mathcal{S}^*$ vérifiant

$$w \curvearrowright_{\mathcal{R}} vu^{-1} \quad \text{et} \quad u^{-1}v \curvearrowright_{\mathcal{R}} w'.$$

De la même façon, déclarons $w \curvearrowright_{\mathcal{R}}^{\boxed{k}} w'$ vrai si, pour $1 \leq i < k$, il existe des mots u_i, v_i de $\mathcal{S}^*$ vérifiant

$$w \curvearrowright_{\mathcal{R}} v_1u_1^{-1} \quad \text{et} \quad u_1^{-1}v_1 \curvearrowright_{\mathcal{R}} v_2u_2^{-1} \quad \text{et ... et} \quad u_{k-1}^{-1}v_{k-1} \curvearrowright_{\mathcal{R}} w'.$$

Autrement dit, on alterne retournement et permutation du numérateur et du dénominateur. La relation $\curvearrowright_{\mathcal{R}}^{\boxed{k}}$ sera appelée *retournement itéré de degré* k, et on dira que le problème de mot du monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$ (*resp.* du groupe $\langle\mathcal{S};\mathcal{R}\rangle$) est résoluble par retournement de degré k si, quels que soient les mots w,w' de $\mathcal{S}^*$ (*resp.* quel que soit le mot w de $(\mathcal{S}\cup\mathcal{S}^{-1})^*$), les mots w et w' représentent le même élément de $\langle\mathcal{S};\mathcal{R}\rangle^+$ (*resp.* w représente l'élément neutre de $\langle\mathcal{S};\mathcal{R}\rangle$) si et seulement si on a $w^{-1}w' \curvearrowright_{\mathcal{R}}^{\boxed{k}} \varepsilon$ (*resp.* $w \curvearrowright_{\mathcal{R}}^{\boxed{k}} \varepsilon$).

Dans le cas d'une présentation $(\mathcal{S},\mathcal{R})$ R-complète et telle que le monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$ admet la simplification à droite, qu'il existe dans $\mathcal{R}$ au plus une relation $s... = t...$ pour chaque paire de lettres s,t de $\mathcal{S}$, et qu'il existe un ensemble fini de mots $\widehat{\mathcal{S}}$ de $\mathcal{S}^*$ qui est clos par retournement au sens où, quels que soient u,v dans $\widehat{\mathcal{S}}$, il existe u',v' dans $\widehat{\mathcal{S}}$ vérifiant $u^{-1}v \curvearrowright_{\mathcal{R}} v'u'^{-1}$ — toutes hypothèses satisfaites notamment par la présentation standard des monoïdes de tresses, et, plus généralement, par les présentations canoniques des monoïdes de Garside — alors le problème de mot du monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$ est résoluble en temps quadratique par retournement itéré de degré 1 (c'est-à-dire par retournement simple), tandis

que le problème de mot du groupe $\langle \mathcal{S}; \mathcal{R} \rangle$ est résoluble, également en temps quadratique, par retournement itéré de degré 2.

La question posée était de savoir ce qui peut se passer lorsqu'on part d'une présentation non complète ou d'un groupe de fonction de Dehn plus que quadratique. Nous étudions plus particulièrement la version discrète du groupe d'Heisenberg, qui est associée à la présentation

$$(a, b, c \mid ab = bac, ac = ca, bc = cb). \tag{4}$$

Le résultat, assez surprenant, est que, bien que la présentation (4) ne soit pas complète, on obtient encore une solution par retournement itéré aux problèmes de mot du monoïde et du groupe associés, mais en augmentant le degré d'une unité par rapport aux exemples antérieurs (proposition III.2.5) :

> **Proposition :** *Le problème de mot du monoïde d'Heisenberg est résoluble par retournement itéré de degré 2. Le problème de mot du groupe d'Heisenberg est résoluble par retournement itéré de degré 3.*

Cet exemple n'est pas isolé et nous construisons d'autres exemples où le même comportement est observé.

DISTANCE COMBINATOIRE ENTRE MOTS DE TRESSE ET ENTRE EXPRESSIONS RÉDUITES DE PERMUTATION

Dans le cas particulier de la présentation d'Artin des monoïdes de tresses B_n^+ à partir des relations (1) et (2), on sait que le retournement (non itéré) résout le problème du mot du monoïde, et, pour chaque valeur de l'indice n fixée, on a une borne supérieure en ℓ^2 sur le nombre d'étapes élémentaires de retournement nécessaire pour retourner des mots de longueur ℓ. Par contre, extrêmement peu de choses étaient connues lorsqu'on fait varier l'indice n, c'est-à-dire quand on considère le retournement de mots sur l'alphabet infini $\{\sigma_1, \sigma_2, ...\}$.

D'une façon générale, si w, w' sont deux mots sur l'alphabet $\{\sigma_1, \sigma_2, ...\}$, on peut leur associer deux nombres entiers :

- le nombre d'étapes élémentaires (desquelles on exclut les étapes de type $(*)$) nécessaire pour retourner le mot $w^{-1}w'$, appelé *distance de retournement* de (w, w') et qu'on note $\mathrm{dist}_{\curvearrowright}(w, w')$,

- et, dans le cas où w et w' sont équivalents vis-à-vis des relations de tresse, ce qu'on notera $w \equiv w'$, la *distance combinatoire* entre w et w', définie comme le nombre minimal de relations de tresse nécessaires pour passer de w à w' et notée $\mathrm{dist}(w, w')$.

Comme le retournement est une stratégie particulière de construction d'un diagramme de van Kampen (donc d'une dérivation), on a la majoration

$$\mathrm{dist}(w, w') \leq \mathrm{dist}_{\curvearrowright}(w, w') \tag{5}$$

pour tout couple de mots de tresse (w, w') vérifiant $w \equiv w'$. L'objet de notre étude est de borner, inférieurement et supérieurement, les nombres $\mathrm{dist}(w, w')$ et $\mathrm{dist}_{\curvearrowright}(w, w')$.

Un cas particulier important est celui des mots de tresse dits *simples*, qui sont les mots codant des diagrammes de tresse dans lesquels deux brins quelconques se croisent au plus une fois. L'intérêt particulier de ces mots est qu'on peut également les voir comme des décompositions réduites d'une permutation en termes de transpositions. Le classique lemme d'échange des groupes de Coxeter affirme que deux décompositions réduites d'une même permutation sont toujours reliées par les relations (1) et (2), de sorte que, pour des mots de tresses simples, le nombre $\mathrm{dist}(w, w')$ est également la distance combinatoire entre les décompositions réduites associées.

Dans ce contexte, nous démontrons (corollaire IV.1.19) :

> **Proposition :** *Pour chaque n, il existe des mots de tresse simples w, w' en les lettres $\sigma_1, ..., \sigma_{n-1}$ vérifiant* $\mathrm{dist}(w, w') \geq n^4/8$.

D'où, en termes de permutations,

> **Corollaire :** *Pour chaque n, il existe des décompositions réduites w, w' d'une même permutation de $\{1, ..., n\}$ vérifiant* $\mathrm{dist}(w, w') \geq n^4/8$.

Ces résultat sont optimaux, car il existe une borne supérieure du même ordre de grandeur.

OPTIMALITÉ DU RETOURNEMENT

Il est facile de montrer que l'inégalité (5) peut être stricte : par exemple, si w et w' sont les mots de tresse $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ et $\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$ considérés plus haut, alors on lit sur les figures 1 ou 2 que la distance de retournement $\mathrm{dist}_{\curvearrowright}(w, w')$ vaut 8, alors qu'on peut construire une dérivation de w à w' de longueur 6, mais pas moins, de sorte que la distance combinatoire $\mathrm{dist}(w, w')$ vaut 6.

Par conséquent, le retournement n'est pas toujours optimal, et la question se pose naturellement de reconnaître les cas où il l'est, c'est-à-dire les cas où (5) est une égalité. Plus généralement, que les mots initiaux w, w' soient ou non équivalents, c'est-à-dire, que le retournement du mot $w^{-1}w'$ se termine avec le mot vide ou non, on souhaite pouvoir reconnaître quand un diagramme de retournement est optimal, au sens où le diagramme de van Kampen obtenu en contractant sur un point toutes les ε-arêtes réalise la distance combinatoire entre les mots qui étiquettent son bord ; on montre le résultat suivant (proposition IV.4.5) :

> **Proposition :** *Un diagramme de retournement ne contenant aucun pavé de type $(*)$ est optimal.*

La démonstration de ce résultat fait appel à la notion de *séparatrices*, qui sont des courbes transversales aux arêtes d'un diagramme de van Kampen provenant de la dualité

nom/position dans les permutations. Le point important est qu'un diagramme de van Kampen où deux séparatrices quelconques se coupent au plus une fois est nécessairement optimal, et que deux séparatrices ne peuvent se couper deux fois ou plus que s'il existe des pavés de type $(*)$. Le critère ci-dessus est d'autant plus intéressant qu'il s'applique également à des diagrammes de retournement légèrement modifiés dans lesquels plusieurs étapes sont regroupées, ce qui a pour effet d'éliminer un grand nombre de pavés de type $(*)$ et donc d'étendre la portée du critère.

COMPLEXITÉ DU RETOURNEMENT DES MOTS DE TRESSE

Pour des mots w, w' sur l'alphabet $\{\sigma_1, \sigma_2, \ldots\}$, la 2-complexité $\mathrm{L}_2(w^{-1}w')$ du mot $w^{-1}w'$ est le nombre de pavés (y compris ceux de type $(*)$) du diagramme de retournement de $w^{-1}w'$. Les résultats suivants visent à encadrer cette complexité. Pour les bornes inférieures, nous montrons (proposition V.2.1) :

> **Proposition :** *Pour chaque ℓ, il existe des mots de tresse simples w, w' de longueur ℓ vérifiant $\mathrm{L}_2(w^{-1}w') \geq \ell^4/8$.*

Cette proposition améliore la meilleure borne inférieure connue jusqu'à présent [12] et n'est pas une conséquence du corollaire IV.1.19 établissant une borne inférieure quartique sur la distance combinatoire : les mots utilisés pour prouver ce corollaire sont de longueur $n^2/2 + O(1)$, donc une transposition de ce résultat à l'aide de l'inégalité (5) ne donne qu'une borne inférieure en $O(\ell^2)$ pour la complexité de retournement $\mathrm{L}_2(w^{-1}w')$, et non en $O(\ell^4)$ comme ci-dessus.

L'étude des bornes supérieures se révèle nettement plus délicate. Nous conjecturons l'existence d'une borne supérieure en $O(\ell^4)$ pour $\mathrm{L}_2(w^{-1}w')$ lorsque w et w' sont des mots de tresse de longueur au plus ℓ, mais nous n'avons pour le moment aucune démonstration complète. Par contre, nous établissons plusieurs résultats partiels.

D'abord, nous améliorons la seule borne supérieure connue à ce jour, établie dans [17], en introduisant un raffinement du retournement, le *retournement pacifique*, ayant la propriété de s'effectuer en plus d'étapes que le retournement classique, quel que soit le mot initial. En bornant supérieurement le retournement pacifique, on montre (proposition V.4.11) :

> **Proposition :** *Quels que soient les mots de tresse w, w' de longueur ℓ, on a $\mathrm{L}_2(w^{-1}w') \leq 3^{4\ell}\ell^2/4$.*

Puis nous utilisons la méthode des courbes séparatrices pour analyser les diagrammes de retournement et obtenir des majorations sur le nombre de pavés pouvant y figurer. Cette analyse mène à l'introduction de *motifs répétiteurs*, des sous-diagrammes particuliers, dont l'apparition dans un diagramme de retournement est équivalente au fait que des séparatrices se recoupent plusieurs fois — c'est-à-dire, d'après ce qui a été mentionné plus haut, lorsqu'on a un diagramme de retournement non optimal. On montre que les motifs répétiteurs

sont caractérisés par la donnée d'un type (parmi trois) et d'un quadruplet de paramètres (pris dans un ensemble fini dont la taille dépend du nombre de brins du mot de tresse initial).

Plus un retournement requiert d'étapes, plus les séparatrices du diagramme associé se croisent souvent. On observe toutefois que le cas de séparatrices se croisant beaucoup n'arrive pas. On est mené à poser (conjecture V.6.12) :

> **Conjecture :** *Un diagramme de retournement ne contient au plus qu'un seul motif répétiteur pour chaque type et chaque valeur des paramètres.*

Moyennant cette hypothèse, on démontre (proposition V.6.13) :

> **Proposition :** *Sous l'hypothèse que la conjecture ci-dessus est vraie, il existe une constante* C *telle que, quels que soient les mots de tresse* w, w' *de longueur* ℓ*, on a* $\mathrm{L}_2(w^{-1}w') \leq \mathrm{C}\,\ell^6$.

Ce résultat reflète l'expérimentation de manière plus pertinente que la meilleure borne prouvée, qui est exponentielle en la longueur, puisqu'aucun calcule ne dépasse la borne quartique. Un résultat analogue vaut encore sous l'hypothèse plus faible que le nombre d'occurrences de chaque type de motif répétiteur est borné supérieurement par $O(\ell)$.

Les résultats des trois dernières parties font l'objet d'une soumission [3].

ORGANISATION DU TEXTE

La rédaction de la thèse suit l'ordre des résultats décrits ci-dessus. La première partie est consacrée à la méthode générale du retournement. Le chapitre I donne les définitions de base et un certain nombre de résultats existant dans la littérature. Le chapitre II est consacré à la comparaison entre les complétions associées au retournement et aux bases de Gröbner-Shirshov. Le chapitre III est consacré au retournement itéré et au monoïde d'Heisenberg.

La seconde partie concerne le retournement des mots de tresse. Dans le chapitre IV, on étudie les liens entre retournement et distance combinatoire. Dans le chapitre V enfin, on établit les bornes sur la complexité du retournement des mots de tresse.

INTRODUCTION

PAS DANS LA LANGUE DE DESPROGES

GENERAL SETTING

This thesis deals with word reversing, a combinatorial technique allowing the study of certain monoids given by a presentation. In particular, it provides some of the times a solution to the associated word problem.

SEMIGROUP PRESENTATIONS AND VAN KAMPEN DIAGRAMS

The presentations to which the word reversing method may be applied are semigroup presentations, that is presentations of the type $(\mathcal{S}, \mathcal{R})$, where $\mathcal{S}$ is a nonempty set of generators (or letters) and where $\mathcal{R}$ is a family of semigroup relations, *i.e.*, a family of relations of the form $u = v$, with u and v nonempty words on the alphabet $\mathcal{S}$. A typical example of such presentation is the standard presentation of the positive braids monoid B_n^+, whose alphabet is $\{\sigma_1, ..., \sigma_{n-1}\}$ and whose relations are

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \qquad \text{for } |i-j| = 1, \tag{6}$$

$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{for } |i-j| \geq 2. \tag{7}$$

In the sequel, we note $\langle \mathcal{S}; \mathcal{R} \rangle^+$ the monoid whose presentation is $(\mathcal{S}, \mathcal{R})$.

By definition, if a monoid M is generated by a family $\mathcal{S}$, then every element of M may be expressed as a product (possibly empty) of elements of $\mathcal{S}$, *i.e.*, it is the evaluation in M of a *word* on the alphabet $\mathcal{S}$. We note $\mathcal{S}^*$ the set of all the words on the alphabet $\mathcal{S}$ and, within the previous setting, if w is a word of $\mathcal{S}^*$, we note $\mathrm{eval}_M(w)$, or simply $\overline{w}$, the element of M represented by w.

Thus, to say that the monoid M admits the presentation $(\mathcal{S}, \mathcal{R})$ amounts to say, by definition, that two words w, w' of $\mathcal{S}^*$ represent the same element of M, *i.e.*, satisfy $\overline{w} = \overline{w'}$, if and only if there exists a *$\mathcal{R}$-derivation from w to w'*, that is a finite sequence of words $w_0, ..., w_N$ of $\mathcal{S}^*$ verifying $w_0 = w$, $w_N = w'$, and such that, for every k, one obtains the word w_k from w_{k-1} by applying a relation of $\mathcal{R}$, that is to say that there exist a relation $u = v$ in $\mathcal{R}$ and words u', u'' satisfying

$$w_{k-1} = u'uu'' \text{ et } w_k = u'vu'', \quad \text{or} \quad w_{k-1} = u'vu'' \text{ and } w_k = u'uu''.$$

For instance, the braid words $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ and $\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$ represent the same element of the monoid B_4^+ since there exists a derivation from one to the other using only braid relations (6) and (7), for example the sequence of length 9 (eight relations applied)

$$\begin{aligned}(8)\quad &\sigma_1\sigma_2[\sigma_1\sigma_3]\sigma_2\sigma_1, \qquad \sigma_1\sigma_2\sigma_3[\sigma_1\sigma_2\sigma_1], \qquad \sigma_1[\sigma_2\sigma_3\sigma_2]\sigma_1\sigma_2,\\ &[\sigma_1\sigma_3]\sigma_2\sigma_3\sigma_1\sigma_2, \qquad \sigma_3\sigma_1\sigma_2[\sigma_3\sigma_1]\sigma_2, \qquad \sigma_3[\sigma_1\sigma_2\sigma_1]\sigma_3\sigma_2,\\ &\sigma_3\sigma_2\sigma_1[\sigma_2\sigma_3\sigma_2], \qquad \sigma_3\sigma_2[\sigma_1\sigma_3]\sigma_2\sigma_3, \qquad \sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3,\end{aligned}$$

where, at each step, the bold subword is the one on which a relation is about to be applied.

Saying that there exists an $\mathcal{R}$-derivation from a word w to a word w' is equivalent to saying that there exists a *van Kampen diagram* whose border is labeled (w, w'). A van Kampen diagram is a directed planar graph whose edges are labeled by letters of $\mathcal{S}$, whose faces are labeled by pairs of words (u, v) such that $u{=}v$ is a relation of $\mathcal{R}$, and whose border consists in two paths respectively labeled w and w', see Figure 3. If the finite sequence $(w_0, ..., w_N)$ is an $\mathcal{R}$-derivation from w to w', then one obtains a van Kampen diagram for (w, w') by starting from a path labeled w and by putting next to each other, according to a perpendicular direction, tiles corresponding to the relations successively applied. Conversely, if $\mathcal{K}$ is a van Kampen diagram for (w, w'), one gets an $\mathcal{R}$-derivation from w to w' by starting from w and by reading the labels of a sequence of paths obtained by visiting one after the other the tiles composing $\mathcal{K}$.

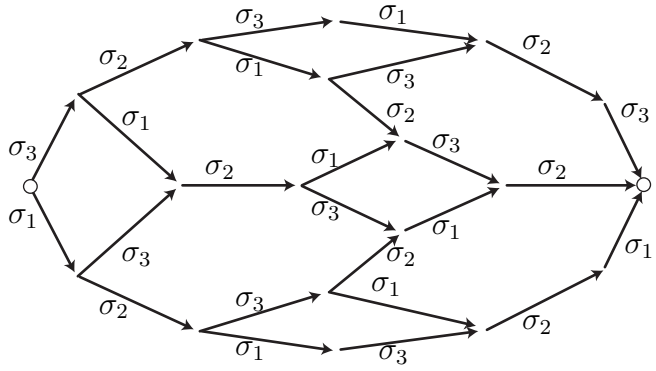


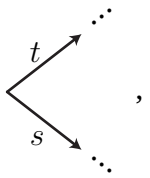
Figure 3: Van Kampen diagram associated to the derivation (8).

WORD REVERSING: THE PRINCIPLE

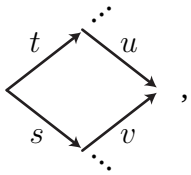
It seems that word reversing was introduced by P. Dehornoy in [11] with the intention of studying a monoid linked to self-distributivity [13]. The word reversing technique independently appears in K. Tatsuoka's work [26] and, in a slightly different—but essentially

the same—manner in R. Corran's [10], as well as in [19] by S. Hermiller et J. Meier. The method was then studied in a more systematic way in [12], for braid groups, followed by [14] and [16] in more general settings.

Word reversing is a strategy that, when it succeeds, provides $\mathcal{R}$-derivations or, equivalently, van Kampen diagrams. Starting from two words w, w' in $\mathcal{S}^*$, this strategy aims at building an $\mathcal{R}$-derivation from w to w' by considering at each step the first disagreement between the words of the derivation that is being built or, equivalently, the leftmost open pattern in the van Kampen diagram that is being built. Such a pattern has the general form



where s and t are two letters of $\mathcal{S}$, and the strategy of word reversing is to complete such a pattern with words u, v such that $sv = tu$ is one of the relations of $\mathcal{R}$:



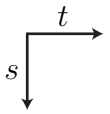
and to iterate the construction. Thus, word reversing merely tries to build a van Kampen diagram starting from the left. We see for instance that we can get the diagram of Figure 3 in such a way.

So far, it is not obvious whether word reversing should succeed, in the sense that, even if we start with two $\mathcal{R}$-equivalent words w, w', hence such that there exists a van Kampen diagram for (w, w'), there is no reason why the strategy of word reversing should provide such a diagram: this is possible that word reversing stop prematurely (no relation $s... = t...$ is available to pursue the procedure) or, on the contrary that it never stop. Also, note that the strategy of reversing provides an actual algorithm only if the considered presentation has the property that, for every pair of letters s, t, there exists at most one relation of the type $s... = t....$

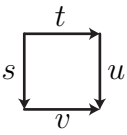
WORD REVERSING: FORMALIZATION

To describe precisely word reversing, it is convenient to draw the associated van Kampen diagrams in a slightly different way: we ask that the diagrams be drawn on a rectangular grid such that the edges only be vertical and down-oriented or horizontal and right-oriented.

Hence the basic reversing step illustrated before now looks like

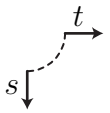


completed in

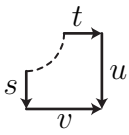


for $sv = tu$ in $\mathcal{R}$.

So as to ensure this convention (which will play a mathematical—as well as notational—role in chapters 4 and 5), we introduce a third kind of edges, labeled by the empty word ε, linking vertices that must be identified. In practice, these ε-edges will be drawn as dotted arcs, and the general representation of a basic reversing step now looks like



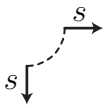
completed in



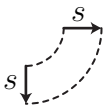
for $sv = tu$ in $\mathcal{R}$,

and, in the case of identical letters, like

(*)



completed in



,

which agrees with the general case provided we take $s = s$ to be a default relation.

With these rules, we get a *reversing diagram*, see Figure 4. The reversing diagram of Figure 4 is not a van Kampen diagram, but it becomes one by contracting the ε-edges on one point.

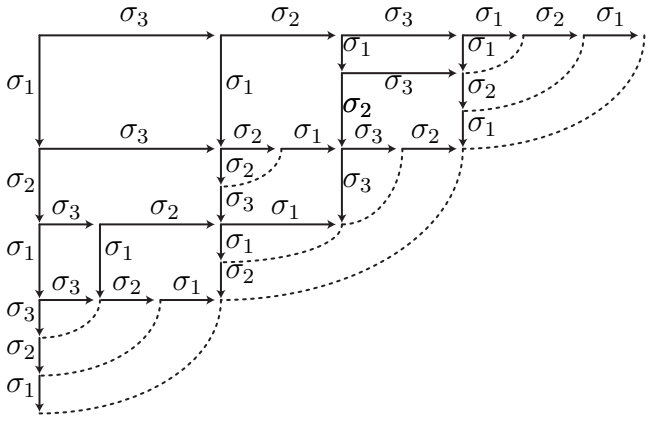


Figure 4: Reversing diagram corresponding to the van Kampen diagram of Figure 3: the edges are either vertical, and oriented downward, or horizontal, and oriented rightward; when contracting the dotted edges to a point, we get the van Kampen diagram of Figure 3.

It is then easy to translate word reversing in purely syntactic terms. To this end, we introduce a copy of the alphabet $\mathcal{S}$, that we denote $\mathcal{S}^{-1}$, containing a letter s^{-1} for each letter s of $\mathcal{S}$, and we code a path in a reversing diagram with the sequence of labels of the edges belonging to this path, according to the convention that an edge labeled s crossed contrary to its orientations contributes s^{-1}.

It follows that, by listing all the paths starting at the bottom left corner and reaching the top right corner—by going either upward or rightward at each step—that are successively obtained while constructing a reversing diagram made of N elementary steps, we get $N+1$ words $w_0, ..., w_N$ on the alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$; the first word is $w^{-1}w'$ and the last is ε. Each elementary step amounts to replacing a subword of the type $s^{-1}t$ with a word vu^{-1} where $sv = tu$ is a relation of $\mathcal{R}$, including the case where $s^{-1}s$ is replaced by the empty word, which corresponds to the implicit relation $s = s$. We see that this basic step consists in replacing a pattern whose signs are $-+$ by a new one with signs $+-$, which explains the denomination "reversing".

With this setting, *i.e.*, as soon as $(\mathcal{S}, \mathcal{R})$ is a semigroup presentation, one can introduce a rewriting rule $\curvearrowright_{\mathcal{R}}$ on the words of $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ by putting that $w \curvearrowright^1_{\mathcal{R}} w'$ holds if one gets w' from w by replacing a subword of the form $s^{-1}t$ with vu^{-1} such that $sv = tu$ is a relation of $\mathcal{R}$, and by defining $\curvearrowright_{\mathcal{R}}$ to be the reflexive–transitive closure of $\curvearrowright^1_{\mathcal{R}}$.

KNOWN RESULTS

A presentation $(\mathcal{S}, \mathcal{R})$ is *complete* (with respect to reversing) if the reversing strategy succeeds as soon as it is possible to, *i.e.*, if for every pair of $\mathcal{R}$-equivalent words w, w', reversing provides a van Kampen diagram for (w, w') or, reformulated in terms of words, if the word $w^{-1}w'$ of $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ reverses to the empty word.

The main result of [12] and (in a more general framework) of [16] states that there exists an effective criterion to recognize whether a presentation is complete. Applying this criterion, we deduce for instance that the Artin presentation of braid monoids aforementioned is complete and, from there, we get, using reversing an algorithmically efficient solution to the word problem of the monoid B_n^+. One can also employ reversing to prove properties of the monoid $\langle \mathcal{S}; \mathcal{R} \rangle^+$ or of the group $\langle \mathcal{S}; \mathcal{R} \rangle$, typically to establish that $\langle \mathcal{S}; \mathcal{R} \rangle^+$ is a Garside monoid.

THE RESULTS OF THIS WORK

In this work, we first investigate properties of word reversing of various presentations and, in a second time, we concentrate on the Artin presentations of braid monoids. We describe below the main new results.

COMPARISON WITH GRÖBNER–SHIRSHOV BASES

The results of [16] give more than a criterion allowing—in good cases—to detect whether a presentation is complete with respect to reversing. Actually, when the criterion is not fulfilled, *i.e.* when the initial presentation $(\mathcal{S}, \mathcal{R})$ is not complete, the criterion computes a new relation $u = v$, consequence of the other relations of $\mathcal{R}$, and which, when added to $\mathcal{R}$, removes the obstruction to the fulfillment of the criterion. We can then apply the criterion to the presentation $(\mathcal{S}, \mathcal{R}')$, where we denote by $\mathcal{R}'$ the set $\mathcal{R} \cup \{u{=}v\}$, whose associated monoid is still $\langle \mathcal{S}; \mathcal{R} \rangle^+$. This procedure can either stop, *i.e.* we obtained a complete presentation, or carry on. Either way, this is a *completion* process, which, starting from an incomplete presentation, leads in finitely or infinitely many steps to a complete presentation.

Formally, this completion procedure is analogous to the construction of a Gröbner-Shirshov basis. At first introduced by Buchberger in the setting of commutative algebra to study ideals in algebras, the Gröbner bases techniques were generalized to wider frameworks such as semigroups and groups by Shirshov and its successors [5, 18, 22, 24]. Similarly to reversing, building a Gröbner-Shirshov basis consists, starting from a presentation $(\mathcal{S}, \mathcal{R})$, in adding (redundant) relations, consequences of those in $\mathcal{R}$, until some completion criterion be satisfied.

The starting point of our work was the observation that, on certain simple presentations, the completions with respect to reversing and Gröbner-Shirshov bases were the same, making the comparison of the two methods natural and even allowing to conjecture that this coincidence behaviour be identical for all— or at least large families of—presentations.

We totally refute this conjecture: the two types of completion, namely the completion with respect to reversing, called *R-completion* below, and the Gröbner-Shirshov completion, called *G-completion* below, do not agree in general. The result that we prove is as follows (Proposition II.4.1):

> **Proposition :** *Each of the following situations exists: there exist semigroup presentations $(\mathcal{S}, \mathcal{R})$ such that*
> (i) *the R-completion and the G-completion are the same,*
> (ii) *the R-completion is a proper subset of the G-completion,*
> (iii) *the G-completion is a proper subset the R-completion,*
> (iv) *the R-completion and the G-completion are not comparable with respect to inclusion.*

We prove this result by exhibiting examples for each of the four types—actually, families of examples for which one proves uniform behaviours. Moreover, the divergence results may be refined to take into account some other properties such as the possible finiteness of the completion. In every case, we conclude to unrelated behaviours in general.

The results of this part are to appear in *European-Asian Journal of Mathematics* [2].

ITERATED REVERSING

Let $(\mathcal{S},\mathcal{R})$ be a semigroup presentation. For w,w' in $(\mathcal{S}\cup\mathcal{S}^{-1})^*$, we declare that $w \curvearrowright_{\mathcal{R}}^{\boxed{2}} w'$ holds if there exists two words u,v in $\mathcal{S}^*$ verifying

$$w \curvearrowright_{\mathcal{R}} vu^{-1} \quad \text{and} \quad u^{-1}v \curvearrowright_{\mathcal{R}} w'.$$

Similarly, we declare that $w \curvearrowright_{\mathcal{R}}^{\boxed{k}} w'$ holds if, for $1 \leq i < k$, there exists words u_i, v_i in $\mathcal{S}^*$ satisfying

$$w \curvearrowright_{\mathcal{R}} v_1u_1^{-1} \quad \text{and} \quad u_1^{-1}v_1 \curvearrowright_{\mathcal{R}} v_2u_2^{-1} \quad \text{and ... and} \quad u_{k-1}^{-1}v_{k-1} \curvearrowright_{\mathcal{R}} w'.$$

In other words, we alternate reversing and permutation of the numerator and the denominator. The relation $\curvearrowright_{\mathcal{R}}^{\boxed{k}}$ shall be called *iterated reversing of degree* k, and we shall say that the word problem of the monoid $\langle\mathcal{S};\mathcal{R}\rangle^+$ (*resp.* of the group $\langle\mathcal{S};\mathcal{R}\rangle$) is solvable by iterated reversing of degree k if, for all words w,w' of $\mathcal{S}^*$ (*resp.* for every word w of $(\mathcal{S}\cup\mathcal{S}^{-1})^*$), the words w and w' represent the same element in $\langle\mathcal{S};\mathcal{R}\rangle^+$ (*resp.* w represents the identity element in $\langle\mathcal{S};\mathcal{R}\rangle$) if and only if $w^{-1}w' \curvearrowright_{\mathcal{R}}^{\boxed{k}} \varepsilon$ holds (*resp.* if and only if $w \curvearrowright_{\mathcal{R}}^{\boxed{k}} \varepsilon$ holds).

In case of a R-complete presentation $(\mathcal{S},\mathcal{R})$ such that the monoid $\langle\mathcal{S};\mathcal{R}\rangle^+$ admits right cancellation, and there exists at most one relation $s\ldots = t\ldots$ in $\mathcal{R}$ for every pair of letters in $\mathcal{S}$, and there exists a finite set of words $\widehat{\mathcal{S}}$ in $\mathcal{S}^*$ closed under reversing, *i.e.*, for all u,v in $\widehat{\mathcal{S}}$, there exists u',v' in $\widehat{\mathcal{S}}$ verifying $u^{-1}v \curvearrowright_{\mathcal{R}} v'u'^{-1}$—all these hypotheses being satisfied by the standard presentations of braid monoids, and more generally, by the canonical presentations of Garside monoids—then the word problem of the monoid $\langle\mathcal{S};\mathcal{R}\rangle^+$ is solvable in quadratic time by iterated reversing of degree 1 (*i.e.*, by mere reversing), whereas the word problem of the group $\langle\mathcal{S};\mathcal{R}\rangle$ is solvable, in quadratic time as well, by iterated reversing of degree 2.

The question was to understand what behaviours should be expected when dealing with an R-incomplete presentation or with a group whose Dehn function is more than quadratic. In particular, we study the discrete version of Heisenberg group, associated to the presentation

$$(a,b,c \mid ab = bac, ac = ca, bc = cb). \tag{9}$$

The result, quite surprising, is that, though the presentation (9) be R-incomplete, one obtains again solutions to the word problems of the associated group and monoid by means of iterated reversing, with the minor drawback of increasing by one unit the degree of the iterated reversing in comparison to previous known results (Proposition III.2.5):

> **Proposition :** *The word problem of Heisenberg monoid is solvable by iterated reversing of degree* 2*. The word problem of Heisenberg group is solvable by iterated reversing of degree* 3*.*

Heisenberg presentation is not the sole presentation featuring this property and we construct other presentations where the same behaviour is observed.

COMBINATORIAL DISTANCE BETWEEN BRAID WORDS / REDUCED EXPRESSIONS OF PERMUTATIONS

In the particular case of the Artin presentation of braid monoids B_n^+ , we know that (non iterated) reversing solves the word problem of the monoid, and, for each value of the index n, we also have an upper bound in ℓ^2 on the number of elementary steps required to reverse words of length ℓ. However, little was known when the index n was allowed to vary, *i.e.*, when we consider reversing of words on the infinite alphabet $\{\sigma_1, \sigma_2, ...\}$.

For two words w, w' on the alphabet $\{\sigma_1, \sigma_2, ...\}$, we can associate the two following integers:

– the number of elementary steps (excl. the type $(*)$ steps) required to reverse the word $w^{-1}w'$, called *reversing distance* between w and w' and noted $\mathrm{dist}_{\curvearrowright}(w, w')$,

– and, when w and w' are equivalent with respect to braid relations, what we shall note $w \equiv w'$, the *combinatorial distance* between w and w', defined to be the minimal number of braid relations needed to transform w into w' and noted $\mathrm{dist}(w, w')$.

Since reversing is a strategy to build van Kampen diagrams (hence a derivation), we have the inequality

$$\mathrm{dist}(w, w') \leq \mathrm{dist}_{\curvearrowright}(w, w') \tag{10}$$

for every couple of braid words (w, w') satisfying $w \equiv w'$. This study aims at establishing lower and upper bounds for the numbers $\mathrm{dist}(w, w')$ and $\mathrm{dist}_{\curvearrowright}(w, w')$.

Amongst braid words, the ones coding braid diagrams in which two strands cross at most once are called *simple*. Simple words play a key role in our work. The fact is that these particular words can be seen as reduced decompositions of a permutation in terms of transpositions. The classical Exchange Lemma for Coxeter groups states that two reduced decompositions of a same permutation are transformable in each other by applying the braid relations (6) and (7), from what we deduce that, for all simple braid words, the number $\mathrm{dist}(w, w')$ is also the combinatorial distance between the associated reduced decompositions.

In this setting, we prove (Corollary IV.1.19):

> **Proposition :** *For every n, there exist simple braid words w, w' on the letters $\sigma_1, ..., \sigma_{n-1}$ satisfying* $\mathrm{dist}(w, w') \geq n^4/8$.

Hence, in terms of permutations,

> **Corollary :** *For every n, there exist reduced decompositions w, w' of a same permutation of $\{1, ..., n\}$ verifying* $\mathrm{dist}(w, w') \geq n^4/8$.

These results are optimal in the sense that there exists an upper bound of the same order.

OPTIMALITY OF REVERSING

It is easy to show that the inequality (10) might be strict: for instance, if w and w' are the aforementioned braid words $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ and $\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$, then one reads on the Figures 3 or 4 that the reversing distance $\mathrm{dist}_{\curvearrowright}(w, w')$ equals 8, despite the existence of a derivation of length 6 from w to w', which is the shortest, hence implying that the combinatorial distance $\mathrm{dist}(w, w')$ equals 6.

As a consequence, reversing is not always optimal, and thus arises the question of identifying the cases when it is, *i.e.*, the cases when (10) is an equality. More generally, whether the initial words w, w' are equivalent or not, *i.e.*, whether reversing the word $w^{-1}w'$ ends with the empty word or not, we wish to be able to recognize when a reversing diagram is optimal, in the sense that the van Kampen diagram obtained by contracting to a point every ε-edge realizes the combinatorial distance between the words labeling the border (Proposition IV.4.5).

Proposition : *A reversing diagram with no type $(*)$ tile is optimal.*

The proof of this result relies on the notion of *separatrices*, which are curves transverse to the edges of a van Kampen diagram coming from the duality name/position in the permutations. The crux is that a van Kampen diagram in which any two separatrices cross a most once is necessarily optimal, and that two separatrices can only cross twice or more if there are type $(*)$ tiles in the diagram. The above criterion is all the more interesting that it stays valid for slightly altered diagrams, in which specific pairs of tiles are combined into one, thus eliminating several type $(*)$ tiles.

COMPLEXITY OF BRAID WORD REVERSING

For words w, w' on the alphabet $\{\sigma_1, \sigma_2, \ldots\}$, we define the 2-complexity $\mathrm{L}_2(w^{-1}w')$ of the word $w^{-1}w'$ to be the number of tiles (incl. type $(*)$ tiles) in the reversing diagram of $w^{-1}w'$. In the sequel, we bound the 2-complexity. For the lower bounds, we show (Proposition V.2.1):

> **Proposition :** *For every ℓ, there exist simple braid words w, w' of length ℓ verifying $\mathrm{L}_2(w^{-1}w') \geq \ell^4/8$.*

This result is an improvement of the best lower bound known so far [12] and is not a consequence of the Corollary IV.1.19 establishing a quartic lower bound for the combinatorial distance: the words used to prove this corollary are of length $n^2/2 + O(1)$, hence a transposition of this result by means of the inequality (10) would yield a lower bound in $O(\ell^2)$ for the reversing complexity $\mathrm{L}_2(w^{-1}w')$, and not in $O(\ell^4)$ as stated above.

Establishing upper bounds appears much trickier. We conjecture the existence of an upper bound in $O(\ell^4)$ for $\mathrm{L}_2(w^{-1}w')$ when w and w' are braid words of length at most ℓ, but we have no proof of it so far. However, we prove partial results.

First, we improve the only upper bound known so far, established in [17], by introducing a refinement of reversing, the *pacific reversing*, whose execution requires more steps than classic reversing, this holding for every initial word. By computing an upper bound for pacific reversing, we prove (Proposition V.4.11):

> **Proposition :** *For all braid words w, w' of length ℓ, we have the upper bound $\mathrm{L}_2(w^{-1}w') \leq 3^{4\ell}\ell^2/4$.*

Then, we use a method involving separatrices to analyze the reversing diagrams and obtain upper bounds on the number of tiles that they can possibly be made of. This analysis leads to the introduction of *repeaters*, specific subdiagrams, whose presence in a reversing diagram is equivalent to the crossing more than once of separatrices, *i.e.*, by previous arguments, equivalent to having a non optimal reversing diagram. We obtain that repeaters are characterized by the following data: a type (amongst three) and a quadruple of parameters (taken in a finite set depending on the number of strands involved in the initial braid word).

The more a reversing sequence is long, the more the separatrices of the associated diagram have to cross. We observe, however, that diagrams featuring separatrices crossing more thant twice do not occur. This leads us to:

> **Conjecture :** *A reversing diagram contains at most one repeater for each type et each value of the parameters.*

Assuming this hypothesis, we prove (Proposition V.6.13):

> **Proposition :** *If the above conjecture is true, then there is constant C such that, for all braid words w, w' of length ℓ, we have $\mathrm{L}_2(w^{-1}w') \leq \mathrm{C}\,\ell^6$.*

This result describes in a more accurate way what experiments show: the better upper bound known so far is exponential in the length of the initial word, whereas no family of complexity more than quartic could be exhibited. An analogous result remains valid under the weaker assumption that the number of occurrences of each type of repeaters is bounded above by $O(\ell)$.

The results of the last three parts are submitted for publication [3].

ORGANIZATION OF THE TEXT

The text of the thesis follows the order of the results described above. The first part is devoted to the reversing method in general. Chapter I gives basic definitions and recalls several known results. Chapter II is devoted to the comparison between the completions associated to reversing and Gröbner-Shirshov bases. In Chapter III, we concentrate on iterated reversing and, in particular, to Heisenberg monoid.

The second part deals more specifically with braid words reversing. In Chapter IV, we compare reversing distance and combinatorial distance. Finally, in Chapter V, we bound reversing complexity of braid words.

Partie A

Retournement : cas général

CHAPITRE I

RETOURNEMENT

Ce chapitre présente les définitions et résultats de base de ce travail de thèse, en particulier ceux concernant la transformation syntaxique appelée retournement.

Une manière privilégiée d'étudier une structure algébrique telle qu'un groupe ou un monoïde est de s'en donner une présentation, c'est-à-dire une liste de générateurs et des relations entre eux. Par l'étude de cette présentation, on accède — dans les bons cas — à des informations sur la structure algébrique elle-même comme la finitude du nombre d'éléments, la simplification pour un monoïde, etc. Étudier une présentation implique de posséder un outil pour manipuler (efficacement) des mots en les générateurs de la présentation. Le retournement de mot est un tel outil : retourner un mot consiste en une transformation de ce mot selon des règles déterminées par les relations de la présentation qu'on étudie.

Une des propriétés du retournement est que, moyennant une hypothèse combinatoire de complétude que doit vérifier la présentation, il fournit une semi-solution au problème du mot, c'est-à-dire que si deux mots sont équivalents, le retournement le prouve en un temps fini mais que, dans le cas contraire, le retournement peut ne pas terminer. De plus, si la présentation ne vérifie pas l'hypothèse de complétude, on peut y remédier en complétant la liste des relations de la présentation par des relations déduites de celles initialement présentes dans la présentation.

L'opération combinatoire de retournement de mot paraît avoir été introduite dans [11] avant d'être étudiée d'abord pour un type de présentation bien particulier, dit complémenté, dans [12], [14], [15] puis dans un cadre plus général [16], [17].

Après les sections 1 et 2 dans laquelle nous définissons le retournement et les notions attachées, nous présentons la notion de complétude en toute généralité dans la section 3. À la section 4, nous introduisons une hypothèse combinatoire caractéristique de la complétude dans certains cas. Cette hypothèse est appelée la condition du cube. Nous donnons un moyen de réparer un défaut de complétude à la section 5 en décrivant un algorithme ajoutant des relations à une présentation incomplète jusqu'à former une nouvelle présentation satisfaisant la condition du cube. Finalement, nous donnons deux applications du retourne-

ment à la section 6 : la première est un critère pour déterminer si le monoïde associé à une présentation admet la simplification, la seconde est un moyen de calculer le ppcm de deux éléments dans certains monoïdes.

1 LE RETOURNEMENT DE MOT

1.1 PRÉSENTATION DE MONOÏDE

On appelle *mot* sur un ensemble $\mathcal{S}$, qu'on nomme *alphabet*, une suite finie d'éléments de $\mathcal{S}$, c'est- à-dire une application d'un intervalle $[\![1, \ell]\!]$ de $\mathbb{N}$ dans $\mathcal{S}$. On dit dans ce cas que le mot est de *longueur* ℓ. On note $|u|$ la longueur d'un mot u. Les éléments de $\mathcal{S}$, et par extension les éléments d'un mot, sont appelés *lettres*. La *concaténation* de deux mots u et v est le mot de longueur $|u| + |v|$ dont les $|u|$ premières lettres sont celles de u et les $|v|$ dernières celles de v. Si $\mathcal{S}$ est un ensemble non vide, on note $\mathcal{S}^*$ l'ensemble des mots écrits sur l'alphabet $\mathcal{S}$. L'ensemble $\mathcal{S}^*$ muni de la concaténation est un monoïde libre de base $\mathcal{S}$. On note ε l'unique mot de longueur 0 et on l'appelle le *mot vide*. On appelle *sous-mot* d'un mot u égal à $u_1 \dots u_\ell$, où $u_1, \dots, u_\ell$ sont des lettres, toute suite de lettres consécutives de u. Le mot vide ε est donc un sous-mot de u, tout comme u_1 et $u_3 \dots u_{\ell-1}$.

Un couple d'ensembles $(\mathcal{S}; \mathcal{R})$ est appelé *présentation de monoïde* si $\mathcal{R}$ est un ensemble de paires de mots non vides sur $\mathcal{S}$. Si $(\mathcal{S}; \mathcal{R})$ est une présentation de monoïde, un élément de $\mathcal{S}$ (resp. $\mathcal{R}$) est appelé *générateur* (resp. *relation*). On notera souvent $u = v$ ou (u, v) la relation $\{u, v\}$. Dans la suite, on travaillera avec des monoïdes plutôt qu'avec des semi-groupes ; on note $\langle \mathcal{S};\ \mathcal{R}\rangle^+$ le monoïde $\mathcal{S}^*/\equiv_{\mathcal{R}}$, où $\equiv_{\mathcal{R}}$ est la plus petite congruence sur $\mathcal{S}^*$ contenant $\mathcal{R}$, c'est-à-dire la plus petite relation d'équivalence contenant $\mathcal{R}$ et compatible avec la loi du monoïde. On définit la relation $\equiv_{\mathcal{R}}^{(1)}$ par : « on a $w \equiv_{\mathcal{R}}^{(1)} w'$ si et seulement si on peut passer de w à w' en n'utilisant qu'une seule relation de $\mathcal{R}$. » Autrement dit, $\equiv_{\mathcal{R}}$ est la clôture transitive de $\equiv_{\mathcal{R}}^{(1)}$.

Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde. Pour toute lettre s de $\mathcal{S}$, on introduit une copie disjointe s^{-1} de s et on note $\mathcal{S}^{-1}$ l'ensemble des éléments s^{-1} et $\langle \mathcal{S}; \mathcal{R}\rangle$ le groupe $(\mathcal{S} \cup \mathcal{S}^{-1})/\equiv_{\mathcal{R}}^{\pm}$, où $\equiv_{\mathcal{R}}^{\pm}$ est la plus petite congruence sur $(\mathcal{S} \cup \mathcal{S}^{-1})$ contenant $\mathcal{R}$ (donc $\equiv_{\mathcal{R}}$ aussi) et toutes les paires $\{ss^{-1}, \varepsilon\}$, $\{s^{-1}s, \varepsilon\}$, c'est-à-dire toutes les relations $ss^{-1} = s^{-1}s = \varepsilon$, pour s dans $\mathcal{S}$. Une lettre de $\mathcal{S}$ (resp. $\mathcal{S}^{-1}$) est dit *positive* (resp. *négative*). Un mot est *positif* (resp. *négatif*) s'il n'est composé que de lettres *positives* (resp. *négatives*). Un mot $s_1 \dots s_m t_1 \dots t_p$, notons-le w, avec les s_i positives et les t_j négatives est dit *positif-négatif*. De façon identique, on dit que w est *négatif-positif* si les t_i sont positives et les s_j négatives. Si u est le mot positif $s_1 \dots s_m$, on définit u^{-1} comme étant le mot négatif $s_m^{-1} \dots s_1^{-1}$.

1.2 RETOURNEMENT ET SUITES DE RETOURNEMENT

Définition 1.1 (retournement [1])**.** À toute présentation de monoïde $(\mathcal{S};\mathcal{R})$, on associe la relation binaire $\curvearrowright_{\mathcal{R}}^{(1)}$ sur $\mathcal{S}\cup\mathcal{S}^{-1}$. Soient les mots w et w' de $\mathcal{S}\cup\mathcal{S}^{-1}$. On dit qu'on a $w \curvearrowright_{\mathcal{R}}^{(1)} w'$ — et on dit qu'on *retourne* w en w' en une étape — si on peut obtenir w' depuis w

- soit en supprimant un sous-mot $s^{-1}s$ avec $s\in\mathcal{S}$,
- soit en remplaçant un sous-mot $s^{-1}t$, avec s, t des lettres positives, par un mot vu^{-1} tel que $su=tv$ soit une relation de $\mathcal{R}$.

Il est clair que le retournement d'un mot dépend de la présentation considérée et que la mention de l'ensemble des relations devrait, en toute rigueur, apparaître sur le symbole du retournement. Toutefois, quand la présentation sera claire d'après le contexte, on notera $\curvearrowright^{(1)}$ au lieu de $\curvearrowright_{\mathcal{R}}^{(1)}$ pour le retournement associé à la présentation $(\mathcal{S};\mathcal{R})$.

Afin d'améliorer la lisibilité des exemples suivants, on remplacera souvent dans un mot les lettres négatives par la lettre capitale correspondante. Ainsi on notera $\mathtt{A}$ pour $\mathtt{a}^{-1}$ ou $\mathtt{B}$ pour $\mathtt{b}^{-1}$. De plus, lors du retournement d'un mot w en un mot w', la présence de crochets autour d'un sous-mot de w signifie que c'est le retournement de ce sous- mot qui mène à w'.

Exemple 1.2. Prenons la présentation d'Artin standard [1] $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{aba})$ du monoïde de tresses B_3^+. Retournons maintenant le mot $\mathtt{Ab}^2$, c'est-à-dire $\mathtt{a}^{-1}\mathtt{b}^2$:

$$\mathtt{Ab}^2=[\mathtt{Ab}]\mathtt{b}\curvearrowright^{(1)}\ \mathtt{baB}[\mathtt{Ab}]\curvearrowright^{(1)}\ \mathtt{ba}[\mathtt{Bb}]\mathtt{aBA}\curvearrowright^{(1)}\ \mathtt{ba}\varepsilon\mathtt{aBA}=\mathtt{ba}^2\mathtt{BA}.$$

Remarquons que le retournement associé à la présentation $(\mathcal{S};\mathcal{R})$ est un système de réécriture des mots sur $\mathcal{S}$. Les règles de réécriture pour la présentation de l'exemple précédent sont $\mathtt{Ab}\to\mathtt{baBA}$, $\mathtt{Ba}\to\mathtt{abAB}$, $\mathtt{Bb}\to\varepsilon$, $\mathtt{Aa}\to\varepsilon$ ainsi que toutes les règles évidentes faisant intervenir le mot vide ε. Naturellement, des questions de convergence du procédé de réécriture se posent. On donnera quelques résultats concernant ce sujet à la section 2.

Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. On dit de $w_0,w_1,\ldots$, une suite (finie ou infinie) de mots, que c'est une *suite de retournements* dès qu'on a $w_i\curvearrowright_{\mathcal{R}}^{(1)}w_{i+1}$ pour tout i. On écrit $w\curvearrowright_{\mathcal{R}}^{(k)}w'$ s'il existe une suite de retournements de longueur k de w à w' ; on dit alors que w est *retournable* en w' en k étapes ou, simplement, que w *se retourne* en w'. Un mot est *terminal* (ou *final*) s'il n'est pas retournable. Une suite de retournements est *maximale* si son dernier mot est final. On note $\curvearrowright_{\mathcal{R}}$ la clôture transitive de $\curvearrowright_{\mathcal{R}}^{(1)}$. Ceci revient à dire que si on a $w\curvearrowright_{\mathcal{R}}w'$, il existe un entier naturel k pour lequel on a $w\curvearrowright_{\mathcal{R}}^{(k)}w'$. Dans l'exemple 1.2, on a $\mathtt{Ab}^2\curvearrowright_{\mathcal{R}}^{(3)}\mathtt{ba}^2\mathtt{BA}$, et donc $\mathtt{Ab}^2\curvearrowright_{\mathcal{R}}\mathtt{ba}^2\mathtt{BA}$.

1. En anglais, *reversing.*

1.3 DIAGRAMMES DE RETOURNEMENT

Le retournement de mot est fastidieux et peu lisible lorsqu'on manipule les mots comme dans l'exemple 1.2, surtout s'ils sont longs. On introduit dans cette section un outil qui pallie ce problème : à toute suite de retournements, on associe un graphe orienté qu'on nomme *diagramme de retournement*. Un diagramme de retournement est (essentiellement) un diagramme de Van Kampen — voir définition précise au chapitre IV — d'un type particulier. Pour l'instant cependant, on se contente de définir les diagrammes de retournement de façon directe.

Chacune des arêtes du graphe est étiquetée par un élément de $\mathcal{S}$. Il y a trois types d'arêtes : les arêtes horizontales, orientées vers la droite, les arêtes verticales, orientées vers le bas, et les arêtes ε, ou ε-arêtes, sans orientation. On associe à la suite de retournements $w_0, \dots, w_n$ le diagramme de retournement $\Gamma(w_0, \dots, w_n)$, défini par récurrence sur n, c'est-à-dire sur le nombre d'étapes de retournement, tel qu'il possède la propriété que le mot formé par les étiquettes du bord gauche est w_0 et que le mot formé par les étiquettes du bord droit est w_n — la lecture d'un mot sur le graphe se fait en respectant la convention que toute arête traversée à l'endroit (resp. à l'envers) contribue positivement (resp. négativement) (voir figure 3).

Pour $n = 0$, le diagramme de retournement $\Gamma(w_0)$ de la suite réduite au mot w_0 est construit comme suit. On se donne un point de départ et si la première lettre de w_0 est positive (resp. négative) on trace une arête horizontale (resp. verticale) d'origine (resp. de but) le point de départ. Pour chaque lettre suivante de w_0, on attache une nouvelle arête à l'extrémité libre de la dernière arête posée en respectant toujours la condition que si la lettre lue est positive (resp. négative), on attache une arête horizontale (resp. verticale). Chacune de ces arêtes est étiquetée avec la lettre à laquelle elle est associée. Sur l'exemple de la figure 1, on lit que la première lettre du mot est σ_1^{-1}, la deuxième σ_2, la troisième σ_2^{-1}, puis σ_3^{-1} et enfin σ_1.

Supposons $n \geq 1$. Le mot w_n est obtenu à partir de w_{n-1} en supprimant un motif $s^{-1}s$, pour s dans $\mathcal{S}$, ou en remplaçant un motif $s^{-1}t$ par uv^{-1}, avec s, t dans $\mathcal{S}$ et u, v dans $\mathcal{S}^*$ tels que $su = tv$ est une relation de $\mathcal{R}$. Dans les deux cas, d'après les conventions de signe adoptées ci-dessus, ce sous-mot négatif-positif dans le mot w_{n-1} correspond dans le diagramme $\Gamma(w_0, \dots, w_{n-1})$ à une flèche horizontale et une flèche verticale divergeant depuis un même point ou à un motif comprenant un ε comme illustré dans les diagrammes de la figure 2. Pour passer de $\Gamma(w_0, \dots, w_{n-1})$ à $\Gamma(w_0, \dots, w_n)$, on complète la diagramme de la façon adéquate parmi les différentes manières de compléter un « motif ouvert » illustrées à la figure 2.

Exemple 1.3. Posons $w_0 = \sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3^{-1}\sigma_2$. On considère le retournement associé à la présentation de monoïde

$$(\sigma_1, \sigma_2, \sigma_3; \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2, \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3, \sigma_1\sigma_3 = \sigma_3\sigma_1).$$

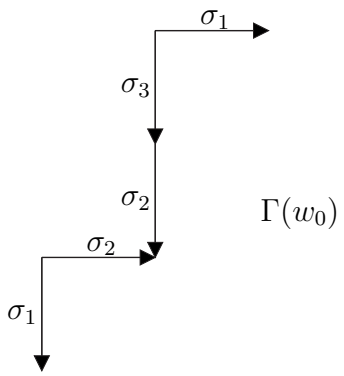


FIGURE 1 – À la suite de retournements réduite au seul mot $w_0 = \sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3^{-1}\sigma_2$, on associe le diagramme de retournement $\Gamma(w_0)$. En lisant les lettres le long des arêtes depuis le coin inférieur gauche jusqu'au coin supérieur droit, avec la convention qu'une flèche parcourue dans le sens de son orientation (resp. à l'envers) contribue au mot positivement (resp. négativement), on retrouve le mot w_0.

La figure 3 illustre les différentes étapes de la construction du diagramme associé à la suite — unique — de retournements issue de w_0 :

$$\begin{aligned}
\sigma_1^{-1}\sigma_2\sigma_2^{-1}[\sigma_3^{-1}\sigma_2] &\curvearrowright \sigma_1^{-1}\sigma_2[\sigma_2^{-1}\sigma_2]\sigma_3\sigma_2^{-1}\sigma_3^{-1} \\
&\curvearrowright [\sigma_1^{-1}\sigma_2]\sigma_3\sigma_2^{-1}\sigma_3^{-1} \\
&\curvearrowright \sigma_2\sigma_1\sigma_2^{-1}[\sigma_1^{-1}\sigma_3]\sigma_2^{-1}\sigma_3^{-1} \\
&\curvearrowright \sigma_2\sigma_1[\sigma_2^{-1}\sigma_3]\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1} \\
&\curvearrowright \sigma_2\sigma_1\sigma_3\sigma_2\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}.
\end{aligned}$$

1.4 PREMIERS RÉSULTATS

Avant de montrer les deux résultats importants de ce paragraphe — la proposition 1.5 et le lemme 1.6 —, on énonce le lemme suivant, dont on omet la preuve en raison de sa technicité et du peu d'éclairage qu'elle apporte sur l'exposition.

Lemme 1.4 ([16, Lem. 1.7])**.** *Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. Soient w un mot sur $\mathcal{S}\cup\mathcal{S}^{-1}$ et u, v des mots positifs satisfaisant $w \curvearrowright_{\mathcal{R}}^{(k)} vu^{-1}$. Alors, pour toute décomposition $w = w_1w_2$, avec $w_1, w_2 \in (\mathcal{S}\cup\mathcal{S}^{-1})^*$, il existe dans $\mathcal{S}^*$ des décompositions $u = u_1u_2$,*

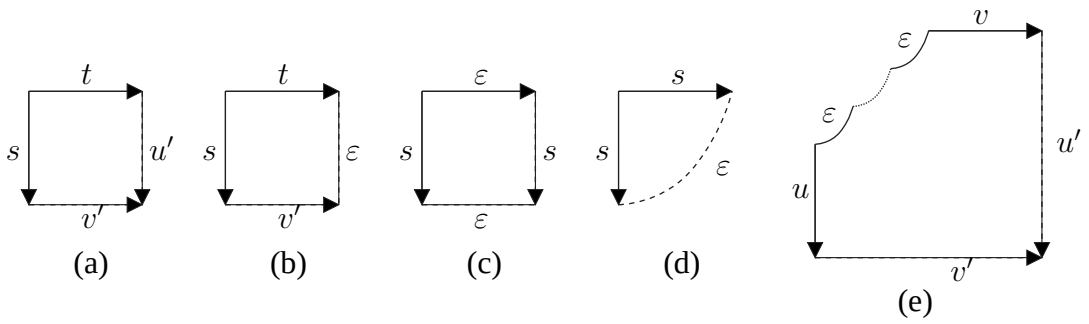


FIGURE 2 – Les motifs (a), (b), (c) et (d) sont les quatre motifs possibles lors de la construction d'un diagramme de retournement — si on exclut le cas où le motif à retourner contient des ε-arêtes. Sur chacun de ces quatre diagrammes, on lit le long du trait plein le motif qu'on retourne et le long du trait tireté le mot retourné. Le cas général est représenté sur le schéma (e) : le motif à retourner peut contenir des ε-arêtes en nombre arbitraire, ici représentées par le trait pointillé. Ainsi, en (a), on lit $u^{-1}v \curvearrowright^{(1)} v'u'^{-1}$. En (b) : $u^{-1}v \curvearrowright^{(1)} v'\varepsilon$. En (c) : $u^{-1}\varepsilon \curvearrowright^{(1)} \varepsilon u'^{-1}$. En (d) : $u^{-1}u \curvearrowright^{(1)} \varepsilon$. En (e) : $u^{-1}v \curvearrowright^{(1)} v'u'^{-1}$.

$v = v_1v_2$ *et* u_0, v_0 *satisfaisant* $w_1 \curvearrowright_{\mathcal{R}}^{(k_1)} v_1u_0^{-1}$, $w_2 \curvearrowright_{\mathcal{R}}^{(k_2)} v_0u_1^{-1}$ *et* $u_0^{-1}v_0 \curvearrowright_{\mathcal{R}}^{(k_0)} v_2u_2^{-1}$ *avec* $k = k_1 + k_2 + k_0$.

Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde. La première proposition qu'on montre est particulièrement importante car elle lie $\curvearrowright_{\mathcal{R}}$ et $\equiv_{\mathcal{R}}$. On montre que bien que les opérations sur les mots semblent se passer au niveau du groupe $\langle \mathcal{S}; \mathcal{R}\rangle$, l'équivalence qu'on obtient se comprend au niveau du monoïde, et ce même si le monoïde $\langle \mathcal{S}; \mathcal{R}\rangle^+$ ne se plonge pas dans le groupe $\langle \mathcal{S}; \mathcal{R}\rangle$.

Proposition 1.5 ([16, Prop. 1.9])**.** *Soit* $(\mathcal{S}; \mathcal{R})$ *une présentation de monoïde. Soient les mots* u, v, u', v' *de* $\mathcal{S}^*$*. Alors* $u^{-1}v \curvearrowright_{\mathcal{R}} v'u'^{-1}$ *implique* $uv' \equiv_{\mathcal{R}} vu'$*.*

Démonstration. On procède par récurrence sur k le nombre d'étapes requises pour retourner $u^{-1}v$ en $v'u'^{-1}$, c'est-à-dire qu'on suppose $u^{-1}v \curvearrowright_{\mathcal{R}}^{(k)} v'u'^{-1}$. Pour $k = 0$, la seule possibilité est que u ou v soit vide, auquel cas on a $u' = u$ ou $v' = v$ et le résultat est vrai. Supposons $k \geq 1$. Dans ce cas, les mots u et v ne peuvent pas être vides. Posons $u = su_0$ et $v = tv_0$, où s, t sont des lettres de $\mathcal{S}$. La première étape dans le retournement de $u^{-1}v$ en $v'u'^{-1}$ concerne forcément le sous-mot $s^{-1}t$, donc il existe une relation $sv_1 = tu_1$ dans $\mathcal{R}$ telle que la suite de retournements se décompose en

$$u^{-1}v = u_0^{-1}s^{-1}tv_0 \curvearrowright_{\mathcal{R}}^{(1)} u_0^{-1}v_1u_1^{-1}v_0 \curvearrowright_{\mathcal{R}}^{(k-1)} v'u'^{-1}.$$

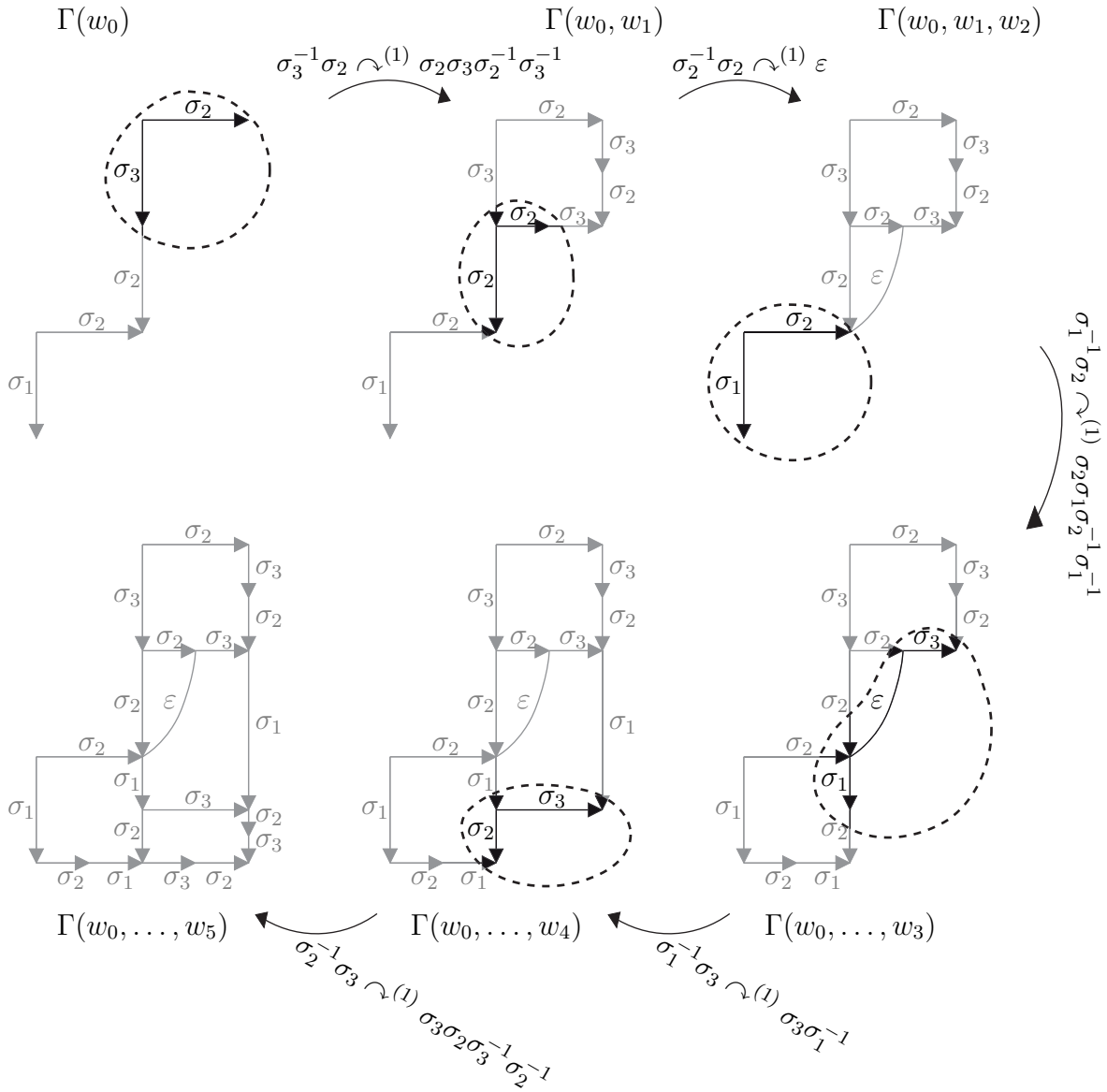


FIGURE 3 – Les diagrammes illustrent les différentes étapes de la suite de retournements w_0, w_1, ... issue du mot w_0 de l'exemple 1.3, à savoir $\sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3^{-1}\sigma_2$. On trouve que la suite est de longueur 6 et on a $w_5 = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}$. À la suite de retournements $w_0, \ldots, w_5$ est associé le diagramme $\Gamma(w_0, \ldots, w_5)$ dont la construction à partir de $\Gamma(w_0)$ est illustrée ici en cinq étapes. Le passage de $\Gamma(w_0, \ldots, w_i)$ à $\Gamma(w_0, \ldots, w_{i+1})$ se fait en complétant un motif ouvert (entouré ici en tireté) grâce aux relations $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$, $\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3$ et $\sigma_1\sigma_3 = \sigma_3\sigma_1$ de la présentation standard d'Artin de B_4^+.

D'après le lemme 1.4, il existe des mots positifs $u_2, v_2, u_3, v_3, u_4, v_4$ et des entiers naturels k_2, k_3, k_4 avec $k_2 + k_3 + k_4 = k - 1$, $u' = u_3u_4$ et $v' = v_2v_4$ tels qu'on ait les relations $u_0^{-1}v_1 \curvearrowright_{\mathcal{R}}^{(k_2)} v_2u_2^{-1}$, $u_1^{-1}v_0 \curvearrowright_{\mathcal{R}}^{(k_3)} v_3u_3^{-1}$ et $u_2^{-1}v_3 \curvearrowright_{\mathcal{R}}^{(k_4)} v_4u_4^{-1}$. Pour i dans $\{2, 3, 4\}$, on a $k_i < k$ et donc on peut utiliser l'hypothèse de récurrence pour obtenir les équivalences $u_0v_2 \equiv_{\mathcal{R}} v_1u_2$, $u_1v_3 \equiv_{\mathcal{R}} v_0u_3$ et $u_2v_4 \equiv_{\mathcal{R}} v_3u_4$, d'où

$$uv' = su_0v_2v_4 \equiv_{\mathcal{R}} sv_1u_2v_4 \equiv_{\mathcal{R}} tu_1u_2v_4 \equiv_{\mathcal{R}} tu_1v_3u_4 \equiv tv_0u_3u_4 = vu',$$

ce qui donne l'équivalence annoncée. □

Une application importante de la proposition précédente est le lemme suivant qui donne un moyen différent de la proposition 1.5 de former des paires de mots équivalents par retournement. On verra plus loin que sur ce lemme repose l'algorithme 5.1 de complétion du retournement.

Lemme 1.6 ([16, Lemma. 1.10])**.** *Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde et soient u, v, w, u', v' des mots sur $\mathcal{S}$ vérifiant $u^{-1}ww^{-1}v \curvearrowright v'u'^{-1}$. Alors on a $uv' \equiv vu'$.*

Démonstration. Par le lemme 1.4, la relation $u^{-1}ww^{-1}v \curvearrowright_{\mathcal{R}} v'u'^{-1}$ implique l'existence de deux décompositions $u' = u'_1u'_2$, $v' = v'_1v'_2$ et de u_0, v_0 satisfaisant $u^{-1}w \curvearrowright_{\mathcal{R}} v'_1u_0^{-1}$, $w^{-1}v \curvearrowright_{\mathcal{R}} v_0u_1'^{-1}$ et $u_0^{-1}v_0 \curvearrowright_{\mathcal{R}} v'_2u_2'^{-1}$. Puis, par la proposition 1.5, on obtient

$$uv' = uv'_1v'_2 \equiv_{\mathcal{R}} wu_0v'_2 \equiv_{\mathcal{R}} wv_0u'_2 \equiv_{\mathcal{R}} vu'_1u'_2 = vu'.$$

□

Jusqu'à présent on a toujours considéré les monoïdes présentés par les présentations de semigroupe. La proposition suivante énonce un résultat concernant le groupe présenté par une présentation de monoïde. On rappelle que si $(\mathcal{S}; \mathcal{R})$ est une présentation de monoïde, le symbole $\equiv_{\mathcal{R}}^{\pm}$ désigne l'équivalence dans le groupe $\langle \mathcal{S}; \mathcal{R} \rangle$ des mots écrits sur $\mathcal{S} \cup \mathcal{S}^{-1}$.

Proposition 1.7 ([16, Lemma. 1.6])**.** *Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde. Soient w et w' deux mots sur $\mathcal{S} \cup \mathcal{S}^{-1}$ satisfaisant $w \curvearrowright_{\mathcal{R}} w'$. Alors on a $w \equiv_{\mathcal{R}}^{\pm} w'$.*

Démonstration. Il suffit de montrer le résultat pour $w \curvearrowright_{\mathcal{R}}^{(1)} w'$. Le cas où un sous-mot $s^{-1}s$ a été supprimé est trivial. Supposons donc que w' a été obtenu depuis w par substitution de $s^{-1}t$ par vu^{-1} où $sv = tu$ est une relation de $\mathcal{R}$. Alors on a $sv \equiv_{\mathcal{R}} tu$ et, a fortiori, $sv \equiv_{\mathcal{R}}^{\pm} tu$, d'où $s^{-1}t \equiv_{\mathcal{R}}^{\pm} vu^{-1}$, ce qui conduit à $w \equiv_{\mathcal{R}}^{\pm} w'$. □

2 CONVERGENCE ET CONFLUENCE

Les questions de savoir si le retournement d'un mot aboutit en un nombre fini d'étapes (problème de convergence), à quels mots il aboutit (problème de confluence) et en combien d'étapes (problème de complexité) sont difficiles en général. Le problème de la complexité est traité dans le cas particulier des mots de tresse dans la partie B. Dans cette section on aborde la convergence et la confleunce ; on montre que toute présentation n'admet pas en général un retournement qui aboutit, même dans des cas simples. Cependant, nous énonçons une proposition établissant un critère pour qu'un retournement termine et faisons le lien avec la notion de multiple commun dans un monoïde.

Définition 2.1. On dit que le retournement associé à une présentation est *convergent* si, pour tout mot w, il existe une borne supérieure à la longueur des suites de retournements maximales partant de w.

Lorsqu'une suite de retournements maximale est de longueur finie — comme dans la suite issue de $\sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3^{-1}\sigma_2$ dans l'exemple 1.3 — et de dernier mot w', cela signifie soit que w' est positif-négatif, soit que pour tout sous-mot de deux lettres $s^{-1}t$ de w' il n'existe aucune relation $s\ldots = t\ldots$ dans la présentation considérée. Cependant, il existe des présentations dont le retournement associé n'est pas convergent, c'est-à-dire qu'il existe des mots admettant des suites de retournements infinies.

Exemple 2.2. Considérons la présentation de Baumslag-Solitar $(\mathtt{a},\mathtt{b};\mathtt{ba}=\mathtt{a}^2\mathtt{b})$ et le mot de départ Bab. On a alors la suite de retournements

$$[\mathtt{Ba}]\mathtt{b} \curvearrowright^{(1)} \mathtt{aB}[\mathtt{Ab}] \curvearrowright^{(1)} \mathtt{aBabA}.$$

Après deux retournements de Bab, le motif Bab apparaît comme sous-mot, d'où on conclut que la suite de retournements issue de Bab est de longueur infinie. Un autre exemple de retournement non convergent est fourni par les les présentations d'Artin-Tits non sphériques : considérons la présentation $(\mathtt{a},\mathtt{b},\mathtt{c};\mathtt{aba}=\mathtt{bab},\mathtt{aca}=\mathtt{cac},\mathtt{bcb}=\mathtt{cbc})$ et le mot Abc ; par retournements successifs, on obtient

$$[\mathtt{Ab}]\mathtt{c} \curvearrowright^{(1)} \mathtt{baB}[\mathtt{Ac}] \curvearrowright^{(1)} \mathtt{baBcaCA}.$$

Remarquons que dans cette présentation, les trois générateurs jouent un rôle symétrique et que dans le dernier mot on trouve le motif Bca, qui est une « permutation circulaire » du mot initial Abc. En poursuivant le retournement, on trouve une autre permutation du mot de départ, à savoir Cab ; encore plus loin dans la suite de retournements, on obtient le sous-mot Abc, montrant que le retournement n'est pas convergent.

On donne à la proposition 2.11 un critère simple permettant de déterminer si une présentation admet un retournement convergent. Auparavant, on définit les termes nécessaires.

Définition 2.3 (présentation complémentée)**.** Une présentation $(\mathcal{S};\mathcal{R})$ est *complémentée* si, pour tout couple de lettres distinctes s,t de $\mathcal{S}$, il existe au plus une relation $s\ldots = t\ldots$ dans $\mathcal{R}$.

Remarque 2.4. La terminologie ici employée a un équivalent en termes de *complément*, notion étudiée dans [12] puis dans [14]. Une présentation $(\mathcal{S};\mathcal{R})$ est *complémentée* si elle admet un complément f, c'est-à-dire une application (partielle) $f : \mathcal{S}\times\mathcal{S} \to \mathcal{S}^*$ dont l'ensemble de définition est un sous-ensemble symétrique de $\mathcal{S}\times\mathcal{S}$, satisfaisant $f(x,x) = \varepsilon$ pour tout x de $\mathcal{S}$, et telle que $\mathcal{R}$ soit l'ensemble des relations $xf(x,y) = yf(y,x)$ pour (x,y) dans l'ensemble de définition de f, avec $x \neq y$.

À partir d'un même mot sont issues possiblement plusieurs suites de retournements. Il n'est pas clair que ces suites, même maximales, admettent un mot final commun (voir le paragraphe suivant la remarque 2.7 pour une courte discussion).

Définition 2.5 (confluence)**.** Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. Le retournement associé à $(\mathcal{S};\mathcal{R})$ est *confluent* si lorsqu'on a trois mots w, w' et w'' vérifiant $w \curvearrowright w'$, $w \curvearrowright w''$ alors il existe un mot w''' satisfaisant $w' \curvearrowright w'''$ et $w'' \curvearrowright w'''$.

Dans le cas des présentations complémentées — en particulier dans le cas des présentations d'Artin des monoïdes de tresses donc —, on a le résultat de confluence suivant.

Proposition 2.6 ([13, Prop. II.1.10])**.** *Soit une présentation complémentée $(\mathcal{S};\mathcal{R})$. Le retournement associé à $(\mathcal{S};\mathcal{R})$ est confluent.*

Démonstration. Soient trois mots w, w' et w'' vérifiant $w \curvearrowright_{\mathcal{R}}^{(n')} w'$, $w \curvearrowright_{\mathcal{R}}^{(n'')} w''$. Il suffit de montrer qu'il existe n et w''' satisfaisant $\sup(n',n'') \leq n \leq n'+n''$, $w' \curvearrowright_{\mathcal{R}}^{(n-n')} w'''$ et $w'' \curvearrowright_{\mathcal{R}}^{(n-n'')} w'''$. Pour $n' = 0$, on a $w = w'$ et on peut prendre $n = n''$, $w''' = w''$. Pour $n'' = 0$, on emploie un argument similaire. Supposons maintenant $n' = n'' = 1$. Alors il existe des sous-mots $s^{-1}t$ et $s'^{-1}t'$ de w, avec s,t,s',t' des lettres positives, qui ont été retournés pour obtenir w' et w''. Ces sous-mots sont soit le même, auquel cas on prend $n = 1$, $w''' = w' = w''$, soit disjoints, auquel cas on prend $n = 2$ et on pose que le w''' est le mot obtenu depuis w en retournant les deux sous-mots ci-dessus.

On raisonne maintenant par récurrence sur $n'+n''$. On a prouvé le cas $n' \leq 1$ et $n'' \leq 1$. Supposons donc $n'+n'' \geq 2$. Soit w_1 un mot vérifiant $w \curvearrowright_{\mathcal{R}}^{(n_1'')} w_1 \curvearrowright_{\mathcal{R}}^{(n_2'')} w''$ avec $n_1''+n_2'' = n''$ et $n_1'' \geq 1$, $n_2'' \geq 1$. Par hypothèse de récurrence, il existe n_1, n_2 avec $n_1 \leq n'+n_1''$ et $n_2 \leq n_1 - n_1'' + n_2''$, et w_1', w''' satisfaisant $w' \curvearrowright_{\mathcal{R}}^{(n_1-n_1')} w_1'$, $w_1 \curvearrowright_{\mathcal{R}}^{(n_1-n_1'')} w_1'$, $w_2' \curvearrowright_{\mathcal{R}}^{(n_2-n_1+n_1'')} w'''$ et $w'' \curvearrowright_{\mathcal{R}}^{(n_2-n_2'')} w'''$. Pour $n = n_1'' + n_2$, on a $w' \curvearrowright_{\mathcal{R}}^{(n-n')} w'''$. □

Remarque 2.7. Cette proposition s'illustre bien avec les diagrammes de retournement : c'est dire que, partant d'un mot w, le retournement associé à une présentation complémentée produit un unique diagramme de retournement maximal, et ce, quel que soit l'ordre des étapes de retournement.

Ce résultat de confluence du retournement est faux en général si on ne suppose pas la présentation complémentée : prenons la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{ab}^2 = \mathtt{b}^2\mathtt{a}, \mathtt{a}^2\mathtt{b} = \mathtt{ba}^2)$ et considérons les retournements du mot $\mathtt{Ab}$; on a $\mathtt{Ab} \curvearrowright^{(1)} \mathtt{abAA}$ d'une part et $\mathtt{Ab} \curvearrowright^{(1)} \mathtt{bbAB}$ d'autre part. Ces deux mots sont finaux et par conséquent on ne peut espérer les retourner en un même mot. On remarque avec la suite de retournements

$$[\mathtt{Ab}]\mathtt{a} \curvearrowright^{(1)} \mathtt{bbA}[\mathtt{Ba}] \curvearrowright^{(1)} \mathtt{bbAba}$$

que ce le retournement associé à cette présentation n'est pas non plus convergent.

Remarque 2.8. La confluence et la convergence sont deux propriétés différentes. La confluence assure l'existence d'un élément en lequel se retournent deux mots distincts provenant de retournements différents d'un même mot ; la convergence assure que le processus s'arrête en un temps fini. Le retournement associé à une présentation complémentée — qui est donc confluent — n'est pas nécessairement convergent : la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{a}^2\mathtt{b} = \mathtt{b})$ est complémentée et la suite de retournements issue de $\mathtt{Bab}$ est périodique de période 2. De la même manière, la convergence n'implique pas la confluence : la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{ab} = \mathtt{b}, \mathtt{a} = \mathtt{ba})$ n'est pas confluente car $\mathtt{Ab}$ se retourne en $\mathtt{b}$ et $\mathtt{A}$, qui sont finaux. En revanche, le retournement associé est convergent : il suffit de voir que si on a $w \curvearrowright w'$ alors $|w'|$ est strictement inférieur à $|w|$ et donc les suites de retournements issues de w sont de longueur bornée supérieurement par $|w|$.

Lorsque le retournement est confluent, on définit une opération sur les mots.

Définition 2.9 (opération $\backslash_{\mathcal{R}}$)**.** Soit une présentation de monoïde $(\mathcal{S}; \mathcal{R})$ dont le retournement associé est confluent. Soient u et v deux mots sur $\mathcal{S}$. On définit $u\backslash_{\mathcal{R}} v$ comme l'unique mot v' satisfaisant $u^{-1}v \curvearrowright_{\mathcal{R}} v'u'^{-1}$, avec u' un mot sur $\mathcal{S}$, si un tel mot u' existe.

De même que pour $\curvearrowright_{\mathcal{R}}$ et $\equiv_{\mathcal{R}}$, l'opération $\backslash_{\mathcal{R}}$ dépend évidemment de la présentation considérée. Et de même, on omettra la référence à l'ensemble des relations lorsque la compréhension n'en pâtira pas.

L'opération $\backslash_{\mathcal{R}}$ est bien définie car l'unicité du mot v' est garantie par la confluence. En revanche, l'existence de v' n'est pas automatique.

Définition 2.10 (convergence forte)**.** On dit que le retournement associé à la présentation complémentée $(\mathcal{S}; \mathcal{R})$ *converge fortement* si $u\backslash_{\mathcal{R}} v$ existe pour tous u et v de $\mathcal{S}^*$.

Il est clair que la convergence forte du retournement implique la convergence. La proposition suivante en donne une caractérisation.

Proposition 2.11 ([13, Prop. 3.5])**.** *Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde complémentée. Le retournement associé à $(\mathcal{S}; \mathcal{R})$ est fortement convergent si et seulement s'il existe un sous-ensemble $\mathcal{S}'$ de $\mathcal{S}^*$ contenant $\mathcal{S}$ et tel que $u\backslash_{\mathcal{R}} v$ existe et appartienne à $\mathcal{S}'$ pour tous u et v de $\mathcal{S}'$.*

Démonstration. Supposons que le retournement soit fortement convergent. Alors il suffit de prendre $\mathcal{S}' = \mathcal{S}^*$. Réciproquement, supposons qu'il existe un sous-ensemble de mots $\mathcal{S}'$ contenant $\mathcal{S}$ et tel que $u\backslash_{\mathcal{R}} v$ existe et appartienne à $\mathcal{S}'$ pour tous u et v de $\mathcal{S}'$. Soit w un mot sur $\mathcal{S} \cup \mathcal{S}^{-1}$. On peut écrire $w = u_1^{e_1} \dots u_r^{e_r}$, avec $u_i \in \mathcal{S}'$, $e_i = \pm 1$ pour tout i, et $r \leq |w|$. Soit p le nombre de e_i positifs. Une simple récurrence montre que w est retournable en un mot $v_1 \dots v_p v_{p+1}^{-1} \dots v_r^{-1}$, avec $v_1, \dots, v_r$ des mots de $\mathcal{S}'$. □

On dira qu'un ensemble $\mathcal{S}'$ tel que $u\backslash_{\mathcal{R}} v$ appartient à $\mathcal{S}'$ dès que u et v appartiennent à $\mathcal{S}'$ est *clos par* $\backslash_{\mathcal{R}}$. Le plus petit ensemble clos par $\backslash_{\mathcal{R}}$ contenant $\mathcal{S}$ est appelé *clôture* de $\mathcal{S}$ par $\backslash_{\mathcal{R}}$.

Remarque 2.12. Une application de la proposition 2.11 est que, pour $n \geq 3$, le retournement associé à la présentation d'Artin-Tits du groupe de tresses B_n est fortement convergent [13, Prop 3.8]. En outre, on montre facilement à partir de cette proposition que si la clôture $\mathcal{S}'$ de l'ensemble des générateurs $\mathcal{S}$ est finie, alors la longueur d'une suite de retournements issue d'un mot de longueur ℓ est dans $O(\ell^2)$. C'est le cas des présentations des groupes de tresses B_n. On établit dans la partie B des bornes inférieures et supérieures pour la longueur des suites de retournements en fonction de la longueur des mots initiaux. Mais, en général, la clôture par $\backslash_{\mathcal{R}}$ de l'ensemble des générateurs $\mathcal{S}$ d'une présentation de monoïde $(\mathcal{S}; \mathcal{R})$ n'est pas finie : la clôture de l'ensemble des générateurs de la présentation du monoïde des tresses positives B_∞^+ est infinie et vérifie les hypothèses de la proposition 2.11 donc le retournement associé est fortement convergent. Toutefois la meilleure borne supérieure qu'on montre sur la longueur de la suite de retournements est exponentielle en la longueur du mot de départ (voir la partie B pour des détails).

3 COMPLÉTUDE

Retourner un mot w consiste en l'application à w d'une suites de règles de réécriture déterminées par la présentation qu'on étudie. Si le mot w est de la forme $u^{-1}v$ avec u et v des mots positifs, et si le retournement est fortement convergent, c'est-à-dire qu'il existe des mots u' et v' positifs vérifiant $u^{-1}v \curvearrowright v'u'^{-1}$, alors on a l'équivalence entre mots positifs $uv' \equiv vu'$ (prop. 1.5) ; autrement dit, s'il existe un multiple commun aux éléments que représentent u et v dans le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$, alors le retournement en trouve un.

Question 3.1. *Que valent u' et v' dans le cas $u \equiv v$?*

Si on avait $u' = v' = \varepsilon$ dès qu'on a l'équivalence $u \equiv v$ alors ce serait dire que le retournement fournit une solution au problème du mot ; il suffirait en effet de produire toutes les suites de retournements issues de $u^{-1}v$ et les mots u et v seraient équivalents si et seulement si on avait $u^{-1}v \curvearrowright \varepsilon$. Ce n'est pas le cas en général : il existe des présentations et des mots u et v équivalents tels qu'aucune suite de retournements issue de $u^{-1}v$ ne s'achève

par le mot vide ε. Dans cette section, nous caractérisons les présentations pour lesquelles le retournement résout le problème du mot et énonçons différents critères pour les reconnaître.

Définition 3.2 (complétude)**.** Une présentation de monoïde $(\mathcal{S};\mathcal{R})$ est *R-complète* si $u \equiv v$ implique $u^{-1}v \curvearrowright \varepsilon$, pour tous mots u, v de $\mathcal{S}^*$.

Il est clair, d'après la proposition 1.5, que $u^{-1}v \curvearrowright \varepsilon$ implique $u \equiv v$. Une présentation est donc dite R-complète si cette implication est en réalité une équivalence, autrement dit, si l'équivalence entre deux mots positifs est calculable par retournement. Le préfixe « R- » indique qu'on parle de la propriété de complétude d'une présentation vis-à-vis du retournement. On verra au chapitre II une autre notion de complétude, la Gröbner-complétude, pour laquelle on emploiera le préfixe « G- ».

Telle qu'elle est définie, la complétude d'une présentation n'est pas une propriété qui peut être testée dans la pratique : il faudrait en effet voir pour toutes les paires de mots positifs équivalents (u, v) si on a $u^{-1}v \curvearrowright \varepsilon$, ce qui présuppose une solution au problème de mot. Dans le but d'énoncer une caractérisation de la complétude pour laquelle le retournement suffit à tout montrer — c'est-à-dire pour laquelle nous n'avons pas recourt à une solution au problème du mot —, nous énonçons la proposition suivante qui est une première reformulation de la complétude :

Proposition 3.3 ([16, Prop. 3.3 (i)])**.** *(Figure 4.) La présentation $(\mathcal{S};\mathcal{R})$ est R-complète si et seulement si pour tous mots u, v, u', v' de $\mathcal{S}^*$ on a l'implication suivante :*

(1) *Si on a $uv' \equiv vu'$, alors il existe u'', v'', w de $\mathcal{S}^*$ vérifiant $u^{-1}v \curvearrowright v''u''^{-1}$, $u' \equiv u''w$ et $v' \equiv v''w$.*

Démonstration. On suppose qu'on a (1) et on montre la R-complétude. Supposons $u \equiv_{\mathcal{R}} v$, c'est-à- dire $u\varepsilon \equiv_{\mathcal{R}} v\varepsilon$. D'après (1), il existe des mots u'', v'' et w tels qu'on ait $u^{-1}v \curvearrowright_{\mathcal{R}} v''u''^{-1}$, $\varepsilon \equiv_{\mathcal{R}} u''w$ et $\varepsilon \equiv_{\mathcal{R}} v''w$. Comme $(\mathcal{S};\mathcal{R})$ est une présentation de monoïde, $\varepsilon \equiv_{\mathcal{R}} u''w$ implique $u'' = w = \varepsilon$ et $\varepsilon \equiv'_{\mathcal{R}} v'w$ implique $v'' = \varepsilon$. On en déduit qu'on a $u^{-1}v \curvearrowright_{\mathcal{R}} \varepsilon$.

Réciproquement, supposons que $(\mathcal{S};\mathcal{R})$ est R-complète et montrons (1). Supposons $uv' \equiv vu'$ donc, par R-complétude, $(uv')^{-1}(vu') \equiv_{\mathcal{R}} \varepsilon$. Du lemme 1.4, on déduit l'existence des mots u'', v'', w', w'' tels qu'on a $u^{-1}v \curvearrowright_{\mathcal{R}} v''u''^{-1}$, $v'^{-1}v'' \curvearrowright_{\mathcal{R}} w'^{-1}$, $u''^{-1}u' \curvearrowright_{\mathcal{R}} w''$ et $w'^{-1}w'' \curvearrowright_{\mathcal{R}} \varepsilon$ (voir figure 5). D'après la proposition 1.5, on déduit $u' \equiv_{\mathcal{R}} u''w''$, $w' \equiv_{\mathcal{R}} w''$ et $v' \equiv_{\mathcal{R}} v''w' \equiv_{\mathcal{R}} v''w''$, ce qui montre (1). □

Autrement dit, cette proposition affirme que si $\overline{u}$ et $\overline{v}$ (où on rappelle que $\overline{u}$ désigne l'élément du monoïde représenté par le mot u) ont un multiple commun représenté par uv' et vu', alors l'équivalence $uv' \equiv vu'$ se factorise par le retournement de $u^{-1}v$ (voir figure 4).

Remarque 3.4. Une autre manière encore d'exprimer cette caractérisation de la R-complétude de la présentation $(\mathcal{S};\mathcal{R})$ est de le voir de la façon suivante : l'équivalence $su \equiv tv$,

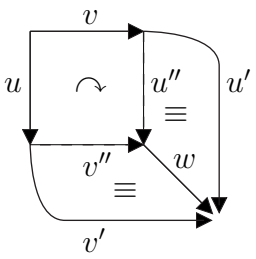


FIGURE 4 – Une autre façon de définir la R-complétude d'une présentation, c'est-à-dire l'équivalence entre $u \equiv v$ et $u^{-1}v \curvearrowright \varepsilon$, est de dire que chaque équivalence $uv' \equiv vu'$ peut se factoriser par le retournement de $u^{-1}v$.

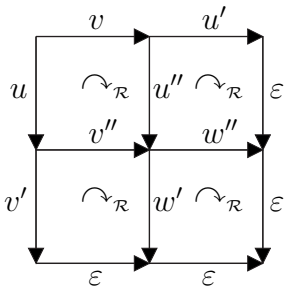


FIGURE 5 – Partant de l'équivalence $uv' \equiv_{\mathcal{R}} vu'$, on montre qu'il existe une factorisation par le retournement de $u^{-1}v$.

avec s, t deux lettres distinctes de $\mathcal{S}$ et u, v dans $\mathcal{S}^*$, signifie qu'il existe des mots u', v' et w de $\mathcal{S}^*$ tels qu'on ait $su \equiv su'w \equiv tv'w \equiv tv$ et $su' = tv'$ soit une relation de $\mathcal{R}$; la R-complétude exprime ici le fait qu'il n'est pas nécessaire pour passer d'un mot débutant par s à un mot équivalent débutant par t d'introduire une lettre intermédiaire r en appliquant, par exemple, d'abord une relation $s \ldots = r \ldots$ puis une relation $r \ldots = t \ldots$.

4 CONDITION DU CUBE

4.1 DÉFINITION ET ÉQUIVALENCE AVEC LA R-COMPLÉTUDE

Aucune des formulations de la R-complétude données jusqu'à présent n'est satisfaisante d'un point de vue pratique. On s'appuie sur la remarque 3.4 pour donner de nouvelles caractérisations de la R-complétude dans le cas de présentations présentant différentes propriétés.

Définition 4.1 (condition du cube)**.** Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde. Pour u, v, w dans $\mathcal{S}^*$, on dit que $(\mathcal{S}; \mathcal{R})$ satisfait la *condition du cube* (resp. la *condition du cube forte*) en u, v, w si on a l'implication suivante :

> Si on a $u^{-1}ww^{-1}v \curvearrowright v'u'^{-1}$ avec u', v' dans $\mathcal{S}^*$, alors il existe u'', v'', w'' dans $\mathcal{S}^*$ vérifiant $u^{-1}v \curvearrowright v''u''^{-1}$, $u' \equiv u''w''$, $v' \equiv v''w''$ (resp. alors on a $(uv')^{-1}(vu') \curvearrowright \varepsilon$).

On énonce maintenant la caractérisation de la R-complétude qui est la plus utile : la proposition suivante établit que demander la R-complétude d'une présentation revient à demander que la condition du cube soit satisfaite en tout triplet de mots.

Proposition 4.2 ([16, Prop. 3.2])**.** *Pour toute présentation de monoïde $(\mathcal{S};\mathcal{R})$, les propriétés suivantes sont équivalentes :*

- $(\mathcal{S};\mathcal{R})$ *est R-complète ;*
- $(\mathcal{S};\mathcal{R})$ *satisfait la condition du cube en tout triplet de $\mathcal{S}^*$;*
- $(\mathcal{S};\mathcal{R})$ *satisfait la condition du cube forte en tout triplet de $\mathcal{S}^*$.*

4.2 CRITÈRES DE R-COMPLÉTUDE

Vérifier la R-complétude d'une présentation revient donc à tester la condition du cube sur tous les triplets de mots positifs. Plus précisément, il s'agit de tester la condition du cube forte, ce qui est d'un point de vue calculatoire beaucoup plus faisable puisque tout s'exprime en termes de retournements. Toutefois, vérifier la condition du cube forte sur tous les triplets de $\mathcal{S}^*$ nécessite une infinité de retournements. En se restreignant à certains types de présentations, on peut considérablement diminuer l'ensemble sur lequel tester la condition du cube. La première famille de présentations qu'on considère est celle des présentations admettant une fonction une pseudolongueur.

Définition 4.3 (homogénéité, pseudolongueur)**.** On dit qu'une présentation de monoïde $(\mathcal{S};\mathcal{R})$ est *homogène* si elle admet une *pseudolongueur*, c'est-à-dire une application $\lambda : \mathcal{S}^* \to \mathbb{N}$ satisfaisant $\lambda(su) > \lambda(u)$ pour tout s de $\mathcal{S}$ et u de $\mathcal{S}^*$, invariante sous $\equiv$. On dit que $(\mathcal{S};\mathcal{R})$ est *homogène* si $\equiv$ préserve une pseudolongueur.

Remarque 4.4. Si les relations de $(\mathcal{S};\mathcal{R})$ conservent la longueur, autrement dit, si pour chaque relation $u = v$ de $\mathcal{R}$ on a $|u| = |v|$, alors la longueur $|.|$ est elle-même une pseudolongueur pour $(\mathcal{S};\mathcal{R})$.

La première amélioration qu'on donne de la proposition 4.2 concerne les présentations homogènes.

Proposition 4.5 ([16, Prop. 4.4])**.** *Supposons que $(\mathcal{S};\mathcal{R})$ est une présentation de monoïde homogène. Alors une condition suffisante (et nécessaire) pour que $(\mathcal{S};\mathcal{R})$ soit R-complète est que l'une des propriétés équivalentes suivantes soit vérifiée :*

- *la condition du cube forte est satisfaite sur $\mathcal{S}$;*
- *la condition du cube est satisfaite sur $\mathcal{S}$.*

On omet la preuve de cette proposition qui est longue. Le point clef de la démonstration est de voir que grâce à l'homogénéité de la présentation, on peut procéder par récurrence sur la pseudolongueur ; la pseudolongueur est le paramètre qui décroît dans la preuve, c'est celui qui mesure, disons, la distance à un multiple commun. Dans le cas général, c'est-à-dire sans pseudolongueur — et sans complémentation —, on ne connaît pas de tel critère.

La proposition 4.5 présente une très nette amélioration par rapport à la proposition 4.2 puisqu'elle permet de réduire les vérifications de la condition du cube à tous les triplets de

lettres (qui sont en nombre fini dès que la présentation est de type fini). En outre, le fait qu'il suffise de vérifier la condition du cube forte permet d'énoncer un critère très simple pour tester — en n'utilisant que des retournements — la R-complétude d'une présentation. Le critère est présenté sous la forme de l'algorithme 4.6 auquel le proposition 4.7 donne une justification.

Algorithme 4.6. *Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde homogène. Pour tout triplet de lettres s, t, r de $\mathcal{S}$:*

1. *Retourner $s^{-1}rr^{-1}t$ en tous les mots positifs-négatifs possibles.*
2. *Pour tout mot uv^{-1} ainsi obtenu, vérifier si on a $(su)^{-1}(tv) \curvearrowright \varepsilon$.*

Proposition 4.7 ([16, Algorithm 4.8])**.** *Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde homogène. La présentation $(\mathcal{S};\mathcal{R})$ est R-complète si et seulement si la réponse à l'étape 2 de l'algorithme 4.6 est positive pour tout triplet de lettres (r,s,t) et pour tout mot uv^{-1} obtenu à l'étape 1.*

On illustre l'application de ce critère aux présentations classiques des monoïdes de tresses.

Exemple 4.8 ([16, Ex. 4.10])**.** Considérons la présentation standard d'Artin

$$\left(\sigma_1,\dots,\sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{pour } |j-i|=1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \text{pour } |j-i|\geq 2 \end{array}\right)$$

du monoïde de tresses à n brins B_n^+. Nous allons montrer que cette présentation est R-complète. Il y a deux types de relations mises en jeu : les relations de longueur 3, $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$, et les relations de longueur 2, $\sigma_i\sigma_j = \sigma_j\sigma_i$, pour $|i-j|\geq 2$. Cette présentation est donc homogène puisque les relations préservent les longueurs (remarque 4.4). Par la proposition 4.7, il nous suffit donc de raisonner sur les triplets de lettres. Or, il est clair d'après les relations qu'il suffit de vérifier la condition du cube sur seulement trois types de triplets : les triplets de type $3,3,2$, ceux de type $3,2,2$ et ceux de type $2,2,2$. (Figure 6) Pour le type $3,3,2$ on teste sur le triplet $(\sigma_1,\sigma_2,\sigma_3)$:

$$\begin{aligned} [\sigma_1^{-1}\sigma_2]\,[\sigma_2^{-1}\sigma_3] &\curvearrowright \sigma_2\sigma_1\sigma_2^{-1}[\sigma_1^{-1}\sigma_3]\sigma_2\sigma_3^{-1}\sigma_2^{-1} \\ &\curvearrowright \sigma_2\sigma_1[\sigma_2^{-1}\sigma_3]\,[\sigma_1^{-1}\sigma_2]\sigma_3^{-1}\sigma_2^{-1} \\ &\curvearrowright \sigma_2\sigma_1\sigma_3\sigma_2\sigma_3^{-1}[\sigma_2^{-1}\sigma_2]\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1} \\ &\curvearrowright \sigma_2\sigma_1\sigma_3\sigma_2[\sigma_3^{-1}\sigma_1]\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1} \\ &\curvearrowright \sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}. \end{aligned}$$

La présentation (4.8) est complémentée donc il n'y a qu'une suite de retournements issue de $\sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3$. Il reste à tester qu'on a $(\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1)^{-1}\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3 \curvearrowright \varepsilon$. On effectue le retournement à la figure 6.

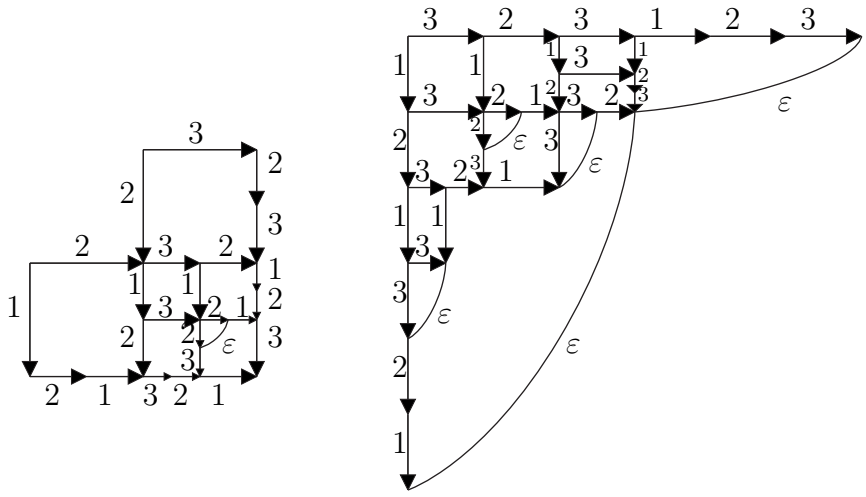


FIGURE 6 – Pour une raison de lisibilité, sur les diagrammes, une étiquette i doit être lue σ_i. On considère la présentation d'Artin standard $(\sigma_1, \sigma_2, \sigma_3; \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2, \sigma_3\sigma_1 = \sigma_1\sigma_3, \sigma_3\sigma_2\sigma_3 = \sigma_2\sigma_3\sigma_2)$ du monoïde de tresses B_3^+. Pour tester la condition du cube forte sur le triplet $(\sigma_1, \sigma_2, \sigma_3)$, on commence par retourner $\sigma_1^{-1}\sigma_2\sigma_2^{-1}\sigma_3$ en $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}$. La présentation d'Artin étant complémentée, il n'y a qu'un seul mot terminal possible. On vérifie ensuite qu'on a $(\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1)^{-1}\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3 \curvearrowright \varepsilon$.

Comme le retournement s'achève par le mot vide, on conclut que la condition du cube est vérifiée sur le triplet $(\sigma_1, \sigma_2, \sigma_3)$. On fait de même avec les triplets $(\sigma_1, \sigma_2, \sigma_4)$ et $(\sigma_1, \sigma_3, \sigma_5)$ et on prouve ainsi que les présentations d'Artin des monoïdes de tresses sont R-complètes.

Toutes les présentations ne sont pas homogènes et on ne peut espérer utiliser le critère de la proposition 4.7 pour toutes les présentations. Cependant, dans le cas des présentations complémentées, on peut, comme pour les présentations homogènes, restreindre l'ensemble de mots sur lequel vérifier la condition du cube.

Proposition 4.9 ([15, Prop. 6.5])**.** *Supposons que $(\mathcal{S}; \mathcal{R})$ est une présentation de monoïde complémentée et que $\mathcal{S}'$ est un ensemble incluant $\mathcal{S}$ et clos par $\backslash_{\mathcal{R}}$. Alors une condition suffisante (et nécessaire) pour que $(\mathcal{S}; \mathcal{R})$ soit complète est que la condition du cube soit vraie sur $\mathcal{S}'$.*

Avant de terminer cette section, citons une application d'un résultat plus général — mettant en jeu la k-cohérence (qu'on n'a pas définie ici) — nous fournissant un critère de R-complétude concernant le cas très particulier des présentations complémentées à deux générateurs.

Proposition 4.10 ([15, Prop. 6.4])**.** *Une présentation de monoïde complémentée à deux générateurs est R-complète.*

5 COMPLÉTION

Dans la section précédente on a donné plusieurs critères pour reconnaître une présentation R-complète. Au-delà de la détection de la propriété de R-complétude d'une présentation donnée, on peut dans les bons cas compléter une présentation non R- complète : le fait qu'une présentation $(\mathcal{S}; \mathcal{R})$ ne soit pas R-complète signifie qu'il existe une paire de mots équivalents (u, v) tels qu'on n'ait pas $u^{-1}v \curvearrowright \varepsilon$. Pour réparer ce défaut, on a la possibilité d'ajouter la relation $u = v$ à la présentation ; cela ne modifie évidemment pas $\equiv$ et on a dorénavant $u^{-1}v \curvearrowright \varepsilon$, par définition du retournement. R-Compléter une présentation consiste ainsi à détecter une obstruction et l'éliminer en ajoutant la relation correspondante à la liste des relations de la présentations.

5.1 MÉTHODE DE COMPLÉTION

En se fondant sur l'algorithme 4.6 et la proposition 4.7, on énonce un algorithme pour construire une présentation de monoïde R-complète à partir d'une présentation de monoïde homogène qui ne l'est pas.

Algorithme 5.1. *Le contexte est celui de l'algorithme 4.6.*

RÉPÉTER
  Retourner $s^{-1}rr^{-1}t$ en tous les mots positifs-négatifs possibles ;
  POUR *tout uv^{-1} ainsi obtenu :*
    SI $(su)^{-1}(tv) \not\curvearrowright \varepsilon$
    ALORS *ajouter la relation $su = tv$ à la présentation ;*
TANT QUE *on a ajouté de nouvelles relations à la présentation ;*
SORTIE : *une présentation.*

C'est le résultat suivant qui donne une utilité à l'algorithme précédent.

Proposition 5.2 ([16, §5])**.** *Quand l'algorithme 5.1 termine, sa sortie est une présentation R-complète.*

5.2 UN EXEMPLE DÉTAILLÉ

On calcule ici la R-complétion de la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{baa})$. Malgré l'apparente simplicité de cette présentation, le retournement associé n'est pas complet : pour montrer

cela, on utilise le critère de la proposition 4.7 qui s'applique aux présentations homogènes. Or la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{baa})$ est homogène puisque l'unique relation conserve la longueur (voir remarque 4.4). D'après le critère de R-complétude, il faut étudier les retournements de tous les mots $s^{-1}rr^{-1}t$, avec s,r,t dans $\{\mathtt{a},\mathtt{b}\}$. Remarquons toutefois qu'il n'y a aucune relation de la forme $\mathtt{a}\ldots=\mathtt{b}\ldots$; ceci implique que seuls les retournements issus de $\mathtt{b}^{-1}\mathtt{bb}^{-1}\mathtt{b}$ sont susceptibles de donner un mot positif-négatif.

Le mot $\mathtt{b}^{-1}\mathtt{bb}^{-1}\mathtt{b}$ se retourne en les mots positifs-négatifs $\mathtt{a}^4\mathtt{BA}^3$ et $\mathtt{a}^2\mathtt{BA}$, et, symétriquement, en $\mathtt{a}^3\mathtt{bA}^4$ et $\mathtt{abA}^2$ (Fig. 7).

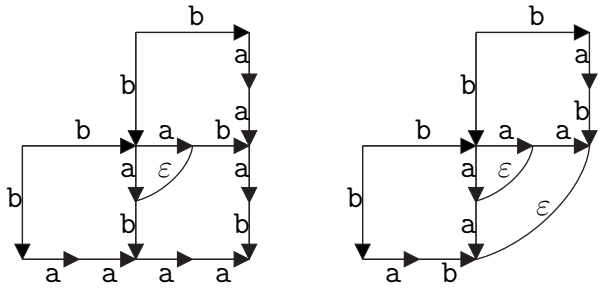


FIGURE 7 – Cas de la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{ba}^2)$. Le mot BbBb se retourne en $\mathtt{a}^4\mathtt{BA}^3$ et $\mathtt{a}^2\mathtt{BA}$ ou, symétriquement, en $\mathtt{a}^3\mathtt{bA}^4$ et $\mathtt{abA}^2$. Le mot BbBb se retourne en plusieurs mots positifs-négatifs car le retournement associé à la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{ba}^2)$ n'est pas déterministe : face au motif Bb, on peut retourner en ε, $\mathtt{abA}^2$ ou $\mathtt{a}^2\mathtt{BA}$. Parmi les multiples retournements de BbBb, on ne considère que ceux s'achevant par un mot positif-négatif afin de pouvoir appliquer le critère de la proposition 4.7.

Donc, d'après l'algorithme 4.6, on doit vérifier qu'on a les retournements $\mathtt{A}^4\mathtt{Bba}^3\mathtt{b} \curvearrowright \varepsilon$ et $\mathtt{A}^2\mathtt{Bbab} \curvearrowright \varepsilon$ (les cas symétriques sont similaires). Puisque $\mathtt{bab}=\mathtt{ba}^2$ est une relation de la présentation, on a trivialement $\mathtt{A}^2\mathtt{Bbab} \curvearrowright \varepsilon$. Autrement dit, s'il existe une façon de retourner $\mathtt{A}^4\mathtt{Bba}^3\mathtt{b}$ qui s'achève en ε alors la présentation est R-complète, sinon on ajoute la relation $\mathtt{ba}^4=\mathtt{ba}^3\mathtt{b}$ à la présentation et on reprend l'algorithme 5.1 avec, pour entrée, la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{ba}^2,\mathtt{ba}^3\mathtt{b}=\mathtt{ba}^4)$. On réalise tous les retournements de $\mathtt{A}^2\mathtt{Bbab}$ et aucun ne se termine par ε (voir figure 8).

On ajoute donc la relation $\mathtt{ba}^3\mathtt{b}=\mathtt{ba}^4$ à la présentation et on cherche à nouveau les obstructions à la R-complétude en retournant BbBb. Munie de la relation $\mathtt{ba}^3\mathtt{b}=\mathtt{ba}^4$, la présentation permet maintenant (entre autres) le retournement $\mathtt{BbBb} \curvearrowright \mathtt{a}^5\mathtt{bA}^6$. On doit alors tester $\mathtt{BA}^5\mathtt{Bba}^6 \curvearrowright \varepsilon$. On montre de manière similaire à la figure 8 que ce retournement n'est pas possible. En ajoutant encore une relation, on ajoute de nouvelles obstructions. En fait, pour $m \geq 1$, aucune présentation

$$(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{a}^2\mathtt{b},\ldots,\mathtt{ba}^{2m-1}\mathtt{b}=\mathtt{ba}^{2m})$$

n'est R-complète. Appliquons l'algorithme 5.1. On a traité plus haut le cas $m=1$. Supposons maintenant $m \geq 2$. Il s'agit donc de retourner de toutes les façons possibles BbBb

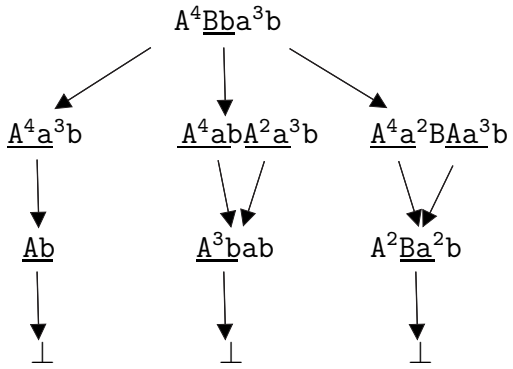


FIGURE 8 – Afin de déterminer la R-complétude de la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{ba}^2)$, l'algorithme 4.6 mène à retourner $\mathtt{A}^4\mathtt{Bba}^3\mathtt{b}$. Comme aucun de ses retournements ne se termine par ε, on en déduit que la présentation n'est pas R-complète et qu'il faut ajouter la relation $\mathtt{ba}^4=\mathtt{ba}^3\mathtt{b}$ à l'ensemble des relations.

à partir du jeu de relations $\{\mathtt{bab}=\mathtt{ba}^2,\ldots,\mathtt{ba}^{2m-1}\mathtt{b}=\mathtt{ba}^{2m}\}$. Le fait que chaque motif $\mathtt{Bb}$ puisse se retourner de nombreuses manières rend le calcul peu aisé. On montre sur la figure 9 les différentes suites de retournements issues du mot $\mathtt{BbBb}$.

Comme pour le cas $m=1$ et toujours en suivant l'algorithme 5.1, retourner $\mathtt{BbBb}$ conduit à différents mots positifs-négatifs (mots entourés de la figure 9). Chacun de ces mots w s'écrit w_+w_- avec w_+,w_- des mots positifs ; l'algorithme 5.1 conduit alors à tester $w_+^{-1}\mathtt{Bb}w_- \curvearrowright \varepsilon$. Les cas $\boxed{1}$ et $\boxed{2}$ étant similaires, on ne réalise que le retournement du cas $\boxed{2}$. Le diagramme de la figure 10 montre que le retournement termine par ε. Le cas $\boxed{3}$ est trivial puisqu'on ne fait que remplacer un motif Xx par ε à chaque étape. Le cas $\boxed{4}$ ne pose pas de problème (figure 11). Finalement, il ne reste plus que le retournement lié à $\boxed{5}$ qu'on réalise à la figure 12. On y montre qu'on n'aboutit pas au mot vide au seul moyen des relations de la forme $\mathtt{ba}^{2n-1}\mathtt{b}=\mathtt{ba}^{2n}$, avec $n<m$. Toutefois, ajouter toutes les relations $\mathtt{ba}^{2n-1}\mathtt{b}=\mathtt{ba}^{2n}$, avec $n\geq m$, résout le problème : reprenant la figure 9, on voit que seul le cas $\boxed{5}$ diffère lorsqu'on travaille avec $\{\mathtt{ba}^{2n-1}\mathtt{b}=\mathtt{ba}^{2n};n\geq 1\}$; dans ce cas, on peut compléter le diagramme par le mot vide ε, montrant que la présentation

$$(\mathtt{a},\mathtt{b};\ \mathtt{ba}^{2n-1}\mathtt{b}=\mathtt{ba}^{2n},n\geq 1).$$

est R-complète.

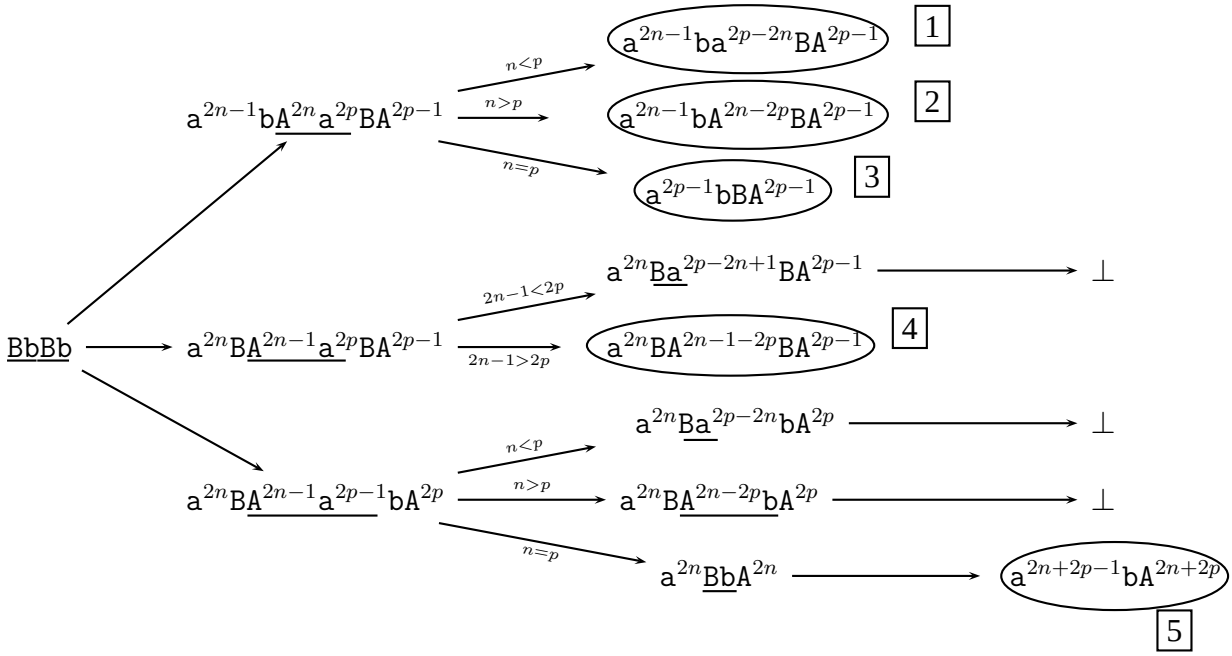


FIGURE 9 – Parmi tous les retournements possibles de BbBb dans la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{a}^2\mathtt{b},\ldots,\mathtt{ba}^{2m-1}\mathtt{b}=\mathtt{ba}^{2m})$, les mots entourés sont les seuls à être positifs-négatifs. C'est grâce à ces mots que va déterminer si la présentation est R-complète ou non. Tous les retournements ne se terminent pas par un mot positif-négatif car les motifs Ab et Ba ne sont pas retournables : les relations de la présentation sont toutes du types $\mathtt{b}\ldots=\mathtt{b}\ldots$, permettant ainsi uniquement le retournements des motifs Bb. Lorsqu'une suite de retournements se termine par $\perp$, cela signifie que les mots terminaux ne sont pas positifs-négatifs.

6 APPLICATIONS

Outre la propriété de détecter, dans les bons cas, les équivalences, nous décrivons dans cette section deux applications du retournement de mot. La première consiste à déterminer si un monoïde M est simplifiable à gauche à partir de la donnée d'une présentation R-complète de M. La deuxième est un critère pour qu'un monoïde admette des ppcm.

6.1 SIMPLIFIABILITÉ

La question de déterminer si un monoïde est simplifiable (c'est-à-dire, pour la simplifiabilité à gauche, si a, x, y sont des éléments du monoïde alors $ax = ay$ implique $x = y$) n'est pas facile en général. Dans le cas des présentations R-complètes toutefois, le retournement est très efficace et on lit directement sur la présentation la simplifiabilité du monoïde

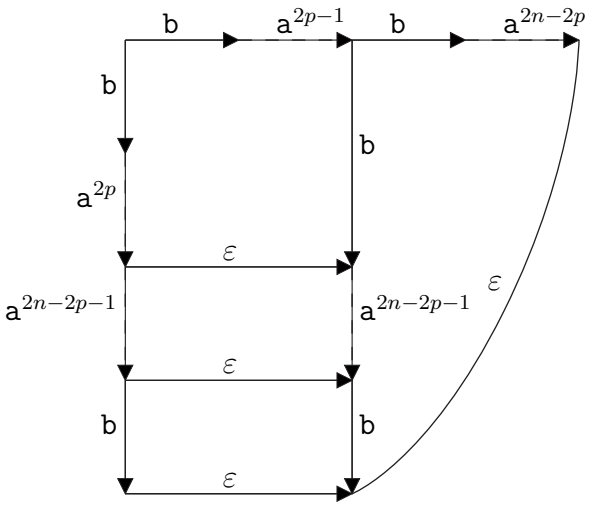


FIGURE 10 – Lors de l'exécution de l'algorithme 5.1, on est amenés à chercher si $\mathtt{BA}^{2n-1}\mathtt{Bba}^{2p-1}\mathtt{ba}^{2n-2p}$ peut se retourner en le mot vide ε en utilisant les relations de la forme $\mathtt{ba}^{2k-1}\mathtt{b} = \mathtt{ba}^{2k}$, avec $k \leq m$ et $p, n \leq m$. Ce diagramme montre que cela est possible.

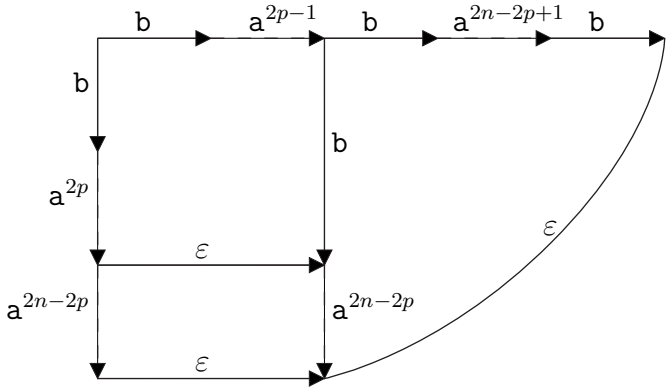


FIGURE 11 – Lors de l'exécution de l'algorithme 5.1, on est amenés à chercher si $\mathtt{A}^{2n}\mathtt{Bba}^{2p-1}\mathtt{ba}^{2n-2p+1}b$ peut se retourner en le mot vide ε en utilisant les relations de la forme $\mathtt{ba}^{2k-1}\mathtt{b} = \mathtt{ba}^{2k}$, avec $k \leq m$ et $p, n \leq m$. Ce diagramme montre que c'est possible.

associé.

Proposition 6.1 ([16, Prop. 6.1])**.** *Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde R-complète. Alors le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ est simplifiable à gauche si et seulement si on a $u^{-1}v \curvearrowright_{\mathcal{R}} \varepsilon$ pour toute relation de la forme $su = sv$ de $\mathcal{R}$ avec $s \in \mathcal{S}$.*

En particulier, on en déduit que prouver qu'un monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ n'est pas simplifiable à

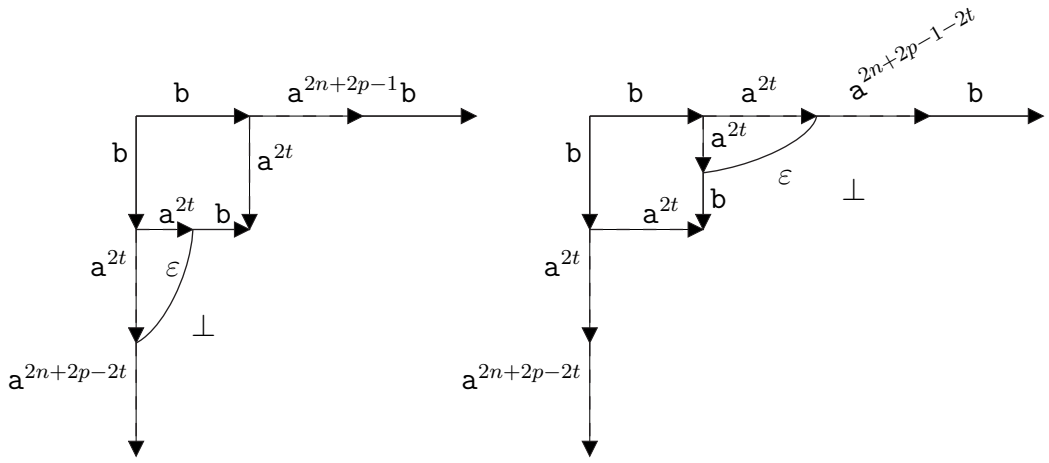


FIGURE 12 – Lors de l'exécution de l'algorithme 5.1, on est amenés à chercher si $\mathtt{A}^{2n+2p}\mathtt{Bba}^{2n+2p-1}\mathtt{b}$ peut se retourner en le mot vide ε en utilisant les relations de la forme $\mathtt{ba}^{2k-1}\mathtt{b} = \mathtt{ba}^{2k}$, avec $k \leq m$ et $p, n \leq m$. Avec $n + p < m$, il est clair que le retournement en le mot vide est possible puisque $\mathtt{ba}^{2n+2p} = \mathtt{ba}^{2n+2p-1}\mathtt{b}$ est une relation. En revanche, si on a $n + p \geq m$ alors le diagramme montre que ce n'est pas possible.

gauche revient à trouver une relation $su = sv$ dans $\mathcal{R}$ pour laquelle on n'a pas $u^{-1}v \curvearrowright_{\mathcal{R}} \varepsilon$, c'est-à-dire, la présentation étant R-complète, une relation $su = sv$ pour laquelle on n'a pas $u \equiv_{\mathcal{R}} v$. Ceci signifie que s'il y a une obstruction à la simplifiabilité, alors elle apparaît déjà dans les relations de la présentation dès que celle-ci est R-complète.

Exemple 6.2. Pour un n fixé, considérons la présentation d'Artin standard de B_n^+. On a montré à l'exemple 4.8 que cette présentation était R-complète. Comme de plus elle est complémentée, il n'y a pas de relation $su = sv$ et on déduit de la proposition 6.1 que le monoïde B_n^+.

Dans le chapitre II, on sera amenés à calculer de nombreuses R-complétions. Toutes les R-complétions infinies, c'est-à-dire des présentations dont l'ensemble des relations est infini, auront la particularité d'être associées à des monoïdes non simplifiables à gauche. Cette remarque mène à la question de savoir si cette situation est générale. Il ne semble pas qu'il y ait dans la littérature d'exemple de présentation de monoïde étudiée du point de vue du retournement possédant à la fois une R-complétion infinie et la propriété d'être simplifiable à gauche. Nous montrons avec la proposition suivante qu'il existe une telle présentation.

Proposition 6.3. *Il existe une présentation de monoïde finie admettant une R-complétion infinie et dont lem monoïde associé est simplifiable à gauche.*

Démonstration. Soit la présentation

$$(2) \qquad (\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d};\ \mathtt{ab}=\mathtt{bac},\mathtt{bc}=\mathtt{cbd},\mathtt{da}=\mathtt{ad},\mathtt{bd}=\mathtt{db},\mathtt{dc}=\mathtt{cd}).$$

Notons $\sharp_{\mathtt{a}<\mathtt{b}}(u)$ (resp. $\sharp_{\mathtt{b}<\mathtt{a}}(u)$) le nombre de paires (i,j) avec $i<j$ telles que la $i^{\text{ème}}$ lettre de u soit un $\mathtt{a}$ (resp. $\mathtt{b}$) et la $j^{\text{ème}}$ lettre soit un $\mathtt{b}$ (resp. $\mathtt{a}$). On définit λ sur l'ensemble des mots comme suit :

$$\lambda(u) = |u| + 2\sharp_{\mathtt{a}<\mathtt{b}}(u) + \sharp_{\mathtt{b}<\mathtt{a}}(u).$$

On vérifie sur les relations de (2) que λ est une pseudolongueur. L'exécution de l'algorithme 5.1 calcule la R-complétion

$$\{\mathtt{ab}=\mathtt{bac},\mathtt{bc}=\mathtt{cbd},\mathtt{da}=\mathtt{ad},\mathtt{bd}=\mathtt{db},\mathtt{dc}=\mathtt{cd}\}\cup\{\mathtt{b}(\mathtt{ac})^n\mathtt{c}=\mathtt{da}^n\mathtt{cb};n\geq 0\},$$

qui est infinie. Finalement, comme il n'y a aucune relation de la forme $s\ldots=s\ldots$ dans la présentation (2), la proposition 6.1 permet de conclure que le monoïde associé est simplifiable à gauche.

la présentation (2) est R-complète à gauche. En employant la version de la proposition 6.1 pour le retournement à gauche, on conclut à la R-complétude à gauche de la présentation et donc à la simplifiabilité à droite. □

6.2 EXISTENCE ET CALCUL DE PPCM

Nous illustrons dans cette section une autre application du retournement : le calcul des ppcm. Avec la proposition 1.5 nous avons vu que le retournement calculait des multiples communs à droite (lorsqu'ils existent). Parmi les multiples communs (à droite) de deux éléments, il est naturel de considérer, s'il existe, le plus petit vis-à-vis de la divisibilité, celui qu'on l'appelle le *ppcm*. Plus formellement, on a la définition :

Définition 6.4 (divisibilité, ppcm)**.** Soit M un monoïde. Soient x et y deux éléments de M. On dit que x *divise à gauche* (resp. à droite) y s'il existe un élément z de M vérifiant $y=xz$ (resp. $y=zx$). On dit qu'un élément z de M est le *ppcm à droite* de x et y dans M si tout multiple commun de x et y est divisible à gauche par z.

La proposition suivante donne des conditions suffisantes pour que le monoïde associé à une présentation de monoïde admette des ppcm. De plus, dans ce cas, le retournement calcule les ppcm.

Proposition 6.5 ([13, Prop. 2.16])**.** *Soit M un monoïde associé à une présentation $(\mathcal{S};\mathcal{R})$ complémentée et R-complète. Soient u et v des mots sur $\mathcal{S}$. Alors les conditions suivantes sont équivalentes :*

- *Le mot $u\backslash_{\mathcal{R}}v$ existe.*

- *Les éléments $\overline{u}$ et $\overline{v}$ admettent un multiple commun à droite.*

Si ces conditions sont vérifiées, les éléments $\overline{u}$ et $\overline{v}$ admettent dans M un (unique) plus petit commun multiple représenté par $u(u\backslash_{\mathcal{R}}v)$ et $v(v\backslash_{\mathcal{R}}u)$.

Démonstration. Supposons que $u\backslash_{\mathcal{R}}v$ existe. Alors on a $u(u\backslash_{\mathcal{R}}v) \equiv_{\mathcal{R}} v(v\backslash_{\mathcal{R}}u)$, ce qui implique une égalité du type $\overline{u}a = \overline{v}b$ dans M, avec a et b des éléments de M. Réciproquement, supposons que $\overline{u}$ et $\overline{v}$ possèdent un multiple commun dans M. Alors il existe deux mots u' et v' sur $\mathcal{S}$ pour lesquels on a $uv' \equiv_{\mathcal{R}} vu'$. Comme le retournement associé à $(\mathcal{S};\mathcal{R})$ est complet, on a $(uv')^{-1}vu' \curvearrowright_{\mathcal{R}} \varepsilon$ et donc $(uv')\backslash_{\mathcal{R}}(vu')$ et $u\backslash_{\mathcal{R}}v$ aussi. De plus, du retournement $v'^{-1}u^{-1}vu' \curvearrowright_{\mathcal{R}} v'^{-1}(u\backslash_{\mathcal{R}}v)(v\backslash_{\mathcal{R}}u)^{-1}u'$ et du lemme 1.4 on déduit l'existence de deux mots w' et w'' vérifiant $v' \equiv_{\mathcal{R}} (u\backslash_{\mathcal{R}}v)w'$, $u' \equiv_{\mathcal{R}} (v\backslash_{\mathcal{R}}u)w''$ et $w' \equiv_{\mathcal{R}} w''$. Ceci signifie que $\overline{vu'}$ est un multiple commun à droite de $\overline{u}(u\backslash_{\mathcal{R}}v)$. □

Les présentations d'Artin-Tits standard des groupes de tresses vérifient les hypothèses de la proposition 6.5. Le retournement calcule donc le ppcm de deux mots de tresse. Mais toutes les présentations n'admettent pas des ppcm. Il se peut en effet qu'il y ait plusieurs éléments minimaux, aucun d'entre eux ne divisant aucun des autres.

Définition 6.6 (mcm)**.** Soit M un monoïde. Pour x, y, z dans M, on dit que z est un *multiple commun minimal à droite* (ou *mcm*) de x et y si z est un multiple commun à droite de x et y mais qu'aucun diviseur à gauche propre de z (c'est-à-dire différent de 1 et z) n'en est un.

Dans le cas où un monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$ n'admet pas de ppcm mais uniquement des mcm et même si la présentation $(\mathcal{S};\mathcal{R})$ est R-complète, le retournement ne calcule pas nécessairement un mcm. Plus précisément, si la présentation $(\mathcal{S};\mathcal{R})$ est R-complète, alors tous les mcm sont atteints par retournement mais tous les mots atteints par retournement ne sont pas des mcm. Pour illustrer ce phénomène, considérons la présentation homogène et R-complète $(\mathtt{a},\mathtt{b};\mathtt{ab}=\mathtt{ba},\mathtt{a}^2=\mathtt{b}^2)$. Le mot $\mathtt{Ab}^2$ se retourne en $\mathtt{b}^2\mathtt{A}$ mais $\mathtt{ab}^2$ ne représente pas un mcm de $\overline{\mathtt{a}}$ et $\overline{\mathtt{b}^2}$ puisque $\overline{\mathtt{a}}$ divise à droite $\overline{\mathtt{a}}$ et $\overline{\mathtt{b}^2}$.

CHAPITRE II

BASES DE GRÖBNER

Dans ce chapitre, nous expliquons comment adapter aux monoïdes présentés le vocabulaire et les résultats classiques de la théorie des bases de Gröbner — dont les algèbres constituent le cadre naturel. Puis nous analysons sur de nombreuses présentations de monoïde les bases de Gröbner et les complétions par retournement qu'on obtient.

La théorie des bases de Gröbner — aussi appelées bases de Gröbner-Shirshov — est une théorie qui naît dans la deuxième moitié du XX^{e} siècle dans trois contextes différents : Buchberger [8] dans le cadre de l'algèbre commutative, Shirshov [25] dans le milieu des algèbres de Lie et Hironaka [21] en géométrie algébrique. Dans les trois cas, le problème motivant était d'ordre calculatoire. Pour Buchberger par exemple, étant donnée une algèbre commutative libre $\mathcal{A}$ et un idéal I de $\mathcal{A}$, il introduit les bases de Gröbner pour répondre à la question de l'appartenance d'un élément de $\mathcal{A}$ à I.

L'extension du cadre originel des algèbres commutatives de Buchberger à celui plus large des algèbres libres [22] permet, via le plongement du monoïde libre de base $\mathcal{S}$ dans une algèbre libre de base $\mathcal{S}$ de développer la théorie en direction des monoïdes [24].

Étant donné un idéal présenté I d'une algèbre $\mathcal{A}$— c'est-à-dire qu'on donne une famille génératrice $\mathcal{F}$ de I —, calculer une base de Gröbner pour cet idéal consiste à construire un ensemble par ajouts d'éléments à $\mathcal{F}$ de telle sorte que tout élément de l'idéal s'exprime comme combinaison $\mathcal{A}$-linéaire des éléments de la famille $\mathcal{F}$ « augmentée ».

Après transport au contexte des monoïdes, la construction d'une base de Gröbner revient au procédé itératif suivant : partant de l'ensemble des relations d'une présentation, on construit une relation qu'on ajoute à la liste des relations si une condition de divisibilité n'est pas vérifiée. Dans le vocabulaire des algèbres, cela signifie qu'on a formé un élément de l'idéal qui ne s'exprime pas comme combinaison $\mathcal{A}$-linéaire d'éléments de la famille generatrice de I, éventuellement augmentée d'éléments de I aux étapes précédentes.

Ce moyen de compléter une structure présentée initialement incomplète par des éléments qui sont conséquences des éléments initiaux, qu'on appellera G-complétion, est parallèle à la technique de R-complétion du chapitre I. On décrit des exemples pour lesquels

les deux complétions coïncident, ce qui conduit à conjecturer qu'au moins pour des classes importantes, la R-complétion et la G-complétion sont les mêmes.

Le but de ce chapitre est de réfuter cette conjecture. On montre (proposition 4.1) :

> **Proposition :** *Chacune des situations suivantes est possible : il existe des présentations de semigroupe $(\mathcal{S}, \mathcal{R})$ telles que*
>
> (i) *la R-complétion et la G-complétion coïncident,*
>
> (ii) *la R-complétion est strictement incluse dans la G-complétion,*
>
> (iii) *la G-complétion est strictement incluse dans la R-complétion,*
>
> (iv) *la R-complétion et la G-complétion ne sont pas comparables pour l'inclusion.*

Le chapitre est organisé comme suit. On rappelle à la section 1 le cadre usuel des bases de Gröbner non commutatives. Dans la section 2, on définit dans le langage des monoïdes tous les concepts relatifs aux bases de Gröbner en s'appuyant largement sur les définitions issues du cadre classique. Dans la section 3, on montre que la base de Gröbner et la R-complétion de la présentation de monoïde traitée au chapitre I coïncident. Puis nous énonçons et prouvons le résultat principal du chapitre à la section 4. On conclut le chapitre par la section 5. On y montre ce que les bases de Gröbner apportent au problème de la simplification d'un monoïde avec un parallèle avec les présentations R-complètes.

1 BASES DE GRÖBNER — CAS DES ALGÈBRES LIBRES

Nous rappelons les principaux résultats concernant la construction des bases de Gröbner dans le cadre des algèbres libres. On se reportera à [22, 27, 24, 6] pour plus de détails. Pour ce chapitre, K désigne un corps.

Définition 1.1. Soit M un monoïde. On dit qu'un ordre $<$ sur M est *admissible* si

- $<$ est un ordre total ;
- $<$ est un bon ordre ;
- $<$ est compatible avec la loi de M.

On rappelle qu'un ordre $<$ sur un ensemble E est *total* (ou *linéaire*) si les éléments de E sont comparables deux à deux ; autrement dit, pour tous x, y distincts de E, on a soit $x < y$ soit $y < x$. On dit que $<$ est un *bon ordre* si toute partie de E admet un plus petit élément. En particulier, il n'y a pas de suites infinies décroissantes d'éléments de E qui ne soient pas ultimement stationnaires. Si M est un monoïde, dire que l'ordre $<$ est *compatible* avec la loi de M signifie qu'on a

$$(\forall f, g \in M)(\ f < g \implies (\forall u, v \in M)(ufv < ugv)).$$

Remarque 1.2. De tels ordres existent. Soit $\mathcal{S}$ un ensemble fini. On appelle *degré* (et on note $\deg(.)$) ou *longueur* (et on note $|.|$) d'un mot ou d'un monôme écrit sur $\mathcal{S}$, le nombre de lettres nécessaires à son écriture. Autrement dit, en posant $w = w_1 \dots w_p$, avec $w_1, \dots, w_p$ dans $\mathcal{S}$, on a $|w| = \deg(w) = p$. Tout ordre total $<$ sur un alphabet fini $\mathcal{S}$ induit un ordre $<$ sur l'ensemble des mots $\mathcal{S}^*$, qu'on appelle *ordre du degré lexicographique*, et souvent, *deglex*, qu'on note encore $<$ et qu'on définit récursivement comme suit : si on a $u = u_1 \dots u_n$ et $v = v_1 \dots v_p$ avec u_i, v_j des lettres de $\mathcal{S}$, alors on a

$$u < v \iff \begin{cases} n < p, \text{ ou} \\ n = p \text{ et } u_2 \dots u_n < v_2 \dots v_p. \end{cases}$$

C'est un exercice simple de montrer que l'ordre du degré lexicographique est un ordre admissible.

Si $\mathcal{S}$ est un ensemble (fini), on note $K\langle\mathcal{S}\rangle$ l'algèbre libre de base $\mathcal{S}$. L'ensemble des monômes de $K\langle\mathcal{S}\rangle$ muni de la multiplication des monômes forme un monoïde libre de base $\mathcal{S}$. À partir de maintenant, on fixe un ordre admissible $<$ sur l'ensemble des monômes $\mathcal{S}^*$. À tout polynôme u de $K\langle\mathcal{S}\rangle$ on associe son plus grand monôme $\hat{u}$ et on étend l'ordre total sur les monômes à un ordre partiel sur $K\langle\mathcal{S}\rangle$ par $u < v \Leftrightarrow \hat{u} < \hat{v}$.

Définition 1.3 (base de Gröbner)**.** Soit I un idéal bilatère de l'algèbre $K\langle\mathcal{S}\rangle$. Un ensemble de polynômes $\mathcal{B}$ dans I est une *base de Gröbner* de I si, pour tout polynôme u de I, il existe un polynôme b de $\mathcal{B}$ tel que $\hat{b}$ soit un sous-mot de $\hat{u}$.

Construire une base de Gröbner repose sur les trois opérations suivantes qu'on itère jusqu'à ce qu'une certaine condition d'arrêt soit vérifiée — ce qui n'est pas nécessairement le cas :

- La *normalisation* : normaliser un polynôme u consiste à le remplacer par l'unique polynôme unitaire proportionnel à u. Normaliser l'ensemble E consiste à normaliser chaque polynôme de E.
- La *réduction* : soient deux polynômes unitaires u et v tels qu'on ait $\hat{u} = g\hat{v}h$, où g et h sont deux monômes. Si on a $u = \hat{u} - u'$ et $v = \hat{v} - v'$, réduire u par v consiste à remplacer u par le polynôme unitaire proportionnel à $gv'h - u'$. Réduire un ensemble E consiste à effectuer toutes les opérations de réduction possibles.
- La *composition* : deux polynômes unitaires u et v sont composables si un suffixe de $\hat{u}$ est également un préfixe de $\hat{v}$, autrement dit, s'il existe un chevauchement entre les mots $\hat{u}$ et $\hat{v}$. Soit y un de ces chevauchements. Il existe donc x et z des monômes tels qu'on ait $\hat{u} = xy$ et $\hat{v} = yz$. Posons $u = \hat{u} - u'$ et $v = \hat{v} - v'$. Le resultat de la composition de u et v au-dessus de y est le polynôme $xv' - u'z$. Remarquons que deux polynômes unitaires peuvent avoir plusieurs compositions différentes.

Algorithme 1.4 (construction d'une base de Gröbner)**.**
ENTRÉE : *Un ensemble de polynômes* E.

0. Poser $i = 0$ et $\mathcal{U}_i$ le normalisé de E ;
1. Réduire $\mathcal{U}_i$;
2. `SI` *il existe une composition dans $\mathcal{U}_i$*
`ALORS` *Poser $\mathcal{U}_{i+1} = \mathcal{U}_i \cup \{$la composition$\}$;*
Incrémenter i et retour à l'étape 1 ;
`SINON` *Renvoyer $\mathcal{U}_i$.*

`SORTIE` : *Un ensemble de polynômes $\mathcal{U}_i$.*

Proposition 1.5 ([27, p. 30])**.** *Soit $\mathcal{A}$ une algèbre libre $K\langle\mathcal{S}\rangle$ de base $\mathcal{S}$. Soit I un idéal bilatère présenté par $(P_1, P_2, \ldots, P_n)$ et notons E l'ensemble $\{P_i; 1 \leq i \leq n\}$. Si E est l'entrée de l'algorithme 1.4 et qu'il termine, alors sa sortie est une base de Gröbner de I.*

2 BASES DE GRÖBNER — CAS DES MONOÏDES

2.1 ADAPTATION AUX MONOÏDES

Dans cette section, on se concentre sur l'application aux monoïdes des techniques habituellement utilisées dans des contextes algébriques plus généraux (voir section 1). Pour tout ce qui concerne les présentations de monoïde, on réutilise les notations définies à la section I.1.1.

Les résultats permettant d'adapter les techniques classiques de Gröbner au cas particulier des monoïdes ne sont pas compliqués. On trouve des allusions dans [22] et ils sont explicitement mentionnés dans [20]. On les rappelle ici sans preuves. La première proposition constitue la première étape pour adapter au cadre des monoïdes la machinerie usuelle de Gröbner : les égalités dans le monoïde présenté $\langle\mathcal{S};\mathcal{R}\rangle^+$ correspondent aux égalités de monômes dans un certain quotient $K\langle\mathcal{S}\rangle/I_{\mathcal{R}}$.

Proposition 2.1. *Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. Soit $I_{\mathcal{R}}$ l'idéal bilatère de l'algèbre libre $K\langle\mathcal{S}\rangle$ engendré par les relations (u, v) de $\mathcal{R}$. Alors, pour tous mots w, w' sur $\mathcal{S}$, les propriétés suivantes sont équivalentes :*
(i) $w \equiv w'$ *;*
(ii) $w - w' \in I_{\mathcal{R}}$.

Le lemme suivant établit que si un idéal est engendré par une liste de générateurs d'un certain type, à savoir des différences de monômes, alors l'algorithme classique de calcul de base de Gröbner n'ajoute que des générateurs de la même forme, donc des différences de monômes.

Lemme 2.2. *Soit I l'idéal bilatère de l'algèbre $K\langle\mathcal{S}\rangle$ engendré par $u_1 - v_1, \ldots, u_p - v_p$, avec les u_i et v_i des mots de $\mathcal{S}^*$. Alors les éléments calculés par l'algorithme 1.4 sont encore du type $u - v$, avec u et v dans $\mathcal{S}^*$.*

Ainsi, au cours du calcul (au moyen de l'algorithme 1.4) de la base de Gröbner d'un idéal engendré par des différences de monômes, les éléments qu'on est amenés à insérer dans la liste des générateurs de l'idéal sont des différences de monômes. Par la proposition 2.1, ces différences de monômes correspondent à des égalités dans le monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$, avec $\mathcal{R} = \{(u_1, v_1), \ldots, (u_p, v_p)\}$, ou encore à des mots $\mathcal{R}$-équivalents sur $\mathcal{S}$. En d'autres termes, la proposition 2.1 et le lemme 2.2 affirment que l'utilisation et la construction d'une base de Gröbner peuvent se faire directement au niveau d'un monoïde dès que l'idéal considéré est un idéal $I_{\mathcal{R}}$, avec $\mathcal{R}$ un ensemble de relations d'une présentation de monoïde $(\mathcal{S};\mathcal{R})$. Afin de ne plus du tout dépendre d'une algèbre dans laquelle on plonge le monoïde — le corps K est en effet superflu dans le cadre particulier des monoïdes —, on redéfinit les opérations nécessaires au calcul des bases de Gröbner dans le cas particulier des monoïdes.

Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. Du fait que $\mathcal{R}$ soit un ensemble de relations, si (w, w') est une relation, alors (w', w) est également une relation. Toutefois, l'introduction d'un ordre sur les mots implique que les relations sont orientables. On notera $w \vec{=} w'$ la relation (w, w') si en plus de $w \equiv_{\mathcal{R}} w'$, on a $w > w'$. Dans ce cas-là, on dira de plus que w est le *mot dominant* de la relation.

Définition 2.3 (réduction d'une relation)**.** Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. Soient les relations (w, w') et $v \vec{=} v'$ satisfaisant $w = v_l v v_d$, avec $v_l, v_d \in \mathcal{S}^*$. Alors la *réduction* de (w, w') par $v \vec{=} v'$ est la relation $(v_l v' v_d, w')$. On dit que la relation (w, w') *se réduit à* 0 par rapport à l'ensemble de relations $\mathcal{R}$, ou simplement, lorsque l'ensemble de relations est clair, que (w, w') se réduit à 0, s'il existe une suite de relations $(w, w') = (w_0, w'_0), \ldots, (w_n, w'_n) = (u, u)$ de $\equiv$ telle que chaque (w_{i+1}, w'_{i+1}) est une réduction de (w_i, w'_i) par une relation (u_i, u'_i) de $\mathcal{R}$.

On notera $(w, w') \rightsquigarrow (v_l v' v_d, w')$ la réduction de (w, w') à $(v_l v' v_d, w')$ avec éventuellement au-dessus du symbole $\rightsquigarrow$ une indication de la relation qui permet la réduction. Dans le cas d'une relation qui se réduit à 0, on conclura la chaîne de réductions par $\rightsquigarrow 0$.

Exemple 2.4. Soit la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{aba})$. Il est nécessaire d'avoir un ordre sur $\{\mathtt{a}, \mathtt{b}\}^*$ pour pouvoir réaliser des réductions. On fixe l'ordre deglex induit par $\mathtt{a} < \mathtt{b}$. Prenons la relation $(\mathtt{baba}, \mathtt{abaa})$ et l'ensemble de relations $\mathcal{R} = \{\mathtt{bab} = \mathtt{aba}\}$. On en déduit, en remplaçant bab par aba, la réduction $(\mathtt{baba}, \mathtt{abaa}) \rightsquigarrow (\mathtt{abaa}, \mathtt{abaa}) \rightsquigarrow 0$. Considérons maintenant la relation $(\mathtt{baaba}, \mathtt{abaab})$ et le même ensemble de relations. Cette relation n'est pas réductible par rapport à $\mathcal{R}$ car ni baaba ni abaab n'admettent bab comme sous-mot. Remarquons que nous n'avons pas prouvé l'équivalence $\mathtt{baaba} \equiv \mathtt{abaab}$ avant d'utiliser $(\mathtt{baaba}, \mathtt{abaab})$ comme une relation. On justifie ce point dans l'exemple 2.10.

Remarque 2.5. On ne peut réduire une relation qu'un nombre fini de fois. En effet, de la réduction $w = w' \rightsquigarrow z = z'$ on déduit l'une des deux inégalités $z < w$ et $z' < w'$. Une infinité de réductions produirait une suite infinie strictement décroissante, ce qui contredirait le fait que l'ordre admissible $<$ est un bon ordre. Lorsque plus aucune relation ne peut réduire une relation, on dit de cette dernière qu'elle est *réduite*.

Définition 2.6 (divisibilité)**.** Soit $\mathcal{R}$ un ensemble de relations. Soient r_1 et r_2 deux relations de $\mathcal{R}$. On dit que r_1 *divise* r_2, ou, de façon équivalente, que r_2 est *divisible* par r_1, si $\hat{r_1}$ est un sous-mot de $\hat{r_2}$. On le note $r_1 \prec r_2$. Plus généralement, on dit que la relation r *divise* l'équivalence $u \equiv_{\mathcal{R}} v$ si $\hat{r}$ est un sous-mot de $\max(u, v)$.

Remarque 2.7. Alors que « être un sous-mot de » est un ordre partiel sur les mots, la relation binaire $\prec$ ne définit pas un ordre partiel sur l'ensemble des relations d'une présentation de monoïde puisque l'antisymétrie n'est pas satisfaite en général : la relation $u \vec{=} v$ divise $u \vec{=} w$ et réciproquement, mais les relations ne sont pas égales si on a $v \neq w$. Toutefois, la relation $\prec$ est réflexive et transitive ; ces propriétés sont facilement déduites de la relation « être un sous-mot de ».

Comme on l'a vu dans la section 1, pour traiter les paires critiques, c'est-à-dire les chevauchements entre termes dominants de deux polynômes, l'algorithme 1.4 réalise des compositions de polynômes. On adapte ici cette définition aux relations.

Définition 2.8 (composition de relations)**.** Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde et soient $w \vec{=} w'$ et $v \vec{=} v'$ des relations dans $\mathcal{R}$ telles que w et v se chevauchent, c'est-à-dire telles qu'on ait $w = xy$ et $v = yz$, avec x, y, z des mots sur $\mathcal{S}$ et y non vide. La *composition* de $w \vec{=} w'$ et $v \vec{=} v'$ avec chevauchement y est l'élément $(xv', w'z)$ de $\mathcal{S}^* \times \mathcal{S}^*$.

Fait 2.9. *La composition de deux éléments de $\equiv$ est un élément de $\equiv$.*

Démonstration. En reprenant les notations de la définition 2.8, on veut montrer $xv' \equiv_{\mathcal{R}} w'z$. On a $xv' \equiv_{\mathcal{R}} xv = xyz = wz \equiv_{\mathcal{R}} w'z$. □

En d'autres termes, lorsqu'on a deux relations de $\equiv$ on peut en créer une troisième par composition. Pour réaliser le calcul de composition de deux relations de la présentation $(\mathcal{S}; \mathcal{R})$, on préférera souvent le réaliser comme on le ferait dans l'algèbre correspondante $K\langle\mathcal{S}\rangle/I_{\mathcal{R}}$, et donc en traitant les relations comme des différences de monômes, ce qui est équivalent d'après la proposition 2.1. Pour calculer la composition de $xy =_{\mathcal{R}} w'$ et $yz =_{\mathcal{R}} v'$ avec chevauchement y, on écrit

$$(wy - w')z - x(yz - v') = xv' - w'z$$

et on en déduit que le résultat de composition est $(xv', w'z)$. On ne sait pas *a priori* si on a $xv' < w'z$ ou l'inégalité inverse $w'z < xv'$.

Exemple 2.10. Soit la présentation $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{aba})$ et l'ordre deglex induit par $a<b$. Composons la relation $\mathtt{bab}\vec{=}\mathtt{aba}$ avec elle-même au-dessus de $\mathtt{b}$. On trouve

$$(\mathtt{bab}-\mathtt{aba})\mathtt{ab}-\mathtt{ba}(\mathtt{bab}-\mathtt{aba})=\mathtt{baaba}-\mathtt{abaab}.$$

Le résultat de composition est donc la relation $(\mathtt{baaba},\mathtt{abaab})$. On justifie ainsi *a posteriori* l'emploi de cette relation dans l'exemple 2.4.

2.2 BASES DE GRÖBNER

On donne maintenant la définition d'une base de Gröbner dans le cadre des monoïdes.

Définition 2.11 (base de Gröbner et G-complétude)**.** Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde. Un sous-ensemble $\mathcal{B}$ de la congruence $\equiv$ engendrée par $\mathcal{R}$ est une *base de Gröbner* de la présentation $(\mathcal{S};\mathcal{R})$ si tout élément (u,v) de $\mathcal{B}$ vérifie $u>v$ et si, pour toute paire de mots équivalents w,w' de $\mathcal{S}^*$ avec $w>w'$, il existe un élément (u,v) de $\mathcal{B}$ tel que u soit un sous-mot de w. Si $\mathcal{R}$ est une base de Gröbner de $(\mathcal{S};\mathcal{R})$, on dit que $(\mathcal{S};\mathcal{R})$ est *G-complète*.

Remarque 2.12. Comme le montre l'exemple 2.4, toutes les présentations ne sont pas G-complètes : bien qu'on ait $\mathtt{baaba}\equiv_{\mathcal{R}}\mathtt{abaab}$, le seul élément de $\mathcal{R}$, à savoir $\mathtt{bab}=\mathtt{aba}$, ne divise pas $\mathtt{baaba}\vec{=}\mathtt{abaab}$. L'ensemble de relations $\mathcal{R}$ n'est donc pas une base de Gröbner pour cette présentation. Supposons qu'on ajoute cette relation à l'ensemble $\mathcal{R}$. On a alors la nouvelle présentation

$$(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{aba},\mathtt{baaba}=\mathtt{abaab}). \tag{1}$$

Cette présentation présente le même monoïde que précédemment, à savoir B_3^+, le monoïde de tresses à trois brins. La question naturelle est de savoir si cette présentation « augmentée » est G-complète. D'après la définition 2.11, il s'agit de vérifier que toute relation $u\vec{=}v$ vérifiée dans (1) est divisible soit par $\mathtt{bab}\vec{=}\mathtt{aba}$ soit par $\mathtt{baaba}\vec{=}\mathtt{abaab}$. Ceci n'est pas une solution viable algorithmiquement.

Malgré tout, pour chaque présentation il existe une base de Gröbner. Il suffit de compléter l'ensemble des relations d'une présentation $(\mathcal{S};\mathcal{R})$ avec toutes les égalités $u\vec{=}v$ vérifiées dans le monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$. L'ensemble étendu obtenu est alors une base de Gröbner puisque toute relation est au moins divisible par elle-même mais l'intérêt pratique d'une telle base est très faible dans la mesure où pour la construire il faut connaître une solution au problème du mot. En outre, cette base de Gröbner présente une redondance très élevée dans le sens où la présence de la relation $u\vec{=}v$ dans la base entraîne la présence de $wu\vec{=}wv$ pour tout mot w. Or cette dernière relation est réductible (à 0) par $u\vec{=}v$, autrement dit, sa présence dans la base ne change rien au fait d'être une base de Gröbner ou non.

Toutefois, nous allons voir par la suite que l'algorithme 2.22 résout ces deux problèmes : pour fonctionner, l'algorithme ne nécessite pas de solution au problème de mot associé à la

présentation, et s'il termine, il renvoie une base de Gröbner de laquelle toute la redondance mentionnée plus haut a disparu.

Définition 2.13 (ensemble réduit)**.** Un ensemble de relations est *réduit* si toute relation de l'ensemble est réduite par rapport à toutes les autres.

L'ensemble $\{\texttt{bab} = \texttt{aba}, \texttt{baaba} = \texttt{abaab}\}$ est réduit car le mot bab n'est sous-mot ni de baaba ni de abaab et symétriquement, baaba n'est sous-mot ni de bab ni de aba. Ce n'est pas le cas en revanche des ensembles de relations $\{\texttt{bab} = \texttt{aba}, \texttt{baba} = \texttt{abaa}\}$ et $\{\texttt{bab} = \texttt{aba}, \texttt{baaba} = \texttt{babab}\}$. Dans le premier cas, bab est un sous-mot de baba ; dans le deuxième cas, bab est un sous-mot de babab.

Remarque 2.14. Un ensemble de relations dans lequel au moins deux relations ont le même mot dominant, n'est pas réduit. Soient $u \vec{=} v$ et $u \vec{=} w$ deux relations avec $v > w$. La réduction de $u \vec{=} v$ par $u \vec{=} w$ donne $v \vec{=} w$. Ces deux relations ne se réduisent plus entre elles. Leurs mots dominants sont différents.

Fait 2.15. *La relation binaire $\prec$ sur un ensemble de relations réduit est un ordre partiel.*

Démonstration. D'après la remarque 2.14, deux relations d'un ensemble réduit ne peuvent avoir le même mot dominant, d'où l'antisymétrie de la relation. De plus, d'après la remarque 2.7, la relation $\prec$ est également transitive et réflexive. □

Tester si un ensemble (fini) est réduit est algorithmiquement aisé. Donc étant donnée une base de Gröbner (finie), on peut vérifier qu'elle constitue un ensemble réduit.

Fait 2.16. *La réduction d'une base de Gröbner est une base de Gröbner.*

Démonstration. Supposons qu'une base de Gröbner $\mathcal{B}$ ne soit pas réduite. Il existe alors deux relations r_1, r_2 de $\mathcal{B}$ avec $r_2 \prec r_1$ et, par transitivité, toute équivalence que divise r_1 est divisible par r_2. □

On appelle *base de Gröbner réduite* une base de Gröbner qui en tant qu'ensemble de relations est réduit.

Proposition 2.17. *Une base de Gröbner réduite est unique.*

Démonstration. Soient $\mathcal{B}_u = \{u_1 \vec{=} u'_1, \ldots, u_p \vec{=} u'_p\}$ et $\mathcal{B}_v = \{v_1 \vec{=} v'_1, \ldots, v_n \vec{=} v'_p\}$ deux bases de Gröbner réduites d'une présentation $(\mathcal{S}; \mathcal{R})$. On va montrer l'inclusion $\mathcal{B}_u \subset \mathcal{B}_v$, l'inclusion inverse se montrant de la même manière. Comme $\mathcal{B}_v$ est une base de Gröbner, la relation $u_1 \vec{=} u'_1$ est divisible par la relation $v_i \vec{=} v'_i$ pour un certain i. Mais $\mathcal{B}_u$ est une base de Gröbner, donc la relation $v_i \vec{=} v'_i$ est divisible par la relation $u_j \vec{=} u'_j$ pour un certain j. Par transitivité, on en déduit que $u_j \vec{=} u'_j$ divise $u_1 \vec{=} u'_1$. Or $\mathcal{B}_u$ est réduite donc nécessairement on a $j = 1$ et donc $u_1 = v_i$. On a donc les équivalences de mots $u'_1 \equiv_{\mathcal{R}} u_1 = v_i \equiv_{\mathcal{R}} v'_i$, d'où

la relation $u'_1 = v'_i$. Si u'_1 et v'_i sont disctincts, alors la relation est réductible par chacune des bases de Gröbner, ce qui contredit le fait qu'on les a supposées réduites. Donc on a $u'_1 = v'_i$ et donc $u_1 \vec{=} u'_1 \in \mathcal{B}_v$. Un raisonnement identique sur les autres éléments de $\mathcal{B}_u$ montre $\mathcal{B}_u \subset \mathcal{B}_v$ □

2.3 DÉTECTION D'UNE BASE DE GRÖBNER

Donc pour obtenir une base de Gröbner réduite à partir d'une base de Gröbner, il suffit de la réduire. Quel que soit l'ordre des réductions, l'ensemble terminal sera l'unique base de Gröbner réduite de la présentation considérée. Mais cela ne répond pas au problème soulevé plus haut de déterminer si un ensemble donné est une base de Gröbner d'une présentation donnée. La proposition suivante nous donne un critère.

Proposition 2.18 (Diamond Lemma)**.** *Soient $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde et $\mathcal{U}$ un ensemble vérifiant $\mathcal{R} \subseteq \mathcal{U} \subseteq \equiv$. Si $\mathcal{U}$ est réduit et si toutes les compositions de relations de $\mathcal{U}$ se réduisent à 0, alors $\mathcal{U}$ est la base de Gröbner réduite de $(\mathcal{S}; \mathcal{R})$.*

Le résultat n'est qu'une récriture du Lemma on Composition de [27, p. 30] adaptée au cadre des monoïdes par la proposition 2.1.

Il est maintenant clair qu'on peut reconnaître si un ensemble de relations est une base de Gröbner : il suffit de réaliser toutes les compositions possibles et de vérifier qu'elles se réduisent bien toutes à 0.

Exemple 2.19. Soit la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{aba}, \mathtt{baaba} = \mathtt{abaab})$. On a vu plus haut qu'elle était réduite. On a également vu que l'ensemble $\{\mathtt{bab} = \mathtt{aba}\}$ sans la relation $\mathtt{baaba} = \mathtt{abaab}$ n'était pas G-complet. Pour vérifier la G-complétude on a vu plus haut qu'il nous fallait tester toutes les relations, ce qui n'était pas algorithmiquement raisonnable. Maintenant, par la proposition 2.18, il suffit de tester que toutes les compositions se réduisent à 0. Composons $\underline{\mathtt{ba}}b \vec{=} \mathtt{aba}$ avec $\mathtt{baa}\underline{\mathtt{ba}} \vec{=} \mathtt{abaab}$ au-dessus de $\mathtt{ba}$. On trouve

$$(\mathtt{baaba} - \mathtt{abaab})\mathtt{b} - \mathtt{baa}(\mathtt{bab} - \mathtt{aba}) = \mathtt{baaaba} - \mathtt{abaabb}.$$

La relation $\mathtt{baaaba} \vec{=} \mathtt{abaabb}$ n'est divisible par aucune relation de $\mathcal{R}$ donc la présentation n'est pas G-complète. Un réflexe naturel est d'ajouter cette relation à la présentation. Non seulement cela engendre le même monoïde mais en plus on a retiré des obstructions, puisque désormais de nouvelles relations sont réductibles par le nouvel ensemble de relations de la nouvelle présentation.

2.4 CONSTRUCTION D'UNE BASE DE GRÖBNER

La proposition 2.18 donne le critère d'arrêt de l'algorithme de construction de base de Gröbner qu'on présentera précisément plus loin (algorithme 2.22). L'idée pour réaliser cet

algorithme est de suivre l'idée de l'exemple 2.19 en ajoutant successivement les résultats de compositions d'éléments de l'ensemble des relations. Le but de cette procédure, quand on l'itère, est de rendre confluent le graphe orienté des réductions issues d'un mot. C'est-à-dire que quelles que soient les réductions successives qu'on réalise à partir d'un mot, on veut obtenir un unique mot terminal, mot qu'on qualifiera de *réduit*.

Pour rendre le processus de réduction confluent, l'algorithme 2.22 force la confluence. En effet, le problème vient de ce qu'il n'y a pas nécessairement une seule façon de réduite un mot. On peut donc avoir $w \rightsquigarrow v$ et $w \rightsquigarrow v'$, avec w, v, v' des mots distincts. Forcer la confluence revient donc à ajouter la relation $v \vec{=} v'$ ou $v' \vec{=} v$. Pour créer des ambiguïtés, c'est-à-dire des mots qu'on peut réduire de deux façons différentes, l'algorithme 2.22 compose des relations, c'est-à-dire qu'il crée effectivement un mot qui a deux réductions différentes, et ajoute, le cas échéant, le résultat de la composition à l'ensemble des relations (voir figure 1).

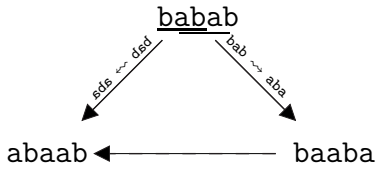


FIGURE 1 – Le mot babab est réductible de deux façons différentes par la relation bab$\vec{=}$aba. En effet, deux motifs bab se chevauchent donnant lieu à une ambiguïté. Pour lever cette ambiguïté, on pose la nouvelle relation baaba$\vec{=}$abaab de telle sorte que quelle que soit la réduction qu'on applique en premier à babab, il existe toujours une suite de réductions qui arrive à abaab. On rend ainsi le processus de réduction confluent.

Pour rendre l'algorithme de calcul de base de Gröbner déterministe, on fixe un ordre total sur les paires de relations afin de pouvoir décider quelle composition effectuer lorsque plusieurs compositions de relations sont possibles.

Remarque 2.20. Dans la pratique, peu importe l'ordre dans lequel on réalise les compositions, dans la mesure où la base de Gröbner réduite est unique (proposition 2.17).

Lemme 2.21. *Soit donc un ordre admissible $<$ sur un ensemble de mots $\mathcal{S}^*$ et soit $\mathcal{R}$ un ensemble de relations réduit. Soient les relations $u_1 \vec{=} v_1$, $u_2 \vec{=} v_2$, $u_3 \vec{=} v_3$ et $u_4 \vec{=} v_4$. L'ordre $<$ défini sur $\mathcal{R} \times \mathcal{R}$ à partir de l'ordre $<$ sur $\mathcal{S}^*$ par*

$$(u_1 \vec{=} v_1, u_2 = v_2) < (u_3 \vec{=} v_3, u_4 = v_4) \Longleftrightarrow u_1 u_2 < u_3 u_4$$

est total.

Démonstration. On ne prouve que le fait que $<$ est un ordre total. Il s'agit de montrer qu'on ne peut pas avoir $u_1 u_2 = u_3 u_4$ dès qu'on a deux paires de relations $(u_1 \vec{=} v_1, u_2 = v_2)$

et $(u_3 \vec{=} v_3, u_4 = v_4)$ distinctes. D'après la remarque 2.14, on ne peut pas avoir $u_1 = u_3$ et $u_2 = u_4$ donc $u_1u_2 = u_3u_4$ implique que u_1 est un préfixe de u_3 ou la situation inverse. Dans chacun de ces deux cas, cela signifie que l'un est sous-mot de l'autre, ce qui contredit le fait que $\mathcal{R}$ est réduit. □

Il ne reste plus maintenant qu'à décrire précisément l'algorithme. On adapte à notre situation l'algorithme de [27] présenté dans un contexte et un vocabulaire d'algèbres libres.

Algorithme 2.22 (G-complétion)**.**
ENTRÉE : *Une présentation de monoïde* $(\mathcal{S}; \mathcal{R})$.

0. Poser $i = 0$ *et* $\mathcal{U}_i = \mathcal{R}$ *;*
1. Réduire $\mathcal{U}_i$ *;*
2. Supprimer toutes les relations $v = v$ *de* $\mathcal{U}_i$ *;*
3. SI *deux relations de* $\mathcal{U}_i$ *sont composables*
ALORS *Poser* $\mathcal{U}_{i+1} = \mathcal{U}_i \cup \{$*la composition de la plus petite paire composable*$\}$ *;*
Incrémenter i *et retour à l'étape 1 ;*
SINON *Renvoyer* $\mathcal{U}_i$*.*

SORTIE : *Un ensemble de relations* $\mathcal{U}_i$*.*

Remarque 2.23. Afin que l'algorithme 2.22 ne boucle pas en composant toujours la même paire de relations, on déclare que deux relations sont *composables* dans le contexte de cette algorithme si et seulement si leur composition au-dessus d'un motif est réalisable d'une part et si cette composition (mêmes relations, même ordre de composition, même motif) n'a pas déjà été effectuée.

Le résultat est que cet algorithme produit, s'il termine, la base de Gröbner réduite de la présentation de monoïde donnée en entrée.

Proposition 2.24. *Si l'algorithme 2.22 termine, alors l'ensemble de relations produit est la base de Gröbner réduite de la présentation fournie en entrée.*

Démonstration. Il suffit de vérifier que l'ensemble de relations produit vérifie les hypothèses de la proposition 2.18 et de conclure par unicité de la base de Gröbner réduite (proposition2.17). □

Exemple 2.25. Considérons la présentation

$$(\mathtt{a}, \mathtt{b}; \mathtt{aba} = \mathtt{b}^2)$$

et l'ordre deglex induit par $\mathtt{a} < \mathtt{b}$. Calculons la G-complétion de la présentation, c'est-à-dire sa base de Gröbner réduite. On suit l'algorithme 2.22 et on pose $\mathcal{U}_0 = \{\mathtt{aba} = \mathtt{b}^2\}$. La seule composition possible est $\mathtt{aba} \vec{=} \mathtt{b}^2$ avec elle-même au-dessus de $\mathtt{a}$

$$(\mathtt{aba} - \mathtt{b}^2)\mathtt{ba} - \mathtt{ab}(\mathtt{aba} - \mathtt{b}^2) = -\mathtt{b}^3\mathtt{a} + \mathtt{ab}^3.$$

On trouve donc par composition la relation $\mathtt{b}^3\mathtt{a} \vec{=} \mathtt{ab}^3$ et on forme

$$\mathcal{U}_1 = \mathcal{U}_0 \cup \{\mathtt{ba}^3 = \mathtt{ab}^3\} = \{\mathtt{aba} = \mathtt{b}^2, \mathtt{b}^3\mathtt{a} = \mathtt{ab}^3\}.$$

Il n'y a aucune réduction à opérer, toutes les relations sont réduites. Il n'y a plus non plus de relations composables donc l'algorithme termine en renvoyant l'ensemble $\mathcal{U}_1$.

Malheureusement, il se peut très bien que l'algorithme 2.22 ne se termine pas. C'est dire donc que parmi les relations qu'on ajoute à l'ensemble qu'on calcule, il y en a toujours qui sont composables avec des relations déjà présentes ou avec elles-mêmes. Le processus est alors sans fin, mais même dans cette situation, il existe des cas où on peut calculer la base de Gröbner réduite de la présentation. En effet, le critère présenté à la proposition 2.18 ne nécessite pas que l'ensemble de relations soit fini. Dans la pratique, l'algorithme 2.22 ne termine pas la plupart du temps, mais il décrit souvent de façon suffisamment précise la base de Gröbner pour qu'on puisse en terminer le calcul sans l'aide de l'algorithme. Nous illustrons cette dernière phrase un peu vague dans la section 3.

3 R-COMPLÉTION ET G-COMPLÉTION ÉGALES

Les deux procédés de R-complétion et G-complétion ajoutent itérativement des relations à une présentation ne vérifiant pas un certain critère de complétude. On a calculé à la section I.5.2 la R-complétion de la présentation de monoïde $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{ba}^2)$. Le but de cette section est de calculer la G-complétion de cette présentation et de montrer qu'elle coïncide avec la R-complétion. Le calcul de la base de Gröbner réduite de cette présentation est également traitée dans [18].

3.1 CALCUL DE LA G-COMPLÉTION

Proposition 3.1. *La G-complétion de la présentation de monoïde* $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{ba}^2)$ *munie de l'ordre deglex induit par* $\mathtt{a} < \mathtt{b}$ *est* $\{\mathtt{ba}^{2n-1}\mathtt{b} = \mathtt{ba}^{2n}; n \geq 2\}$.

Démonstration. Pour calculer la G-complétion de la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{ba}^2)$, on exécute pas à pas l'algorithme 2.22. On ne se soucie pas de l'ordre des compositions (remarque 2.20). On pose $\mathcal{U}_1 = \{\mathtt{bab} = \mathtt{ba}^2\}$, qui est réduit puisqu'il n'y a qu'une seule relation, qu'on appelle (1). Composons (1) avec elle-même :

$$(2) \qquad (\mathtt{bab} - \mathtt{ba}^2)\mathtt{ab} - \mathtt{ba}(\mathtt{bab} - \mathtt{ba}^2) = -\mathtt{ba}^3\mathtt{b} + \mathtt{baba}^2 \overset{(1)}{\rightsquigarrow} -\mathtt{ba}^3\mathtt{b} + \mathtt{ba}^4.$$

Remarquons que la réduction par (1) ne devrait pas avoir lieu dès ici. L'algorithme prévoit qu'on ajoute d'abord la relation issue de la composition, puis qu'on réduise l'ensemble

des relations. On se permet là aussi cet écart sans incidence sur le calcul. On obtient la relation $\mathtt{ba}^3\mathtt{b} \vec{=} \mathtt{ba}^4$ qu'on ajoute à $\mathcal{U}_1$ pour obtenir $\mathcal{U}_2 = \{\mathtt{bab} = \mathtt{ba}^2, \mathtt{ba}^3\mathtt{b} = \mathtt{ba}^4\}$. Toutes les relations de $\mathcal{U}_2$ sont réduites. La composition de (2) avec (1) donne

$$(3) \qquad (\mathtt{ba}^3\mathtt{b} - \mathtt{ba}^4)\mathtt{ab} - \mathtt{ba}^3(\mathtt{bab} - \mathtt{ba}^2) = -\mathtt{ba}^5\mathtt{b} + \mathtt{ba}^3\mathtt{ba}^2 \overset{(2)}{\rightsquigarrow} -\mathtt{ba}^5\mathtt{b} + \mathtt{ba}^6.$$

Ainsi on a $\mathcal{U}_3 = \{\mathtt{bab} = \mathtt{ba}^2\, \mathtt{ba}^3\mathtt{b} = \mathtt{ba}^4, \mathtt{ba}^5\mathtt{b} = \mathtt{ba}^6\}$. Continuer à composer la nouvelle relation avec (1) à chaque nouvelle itération nous mène à considérer l'ensemble de relations infini

$$\mathcal{U}_\infty = \{\mathtt{ba}^{2n-1}\mathtt{b} = \mathtt{ba}^{2n}; n \geq 1\}.$$

Il suffit de voir que la relation (n) composée avec la relation (1) donne la relation $(n+1)$: (n+1)

$$(\mathtt{ba}^{2n-1}\mathtt{b} - \mathtt{ba}^{2n})\mathtt{ab} - \mathtt{ba}^{2n-1}(\mathtt{bab} - \mathtt{ba}^2) = -\mathtt{ba}^{2n+1}\mathtt{b} + \mathtt{ba}^{2n-1}\mathtt{ba}^2 \overset{(n)}{\rightsquigarrow} -\mathtt{ba}^{2n+1}\mathtt{b} + \mathtt{ba}^{2n+2}.$$

Enfin, il suffit de montrer que $\mathcal{U}_\infty$ vérifie les conditions de la proposition 2.18 pour montrer qu'on a obtenu une base de Gröbner réduite. Montrons donc que toutes les compositions de relations de $\mathcal{U}_\infty$ se réduisent à 0. Soient donc deux relations (n) et (p) et composons-les :

$$\begin{aligned}(\mathtt{ba}^n\mathtt{b} - \mathtt{ba}^{n+1})\mathtt{a}^p\mathtt{b} - \mathtt{ba}^n(\mathtt{ba}^p\mathtt{b} - \mathtt{ba}^{p+1}) \quad &= \quad -\mathtt{ba}^{n+1}\mathtt{a}^p\mathtt{b} + \mathtt{ba}^n\mathtt{ba}^{p+1} \\ &\overset{(n)}{\rightsquigarrow} \quad -\mathtt{ba}^{n+1+p}\mathtt{b} + \mathtt{ba}^{n+1}\mathtt{a}^{p+1} \\ &\overset{(n+p+1)}{\rightsquigarrow} \quad -\mathtt{ba}^{n+p+2} + \mathtt{ba}^{n+p+2} = 0.\end{aligned}$$

Toutes les compositions se réduisent à 0 et l'ensemble est réduit : la base de Gröbner réduite de la présentation de monoïde $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{ba}^2)$ est donc $\mathcal{U}_\infty$. □

3.2 ÉGALITÉ DES COMPLÉTIONS

Bien que les opérations constitutives des deux procédés de complétion soient de natures différentes, en combinant les propositions I.5.2 et 3.1 on a :

Fait 3.2. *La R-complétion et la G-complétion de la présentation* $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{ba}^2)$ *coïncident et valent* $\{\mathtt{ba}^{2n-1}\mathtt{b} = \mathtt{ba}^{2n}; n \geq 2\}$.

D'autres présentations simples telles que $(\mathtt{a}, \mathtt{b}; \mathtt{a}^2\mathtt{b} = \mathtt{ba}^2, \mathtt{b}^2\mathtt{a} = \mathtt{ab}^2)$ ou les présentations de type Baumslag-Solitar $(\mathtt{a}, \mathtt{b}; \mathtt{ba} = \mathtt{a}^n\mathtt{b})$ donnent lieu à un phénomène identique d'égalité des complétions. Il en découle la question naturelle suivante.

Question 3.3. *La R-complétion et la G-complétion coïncident-elles pour toute présentation de monoïde — ou, au moins, pour toute présentation de monoïde d'une famille naturelle ?*

Cette remarque est à l'origine de l'étude menée dans [2] et dont ce chapitre est une version étoffée.

4 DIVERGENCE DES COMPLÉTIONS

Dans cette section, nous répondons à la question 3.3 par la négative.

Proposition 4.1. *Il existe des présentations de monoïde finies pour lesquelles la G-complétion et la R-complétion ne coïncident pas. Plus précisément, en notant $\widehat{\mathcal{R}}^G$ (resp. $\widehat{\mathcal{R}}^R$) pour la G-complétion (resp. la R-completion), il existe des présentations de monoïde finies $(\mathcal{S};\mathcal{R})$ exhibant chacun des comportements suivants :*

- *type 1 : $\widehat{\mathcal{R}}^R$ est un sous-ensemble propre de $\widehat{\mathcal{R}}^G$, avec $\widehat{\mathcal{R}}^R$ fini et $\widehat{\mathcal{R}}^G$ infini ;*
- *type 1' : $\widehat{\mathcal{R}}^R$ est un sous-ensemble propre de $\widehat{\mathcal{R}}^G$, avec $\widehat{\mathcal{R}}^R$ et $\widehat{\mathcal{R}}^G$ finis ;*
- *type 2 : $\widehat{\mathcal{R}}^G$ est un sous-ensemble propre de $\widehat{\mathcal{R}}^R$, avec $\widehat{\mathcal{R}}^G$ fini et $\widehat{\mathcal{R}}^R$ infini ;*
- *type 3 : $\widehat{\mathcal{R}}^G$ et $\widehat{\mathcal{R}}^R$ ne sont pas comparables en terme d'inclusion.*

Pour montrer la proposition, nous allons construire pour chacun des types des exemples de présentations de monoïde du type en question.

4.1 CONTRE-EXEMPLES DE TYPE 1

Il est relativement facile de trouver des contre-exemples de type 1, et nous allons en exhiber diverses familles.

Proposition 4.2. *Toute présentation*

$$(\mathtt{a},\mathtt{b},\mathtt{c},\ldots;\ \mathtt{b}w\mathtt{b}=\mathtt{ab}w),\ w\in\{\mathtt{a},\mathtt{b},\mathtt{c},\ldots\}^* \tag{2}$$

munie de l'ordre deglex avec a *minimal est un contre-exemple de type 1.*

Démonstration. Soit Π_w la présentation de (2). Chaque présentation Π_w est homogène : les relations conservent les longueurs donc la longueur est une pseudolongueur. De plus, chaque présentation a exactement une relation et celle-ci est du type $\mathtt{a}\ldots=\mathtt{b}\ldots$; par la proposition I.4.7, la présentation Π_w est donc R-complète.

Regardons maintenant la G-complétude. Premièrement, considérons le cas $w=\varepsilon$. Alors la composition de $\mathtt{bb}\vec{=}\mathtt{ab}$ avec elle-même puis avec le résultat de la composition mène aux relations R_m : $\mathtt{ba}^m\mathtt{b}=\mathtt{a}^{m+1}\mathtt{b}$. Or la composition de R_m avec R_n se réduit à 0. La proposition I.4.7 implique que $\{\mathtt{ba}^m b=\mathtt{a}^{m+1}\mathtt{b};m\geq 0\}$ est une base de Gröbner réduite de Π_ε. Donc, dans ce cas, la R-complétion de Π_ε, qui est Π_ε, est strictement incluse dans la G-complétion de Π_ε, et Π_ε est bien un contre-exemple de type 1.

Supposons $w\neq\varepsilon$. La composition de $\mathtt{b}w\mathtt{b}=\mathtt{ab}w$ avec elle-même donne $\mathtt{b}w\mathtt{ab}w=\mathtt{ab}w^2\mathtt{b}$, qui, composée avec $\mathtt{b}w\mathtt{b}=\mathtt{ab}w$, donne $\mathtt{b}w\mathtt{a}^2\mathtt{b}w=\mathtt{ab}w^2\mathtt{b}^2$. L'itération de ces compositions, c'est-à-dire composer $\mathtt{b}w\mathtt{b}=\mathtt{ab}w$ avec le résultat de composition précédente, produit toutes les relations $\mathtt{b}w\mathtt{a}^m\mathtt{b}w=\mathtt{ab}w^2\mathtt{b}^m$ avec $m\geq 1$.

On veut prouver que la G-complétion $\mathcal{B}$ de la présentation Π_w est infinie. On a vu que, pour chaque $m \geq 1$, on a $\mathtt{b}w\mathtt{a}^m\mathtt{b}w \equiv \mathtt{ab}w^2\mathtt{b}^m$. Il suffit de montrer qu'aucune relation de $\mathcal{B}$ ne peut réduire un nombre infini de mots différents $\mathtt{b}w\mathtt{a}^m\mathtt{b}w$. Raisonnons par l'absurde et supposons que (i) $u \vec{=} v$ est une relation de $\mathcal{B}$ avec $\ell := |u|$ et (ii) il existe $A \subsetneq \mathbb{N}$ infini avec $\ell \leq \min A$ tel que $u \vec{=} v$ réduise tous les mots $\mathtt{b}w\mathtt{a}^m\mathtt{b}w$ pour $m \in A$.

Dans la suite, un mot w est dit *isolé* s'il n'est $\equiv$-équivalent à aucun autre mot. Pour un mot w, on note $\sharp_{\mathtt{b}}(w)$ le nombre de fois où la lettre $\mathtt{b}$ apparaît dans le mot w.

Si on a $\ell \leq 1 + |w|$ alors u est trop court pour admettre bwb ou abw comme sous-mot, et donc u est isolé, contredisant (i).

Cas 0 : le mot u ne débute pas avant la position $2 + |w|$ et termine au plus tard $2 + |w|$ avant la fin, donc u est de la forme $\mathtt{a}^\ell$. Mais $\mathtt{a}^\ell$ n'inclut pas $\mathtt{b}w\mathtt{b}$ ni $\mathtt{ab}w$ et de ce fait est isolé, ce qui contredit (i).

Cas 1 : il existe un entier naturel q tel que u est un préfixe de $\mathtt{b}w\mathtt{a}^q$. Comme $m > \ell$, le mot u est de la forme $\mathtt{b}w\mathtt{a}^p$, $p \geq 1$. Donc il ne contient pas de sous-mot $\mathtt{b}w\mathtt{b}$ puisqu'on a $\sharp_{\mathtt{b}}(\mathtt{b}w\mathtt{b}) > \sharp_{\mathtt{b}}(\mathtt{b}w\mathtt{a}^p)$. De façon analogue, le mot u ne contient pas de sous-mot $\mathtt{ab}w$ puisque $\mathtt{ab}w \subseteq \mathtt{b}w\mathtt{a}^p$ implique $\mathtt{ab}w \subseteq w\mathtt{a}^p$, donc $\sharp_{\mathtt{b}}(\mathtt{b}w) \leq \sharp_{\mathtt{b}}(w)$, et donc u est isolé, ce qui contredit (i).

Cas 2 : le mot u débute à la position i, avec $i \geq 2$; d'où, il existe un entier naturel q tel que u est un préfixe de $w'\mathtt{a}^q$, où w' est un suffixe de w. On a $\sharp_{\mathtt{b}}(u) < \sharp_{\mathtt{b}}(\mathtt{b}w\mathtt{b})$ et $\sharp_{\mathtt{b}}(u) < \sharp_{\mathtt{b}}(\mathtt{ab}w)$ et donc ni $\mathtt{b}w\mathtt{b}$ ni $\mathtt{ab}w$ ne sont sous-mots de u ; donc u est isolé, ce qui contredit (i).

Cas 3 : le mot u termine au plus tard à la position $1 + |w|$ avant la fin. Alors on a $u = \mathtt{a}^p\mathtt{b}w'$ avec $p \geq 1$ et w' préfixe de w ; puisque $\ell > 1 + |w|$, on exclut les cas où u est un préfixe de w. En raison de l'ordre deglex, un mot v qui conviendrait serait de la forme $\mathtt{a}^p v'$ et donc, par simplification (voir prop I.6.1), $\mathtt{b}w$ se réduit à v', ce qui est impossible parce que $\mathtt{b}w$ est de longueur $1 + |w|$ et de ce fait est trop court pour ne pas être isolé. Ceci contredit (i). □

Parmi les remarques de la section 3.2, on notait que lors du calcul d'une base de Gröbner infinie, bien que l'algorithme 2.22 ne puisse pas terminer, il pouvait fournir suffisamment d'intuition sur les relations pour que finisse le calcul manuellement. Ici, la situation diffère en ce sens qu'on ne peut pas connaître la forme exacte des relations, on n'a pas d'expression régulière en les lettres de l'alphabet ; c'est pourquoi on a été obligés de prouver l'infinitude de la base de Gröbner réduite par un autre moyen que l'usage classique de la proposition 2.18.

Un exemple typique d'application de la proposition 4.2 est la présentation standard du monoïde des tresses B_3^+.

Exemple 4.3. La présentation standard $(\mathtt{a}, \mathtt{b}; \mathtt{bab} = \mathtt{aba})$ du monoïde de tresses B_3^+, avec l'ordre deglex induit par $\mathtt{a} < \mathtt{b}$, satisfait les hypothèses de la proposition 4.2 et est par conséquent un contre-exemple de type 1. Un calcul facile [5, Lemma 4.1] donne la base de

Gröbner réduite

$$\{\mathtt{bab} = \mathtt{aba}\} \cup \{\mathtt{ba}^n\mathtt{ba} = \mathtt{aba}^2\mathtt{b}^{n-1}; n \geq 2\},$$

qui est compatible avec la proposition 4.2. Considérons maintenant une présentation non standard de ce monoïde. Prenons la présentation de Birman-Ko-Lee $(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ab} = \mathtt{bc} = \mathtt{ca})$, connue sous le nom de présentation duale. Il a été établi dans [4] que cette présentation homogène satisfaisait la condition du cube. Elle est donc R-complète. On fixe l'ordre deglex induit par $\mathtt{a} < \mathtt{b} < \mathtt{c}$. Remarquons que les générateurs apparaissant de manière tout à fait symétrique dans les relations, les différentes bases de Gröbner réduites qu'on obtiendrait en faisant varier l'ordre sont les mêmes, à permutation des lettres près. Pour cet ordre, la base de Gröbner réduite qu'on obtient par calcul est

$$\{\mathtt{ca} = \mathtt{ab}, \mathtt{bc} = \mathtt{ab}\} \cup \{\mathtt{ba}^n\mathtt{b} = \mathtt{abac}^{n-1}; n \geq 1\},$$

faisant de cette présentation un contre-exemple de type 1.

Nous allons maintenant donner d'autres contre-exemples. La présentation standard du monoïde de tresses B_3^+ est le premier cas non trivial d'une présentation d'Artin à deux générateurs, et on peut obtenir plus de contre-exemples de type 1 en considérant des présentations d'Artin plus générales.

Proposition 4.4. *Toute présentation d'Artin à deux générateurs*

$$(\mathtt{a}, \mathtt{b}; \underbrace{\mathtt{baba}\ldots}_{\text{longueur } m} = \underbrace{\mathtt{abab}\ldots}_{\text{longueur } m})$$

est un contre-exemple de type 1, quel que soit l'ordre deglex considéré.

Démonstration. Il y a deux cas. Si la présentation est du type $(\mathtt{a}, \mathtt{b}; (\mathtt{ba})^n\mathtt{b} = (\mathtt{ab})^n\mathtt{a})$, avec $n \geq 1$, alors, d'après la proposition 4.2, la présentation est un contre-exemple de type 1.

Supposons donc que la présentation est de la forme $(\mathtt{a}, \mathtt{b}; (\mathtt{ba})^n = (\mathtt{ab})^n)$, avec $n \geq 1$. Composons $(\mathtt{ba})^n = (\mathtt{ab})^n$ avec elle-même comme suit :

$$((\mathtt{ba})^n - (\mathtt{ab})^n)\,\mathtt{ba} - \mathtt{ba}\,((\mathtt{ba})^n - (\mathtt{ab})^n) = -(\mathtt{ab})^n\mathtt{ba} + \mathtt{ba}(\mathtt{ab})^n.$$

Composons la nouvelle relation avec $(\mathtt{ba})^n = (\mathtt{ab})^n$. On obtient

$$(\mathtt{ba}(\mathtt{ab})^n - (\mathtt{ab})^n\mathtt{ba})\,\mathtt{a} - \mathtt{ba}^2\,((\mathtt{ba})^n - (\mathtt{ab})^n) = -(\mathtt{ab})^n\mathtt{ba}^2 + \mathtt{ba}^2(\mathtt{ab})^n.$$

En itérant les compositions, on obtient l'ensemble de relations

$$\{(\mathtt{ba})^n = (\mathtt{ab})^n\} \cup \{\mathtt{ba}^p(\mathtt{ab})^n = (\mathtt{ab})^n\mathtt{ba}^p; p \geq 1\}\,.$$

Par la proposition 2.18, il suffit de vérifier que chaque composition se réduit à 0. Pour p et q dans $\mathbb{N}$, on calcule explicitement la composition de $\mathtt{ba}^p(\mathtt{ba})^n = (\mathtt{ba})^n\mathtt{ba}^p$ avec $\mathtt{ba}^q(\mathtt{ba})^n = (\mathtt{ba})^n\mathtt{ba}^q$:

$$\begin{aligned}
(\mathtt{ba}^p(\mathtt{ab})^n - (\mathtt{ab})^n\mathtt{ba}^p)\mathtt{a}^q(\mathtt{ab})^n - \mathtt{ba}^p(\mathtt{ab})^{n-1}\mathtt{a}(\mathtt{ba}^q(\mathtt{ab})^n - (\mathtt{ab})^n\mathtt{ba}^q) \\
&= -(\mathtt{ab})^n\mathtt{ba}^{p+q}(\mathtt{ab})^n + \mathtt{ba}^p(\mathtt{ab})^{n-1}\mathtt{a}(\mathtt{ab})^n\mathtt{ba}^q \\
&\rightsquigarrow -(\mathtt{ab})^n(\mathtt{ab})^n\mathtt{ba}^{p+q} + \mathtt{ba}^p(\mathtt{ab})^{n-2}\mathtt{aba}(\mathtt{ab})^n\mathtt{ba}^q \\
&\rightsquigarrow -(\mathtt{ab})^{2n}\mathtt{ba}^{p+q} + \mathtt{ba}^{p+1}(\mathtt{ab})^n(\mathtt{ba})^{n-1}\mathtt{ba}^q \\
&\rightsquigarrow -(\mathtt{ab})^{2n}\mathtt{ba}^{p+q} + (\mathtt{ab})^n\mathtt{ba}^{p+1}(\mathtt{ba})^{n-1}\mathtt{ba}^q \\
&\rightsquigarrow -(\mathtt{ab})^{2n}\mathtt{ba}^{p+q} + (\mathtt{ab})^n\mathtt{ba}^p(\mathtt{ab})^n\mathtt{a}^q \\
&\rightsquigarrow -(\mathtt{ab})^{2n}\mathtt{ba}^{p+q} + (\mathtt{ab})^n(\mathtt{ab})^n\mathtt{ba}^p\mathtt{a}^q = 0.
\end{aligned}$$

□

Une autre famille infinie de contre-exemples de type 1 généralisant, mais dans une autre direction que la proposition 4.4, le résultat de l'exemple 4.3 est la famille des présentations standard des monoïdes de tresses :

Proposition 4.5. *Pour $n \geq 3$, la présentation d'Artin-Tits*

$$\left(\sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \textit{pour } |j-i| = 1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \textit{pour } |j-i| \geq 2 \end{array}\right) \tag{3}$$

du monoïde de tresses B_n^+ est un contre-exemple de type 1.

Démonstration. On a montré à l'exemple I.4.8 que les monoïdes B_n^+ sont R-complets.

Prenons un $i \leq n-2$; posons $\mathtt{b} = \max(\sigma_i, \sigma_{i+1})$ et $\mathtt{a} = \min(\sigma_i, \sigma_{i+1})$. Comme dans le cas de B_3^+, la relation $\mathtt{bab} = \mathtt{aba}$ de B_n^+ conduit l'algorithme 2.22 à ajouter toutes les relations $\mathtt{ba}^n\mathtt{ba} = \mathtt{aba}^2\mathtt{b}^{n-1}$, avec $n \geq 2$. Il suffit de prouver que ces relations ne sont pas réduites par les relations de la base de Gröbner réduite $\mathcal{B}$. Raisonnons par l'absurde et supposons qu'il existe une relation $u = v$ de $\mathcal{B} - (\{\mathtt{bab} = \mathtt{aba}\} \cup \{\mathtt{ba}^n\mathtt{ba} = \mathtt{aba}^2\mathtt{b}^{n-1}; n \geq 2\})$ réduisant au moins une relation $\mathtt{ba}^n\mathtt{ba} = \mathtt{aba}^2b^{n-1}$. Donc on a $u \in \{\mathtt{a}, \mathtt{b}\}^*$. Maintenant, l'équivalence $u \equiv v$ implique qu'il existe une suite de mots $u_0, u_1, \dots, u_n$ satisfaisant

$$u = u_0 \equiv^{(1)} u_1 \equiv^{(1)} \cdots \equiv^{(1)} u_{n-1} \equiv^{(1)} u_n = v.$$

Mais il n'y a qu'une seule relation dans la présentation de B_n^+ n'impliquant que des $\mathtt{a}$ et des $\mathtt{b}$, à savoir $\mathtt{bab} = \mathtt{aba}$. De ce fait, $u_0 \equiv^{(1)} u_1$ implique $u_1 \in \{\mathtt{a}, \mathtt{b}\}^*$, et il s'ensuit que v est élément de $\{\mathtt{a}, \mathtt{b}\}^*$ et que la relation $u = v$ a lieu dans B_3^+ ; donc les relations $\mathtt{ba}^n\mathtt{ba} = \mathtt{aba}^2\mathtt{b}^{n-1}$, avec $n \geq 2$, et $\mathtt{bab} = \mathtt{aba}$ réduisent $u = v$ à 0, contredisant le fait que $\mathcal{B}$ était réduite. □

À titre d'illustration de la proposition précédente, on donne dans l'exemple suivant la base de Gröbner réduite dans le cas de la présentation du monoïde B_4^+.

Exemple 4.6. Par la proposition 4.5, on sait que la présentation d'Artin standard du monoïde de tresses B_4^+

$$(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{bab} = \mathtt{aba}, \mathtt{ca} = \mathtt{ac}, \mathtt{cbc} = \mathtt{bcb})$$

avec l'ordre deglex induit par $\mathtt{a} < \mathtt{b} < \mathtt{c}$ est un contre-exemple de type 1. En fait, un calcul direct montre que la G-complétion est

$$\begin{aligned}
\mathtt{bab} &= \mathtt{aba}, \\
\mathtt{cbc} &= \mathtt{bcb}, \\
\mathtt{ca} &= \mathtt{ac}, \\
\mathtt{ba}^n\mathtt{ba} &= \mathtt{aba}^2\mathtt{b}^{n-1}, n \geq 2, \\
\mathtt{cb}^n\mathtt{cb} &= \mathtt{bcb}^2\mathtt{c}^{n-1}, n \geq 2, \\
\mathtt{cba}^n\mathtt{c} &= \mathtt{bcba}^n, n \geq 1, \\
\mathtt{cba}^n\mathtt{b}^p\mathtt{cb} &= \mathtt{bcba}^n\mathtt{bc}^p, n \geq 2, p \geq 1, \\
\mathtt{cb}^{n_1}\mathtt{a}^{n_2}\mathtt{b}^{n_3}\dots\mathtt{b}^{n_k}\mathtt{cba} &= \mathtt{bcb}^2\mathtt{ac}^{n_1-1}\mathtt{b}^{n_2}\mathtt{c}^{n_3}\dots\mathtt{c}^{n_k},
\end{aligned}$$

avec $k \geq 2$, et les n_i sont des entiers naturels satisfaisant $n_2, n_3, \dots, n_{k-1} \geq 2$, avec les conditions supplémentaires suivantes : $n_1 \geq 2$ si on a $k = 2$ ou $k = 3$, et $n_k \geq 2$ si k est impair. Toutes ces conditions sur les puissances des lettres intervenant dans les relations garantissent le caractère réduit de la base de Gröbner. Sans ces contraintes, la plupart des relations seraient encore vraies mais la base ne serait plus réduite.

Remarque 4.7. Bokut *et al.* [5, Th. 4.2] donnent des bases de Gröbner pour toutes les présentations d'Artin des monoïdes de tresses B_n^+, avec $n \geq 3$. Ces dernières coïncident avec celles qu'on a calculées dans les exemples exemples 4.3 et 4.6. Bien que presque explicites, ces bases ne sont pas réduites dans les cas $n \geq 5$ et de ce fait ne permettent pas de conclure que les présentations de (3) sont des contre-exemples de type 1, contrairement à la proposition 4.5.

Jusqu'à présent, nous n'avons considéré que des contre-exemples de type 1. Nous concluons cette section avec ce qu'on a appelé les contre-exemples de type $1'$ dans la proposition 4.1, c'est-à-dire les présentations pour lesquelles la R-complétion est un sous-ensemble propre de la G-complétion et toutes deux sont finies. On donne ici l'exemple d'une présentation généralisant la présentation du monoïde de Garside $M_\bullet$ de [23].

Proposition 4.8. *Pour tout $n \geq 1$ et $p \geq 1$, la présentation*

$$(\mathtt{a}, \mathtt{b}; (\mathtt{ab})^n\mathtt{a} = \mathtt{b}^p) \tag{4}$$

munie de l'ordre deglex induit par $\mathtt{a} < \mathtt{b}$ est un contre-exemple de type $1'$.

Démonstration. D'après la proposition I.4.10, la présentation (4) est R-complète puisque sa seule relation est du type $\mathtt{a}\ldots = \mathtt{b}\ldots$. Puis, on vérifie avec la proposition 2.18 que l'ensemble

$$\mathcal{B} = \{(\mathtt{ab})^n\mathtt{a} = \mathtt{b}^p, \mathtt{b}^{p+1}\mathtt{a} = \mathtt{ab}^{p+1}\}$$

est la base de Gröbner réduite de la présentation (4). □

4.2 CONTRE-EXEMPLES DE TYPE 2

Dans cette section, on donne des exemples de présentations dont la G-complétion est strictement incluse dans leur R-complétion.

Lemme 4.9. *Soit* $(\mathtt{a},\mathtt{b};\mathcal{R})$ *une présentation avec aucune relation de la forme* $\mathtt{a}\ldots = \mathtt{a}\ldots$ *ou* $\mathtt{b}\ldots = \mathtt{b}\ldots$. *Alors, pour chaque mot non vide* w *sur* $\{\mathtt{a},\mathtt{b}\}$, *la R-complétion de* $(\mathtt{a},\mathtt{b};\mathcal{R},\mathtt{b}w = \mathtt{b})$ *inclut* $\{\mathtt{b}w^n = \mathtt{b}; n \in \mathbb{N}\}$.

Démonstration. La relation $\mathtt{b}w = \mathtt{b}$ implique $\mathtt{b}w^n \equiv \mathtt{b}$, avec $n \geq 1$. On prouve par récurrence sur n, que $(\mathtt{b}w^n)^{-1}\mathtt{b}$ ne peut pas être retourné en ε même si toutes les relations $\mathtt{b}w^m = \mathtt{b}$, $m < n$, ont été ajoutées à la présentation. Puisque $(\mathtt{b}w^2)^{-1}\mathtt{b}$ se retourne en w^{-1}, on suppose $n > 2$. Par hypothèse, il n'y a pas de relation $s\ldots = s\ldots$ dans $\mathcal{R}$ et donc, les seuls retournements de $(\mathtt{b}w^n)^{-1}\mathtt{b}$ sont, pour tous p et m satisfaisant $p < m < n$, $(\mathtt{b}w^n)^{-1}\mathtt{b} \curvearrowright w^{-m}w^p \curvearrowright (w^{m-p})^{-1}$; ceci achève la récurrence. □

Proposition 4.10. *Avec les hypothèses du lemme 4.9, toute présentation G-complète de la forme* $(\mathtt{a},\mathtt{b};\mathtt{b}w = \mathtt{b})$ *est un contre-exemple de type 2.*

Démonstration. D'après le lemme 4.9, la R-complétion de $(\mathtt{a},\mathtt{b};\mathtt{b}w = \mathtt{b})$ contient l'ensemble $\{\mathtt{b}w^n = \mathtt{b}; n \in \mathbb{N}\}$ qui, à son tour, contient la G-complétion, à savoir $\{\mathtt{b}w = \mathtt{b}\}$. □

Exemple 4.11. L'illustration la plus simple de la proposition 4.10 est $(\mathtt{a},\mathtt{b};\mathtt{ba} = \mathtt{b})$ dont la base de Gröbner réduite consiste simplement en la relation $\mathtt{ba} = \mathtt{b}$ et dont la R-complétion est $\{\mathtt{ba}^n = \mathtt{b}; n \in \mathbb{N}\}$.

Le résultat suivant est une autre application du lemme 4.9 différant de la proposition 4.10 en ce que l'ensemble $\mathcal{R}$ est non vide.

Proposition 4.12. *Pour tous* n, q, p *satisfaisant* $n + q > p$, *les présentations*

$$(\mathtt{a},\mathtt{b};\ \mathtt{a}^n\mathtt{b}^q = \mathtt{b}^p, \mathtt{ba} = \mathtt{b})$$

munies de l'ordre deglex induit par $b > a$ *sont des contre-exemples de type 2.*

Démonstration. On calcule tout d'abord la G-complétion. Il n'y a qu'une seule composition à calculer :

$$\begin{array}{rcl}(\mathtt{a}^n\mathtt{b}^q - \mathtt{b}^p)\mathtt{a} - \mathtt{a}^n\mathtt{b}^{q-1}(\mathtt{ba} - \mathtt{b}) & = & -\mathtt{b}^p\mathtt{a} + \mathtt{a}^n\mathtt{b}^q \\ & \rightsquigarrow & -\mathtt{b}^p + \mathtt{a}^n\mathtt{b}^q \quad \rightsquigarrow \quad 0.\end{array}$$

Donc la présentation $(\mathtt{a}, \mathtt{b};\ \mathtt{a}^n\mathtt{b}^q = \mathtt{b}^p, \mathtt{ba} = \mathtt{b})$ est G-complète. Le lemme 4.9 permet de conclure. □

Tous les contre-exemples de type 2 ci-dessus présentent la particularité d'être déjà G-complets, autrement dit, l'ensemble $\mathcal{R}$ de chaque présentation de monoïde $(\mathcal{S}; \mathcal{R})$ de type 2 considérée jusqu'à présent est une base de Gröbner. On donne maintenant deux contre-exemples de type 2 qui ne sont pas d'emblée G-complets. Le premier a une base de Gröbner réduite finie, ce qui, dans la pratique, est plutôt rare. Le deuxième a une base infinie. Dans les deux cas, par définition du type 2, la R-complétion les contient.

Proposition 4.13. *Quel que soit l'ordre deglex, la présentation* $(\mathtt{a}, \mathtt{b}; \mathtt{ba}^2 = \mathtt{ab}, \mathtt{a}^2\mathtt{b} = \mathtt{b}^2)$ *est un contre-exemple de type 2.*

Démonstration. L'algorithme 2.22 donne pour l'ordre induit par $b > a$ la base de Gröbner réduite

$$\{\mathtt{ba}^2 = \mathtt{ab}, \mathtt{a}^2\mathtt{b} = \mathtt{ab}, \mathtt{b}^2 = \mathtt{ab}, \mathtt{bab} = \mathtt{ab}\}$$

et pour l'ordre induit par $a > b$ la base

$$\{\mathtt{ab} = \mathtt{b}^2, \mathtt{ba}^2 = \mathtt{b}^2, \mathtt{b}^3 = \mathtt{b}^2\}.$$

Il suffit ensuite de montrer pour chacune de ces relations $u = v$ qu'on n'a pas $u^{-1}v \curvearrowright \varepsilon$. □

Pour le deuxième contre-exemple, on utilise une présentation de monoïde proche de celle qu'on a vue aux sections I.5.2 et 3.1. On y calculait les complétions pour la relation $\mathtt{ba}^n\mathtt{b} = \mathtt{ba}^{n+1}$ avec $n = 1$. Ici on considère le cas $n = 0$.

Proposition 4.14. *La présentation* $(\mathtt{a}, \mathtt{b}; \mathtt{bb} = \mathtt{ba})$ *est un contre-exemple de type 2 pour tout ordre admissible.*

Démonstration. Le cas où l'ordre vérifie $\mathtt{b} < \mathtt{a}$ implique $\mathtt{bb} < \mathtt{ba}$ et donc la présentation est G-complète puisque la seule relation, $\mathtt{ba} \vec{=} \mathtt{bb}$, n'est pas composable avec elle-même. Pour tout ordre admissible satisfaisant $\mathtt{b} < \mathtt{a}$, le calcul est tout à fait similaire à celui qu'on a effectué dans l'exemple de la section 3.1. On trouve la base de Gröbner réduite

$$\{\mathtt{ba}^n\mathtt{b} = \mathtt{ba}^{n+1}; n \geq 0\}.$$

On peut reprendre le calcul de la section I.5.2 pour trouver que la R-complétion contient la base de Gröbner réduite. Mais la R-complétion est plus grosse : l'équivalence $\mathtt{b}^2\mathtt{a}^2 \equiv \mathtt{ba}^3$ n'est pas prouvable par retournement. □

Remarque 4.15. Il est naturel, comme dans la section 4.1, de définir la notion de contre-exemple de type $2'$ comme étant une présentation de monoïde $(\mathcal{S}; \mathcal{R})$ satisfaisant $\widehat{\mathcal{R}}^G \subsetneq \widehat{\mathcal{R}}^R$ et $|\widehat{\mathcal{R}}^R| < \infty$. Cependant, contrairement au type $1'$, on ne connaît pas de présentation de type $2'$ à ce jour. La plus grosse difficulté réside dans le calcul de la R-complétion. En effet, au cours du processus de complétion, le retournement devient souvent, si ce n'était pas déjà le cas, non déterministe : si, à un moment donné, on a une relation $s \ldots = s \ldots$ disponible et qu'on doit retourner un motif $s^{-1}s$, alors on a deux façons de le retourner, menant à deux mots terminaux différents en général.

4.3 CONTRE-EXEMPLES DE TYPE 3

On conclut la liste des contre-exemples avec les contre-exemples de type 3, c'est-à-dire les présentations de monoïde pour lesquelles les complétions ne sont pas comparables en terme d'inclusion. D'abord, nous verrons qu'on peut créer facilement de tels contre-exemples à partir de contre-exemples de type 1 et de type 2. Ensuite, nous montrerons qu'il existe des contre-exemples moins artificiels comme la présentation standard d'Heisenberg.

On note $X_1 \sqcup X_2$ l'union disjointe des ensembles X_1 et X_2, c'est-à-dire

$$X_1 \sqcup X_2 = X_1 \times \{1\} \cup X_2 \times \{2\}.$$

Définition 4.16. Le *produit direct* des présentations $(\mathcal{S}_1, \mathcal{R}_1)$ et $(\mathcal{S}_2, \mathcal{R}_2)$ est la présentation qu'on note $(\mathcal{S}_1, \mathcal{R}_1) \times (\mathcal{S}_2, \mathcal{R}_2)$ et égale à $(\mathcal{S}_1 \sqcup \mathcal{S}_2, \mathcal{R}_1 \sqcup \mathcal{R}_2 \sqcup \mathcal{R})$ avec $\mathcal{R} = \{s_1 s_2 = s_2 s_1; s_1 \in \mathcal{S}_1, s_2 \in \mathcal{S}_2\}$.

Dans la suite, les ordres considérés sur le produit direct de deux présentations ordonnées seront l'ordre deglex avec les lettres ordonnées comme suit : les ordres sur $\mathcal{S}_1$ et $\mathcal{S}_2$ sont préservés et on pose $\max \mathcal{S}_1 < \min \mathcal{S}_2$.

Lemme 4.17. *Soit $\mathcal{P}$ le produit direct des présentations de monoïde $(\mathcal{S}_1, \mathcal{R}_1)$ et $(\mathcal{S}_2, \mathcal{R}_2)$. Alors, en utilisant les notations introduites à la proposition 4.1, la base de Gröbner réduite de $\mathcal{P}$ est $\widehat{\mathcal{R}_1}^G \sqcup \widehat{\mathcal{R}_2}^G \sqcup \mathcal{R}$ et son ensemble de relations R-complété est $\widehat{\mathcal{R}_1}^R \sqcup \widehat{\mathcal{R}_2}^R \sqcup \mathcal{R}$.*

Démonstration. Pour prouver que $\widehat{\mathcal{R}_1}^G \sqcup \widehat{\mathcal{R}_2}^G \sqcup \mathcal{R}$ est la base de Gröbner réduite de $\mathcal{P}$, il suffit, d'après la proposition 2.18, de vérifier que toutes les compositions se réduisent à 0. Il n'y a pas de composition possible dans $\widehat{\mathcal{R}_1}^G$ ni dans $\widehat{\mathcal{R}_2}^G$ puisque ces deux ensembles de relations sont réduits. Il est clair que $\mathcal{R}$ ne contient pas non plus de composition. Les seules compositions ne se réduisant pas à 0 doivent donc impliquer des relations de deux ensembles distincts parmi $\widehat{\mathcal{R}_1}^G$, $\widehat{\mathcal{R}_2}^G$ et $\mathcal{R}$. Comme $\mathcal{S}_1$ et $\mathcal{S}_2$ sont d'intersection vide, il n'y a pas de composition possible entre $\widehat{\mathcal{R}_1}^G$ et $\widehat{\mathcal{R}_2}^G$. De plus, puisqu'on a $s_2 > s_1$ pour tous s_2 de $\mathcal{S}_2$ et s_1 de $\mathcal{S}_1$, la première lettre du mot dominant de toute relation de $\mathcal{R}$ est dans $\mathcal{S}_2$ et la dernière est dans $\mathcal{S}_1$. On laisse les détails de la vérification que toute composition de $\widehat{\mathcal{R}_2}^G$ et $\mathcal{R}$ se réduit à 0. Le cas mettant en jeu $\widehat{\mathcal{R}_1}^G$ est similaire.

Pour prouver que $(\mathcal{S}_1 \sqcup \mathcal{S}_2; \widehat{\mathcal{R}_1}^R \sqcup \widehat{\mathcal{R}_2}^R \sqcup \mathcal{R})$ est R-complète, il suffit de vérifier que dès qu'on a deux mots équivalents, on peut le prouver par retournement. Or, si u et v sont équivalents, alors on a $u \equiv u_1u_2$ et $v \equiv v_1v_2$, avec u_1, v_1 dans $\mathcal{S}_1^*$ et u_2, v_2 dans $\mathcal{S}_2^*$, satisfaisant $u_1 \equiv v_1 \ u_2 \equiv v_2$. Ces dernières équivalences sont prouvables par retournement (puisqu'on a toutes les relations de $\widehat{\mathcal{R}_1}^R$ et $\widehat{\mathcal{R}_2}^R$) et on peut vérifier que trouver une suite de retournements de $u^{-1}v$ à ε revient à trouver des retournements de $u_1^{-1}v_1$ et $u_2^{-1}v_2$ à ε. □

La proposition suivante exploite ces résultats pour créer un contre-exemple de type 3 à partir de contre-exemples de type 1 et de type 2.

Proposition 4.18. *Soit $(\mathcal{S}_1, \mathcal{R}_1)$ un contre-exemple de type 1, et soit $(\mathcal{S}_2, \mathcal{R}_2)$ un contre-exemple de type 2. Alors $(\mathcal{S}_1, \mathcal{R}_1) \times (\mathcal{S}_2, \mathcal{R}_2)$ est un contre-exemple de type 3.*

Démonstration. Par hypothèse, les ensembles $\widehat{\mathcal{R}_1}^R \sqcup \widehat{\mathcal{R}_2}^R$ et $\widehat{\mathcal{R}_1}^G \sqcup \widehat{\mathcal{R}_2}^G$ ne sont pas comparables. Ainsi, par le lemme 4.17, la G-complétion et la R-complétion de $(\mathcal{S}_1, \mathcal{R}_1) \times (\mathcal{S}_2, \mathcal{R}_2)$ ne sont pas comparables. □

Cette dernière proposition fournit un moyen de construire des contre-exemples de type 3 comme produit direct de contre-exemples de type 1 et de type 2. Il y a cependant des présentations moins triviales de type 3 qui ne sont pas des produits directs d'autres présentations.

Proposition 4.19. *Munie de l'ordre deglex induit par $\mathtt{a} < \mathtt{b} < \mathtt{c}$, la présentation d'Heisenberg*

$$(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ab} = \mathtt{bac}, \mathtt{ac} = \mathtt{ca}, \mathtt{bc} = \mathtt{cb})$$

est un contre-exemple de type 3.

Démonstration. D'après [16, Ex. 5.4], la présentation d'Heisenberg R-complétée est

$$(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ab} = \mathtt{bac}, \mathtt{ac} = \mathtt{ca}, \mathtt{bc} = \mathtt{cb}, \mathtt{cba} = \mathtt{ab}).$$

Par ailleurs, l'exécution de l'algorithme 2.22 donne la G-complétion suivante :

$$\begin{aligned}\{\mathtt{cb} = \mathtt{bc}, \mathtt{ca} = \mathtt{ac}\} \ &\cup \ \{\mathtt{ba}^{n+1}\mathtt{c} = \mathtt{aba}^n; n \geq 0\} \\ &\cup \ \{\mathtt{ba}^{2n}\mathtt{b} = \mathtt{a}^n\mathtt{b}^2\mathtt{a}^n; n \geq 1\} \cup \{\mathtt{ba}^{2n+1}\mathtt{b} = \mathtt{a}^n\mathtt{baba}^n; n \geq 1\}.\end{aligned}$$

On remarque que la G-complétion est infinie et donc la présentation d'Heisenberg n'est ni de type $1'$, ni de type 2 ni de type $2'$. De plus, la relation $\mathtt{cba} = \mathtt{ab}$ de la R-complétion n'est pas dans la G-complétion et donc la présentation d'Heisenberg n'est pas de type 1. □

La présentation d'Heisenberg est un contre-exemple de type 3 dont la R-complétion est finie. De cette R-complétion et de la proposition I.6.1 on déduit que le monoïde d'Heisenberg est simplifiable à gauche. Cette situation, à savoir un contre-exemple de type 3 dont la R-complétion est finie d'une part et qui est est associé à un monoïde simplifiable d'autre part, n'est à nouveau pas générale comme le montre la proposition suivante.

Proposition 4.20. (i) *Il existe un contre-exemple de type 3 à R-complétion finie. De plus, le monoïde associé est simplifiable à gauche.*
(ii) *Il existe un contre-exemple de type 3 à R-complétion infinie. De plus, le monoïde associé n'est pas simplifiable à gauche.*
(iii) *Il existe un contre-exemple de type 3 à R-complétion finie. De plus, le monoïde associé n'est pas simplifiable à gauche.*

Démonstration. On a montré (i) dans la proposition 4.19, la présentation d'Heisenberg est un tel contre-exemple.

Montrons (ii). Considérons la présentation

$$(\mathtt{a},\mathtt{b},\mathtt{c};\mathtt{ab}=\mathtt{ba},\mathtt{ac}=\mathtt{ca},\mathtt{bb}=\mathtt{ca}) \tag{5}$$

munie de l'ordre deglex induit par $\mathtt{a}<\mathtt{b}<\mathtt{c}$. Une autre application de l'algorithme 2.22 mène à considérer deux familles infinies de relations qu'on montre faire partie de la base de Gröbner réduite par la proposition 2.18. La base de Gröbner réduite de cette présentation est

$$\{\mathtt{ba}=\mathtt{ab},\mathtt{ca}=\mathtt{ac},\mathtt{bb}=\mathtt{ac}\}\cup\{\mathtt{ac}^n\mathtt{b}=\mathtt{abc}^n;n\geq 1\}\cup\{\mathtt{abc}^n\mathtt{b}=\mathtt{a}^2\mathtt{c}^{n+1};n\geq 1\}.$$

De l'équivalence $\mathtt{acb}\equiv\mathtt{abc}$ et du fait que $\mathtt{bc}$ est isolé, on déduit que le monoïde associé à la présentation (5) n'est pas simplifiable à gauche.

On remarque immédiatement que la présentation (5) n'est pas R-complète car on a les relations $\mathtt{ac}=\mathtt{ca}$ et $\mathtt{bb}=\mathtt{ca}$ mais pas $\mathtt{bb}=\mathtt{ac}$. Les trois relations conservant la longueur, la présentation est homogène (remarque I.4.4) ; on utilise donc l'algorithme I.5.1 pour R-compléter la présentation (5). Sans calculer toute la R-complétion, on trouve qu'elle contient néanmoins l'ensemble de relations

$$\{\mathtt{ac}^n\mathtt{b}=\mathtt{abc}^n;\mathtt{n}\geq 1\}$$

ainsi que la relation $\mathtt{abc}=\mathtt{cab}$. La R-complétion est donc infinie et n'est pas incluse dans la G-complétion car la relation $\mathtt{abc}=\mathtt{cab}$ ne fait pas partie de la base de Gröbner réduite. Réciproquement, la relation $\mathtt{abcb}=\mathtt{a}^2\mathtt{c}^2$ de la G-complétion n'est pas dans la R-complétion : en effet, les relations qu'on connaît de la R-complétion suffisent à montrer l'équivalence $\mathtt{abcb}\equiv\mathtt{a}^2\mathtt{c}^2$ par retournement, autrement dit, on a $(\mathtt{abcb})^{-1}\mathtt{a}^2\mathtt{c}^2\curvearrowright\varepsilon$, comme l'illustre le diagramme de la figure 2.

Pour montrer (iii) on considère la présentation $(\mathtt{a},\mathtt{b},\mathtt{c};\mathtt{ab}=\mathtt{ba},\mathtt{bc}=\mathtt{cb},\mathtt{ab}=\mathtt{cb})$, qui est homogène (remarque I.4.4). L'application classique de la proposition I.5.2 montre qu'il faut ajouter les relations $\mathtt{ba}=\mathtt{bc}$, $\mathtt{ab}=\mathtt{bc}$ et $\mathtt{cb}=\mathtt{ba}$. Un autre calcul à l'aide de l'algorithme 2.22 et de la proposition 2.18 mène à la G-complétion

$$\{\mathtt{ba}=\mathtt{ab},\mathtt{bc}=\mathtt{ab}\}\cup\{\mathtt{ca}^n\mathtt{b}=\mathtt{a}^{n+1}\mathtt{b};n\geq 0\}.$$

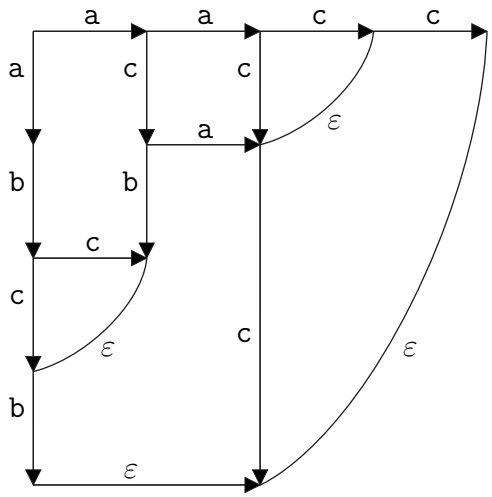


FIGURE 2 – En montrant qu'on peut retourner $(\mathtt{abcb})^{-1}\mathtt{a}^2\mathtt{c}^2$ en le mot vide ε, on montre que la relation $\mathtt{abcb} = \mathtt{a}^2\mathtt{c}^2$ n'est pas dans la R-complétion de la présentation $(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ab} = \mathtt{ba}, \mathtt{ac} = \mathtt{ca}, \mathtt{bb} = \mathtt{ca})$ alors qu'elle appartient à la G-complétion. Cette présentation est donc un bon candidat pour être un contre-exemple de type 3.

La présentation n'est pas un contre-exemple de type 1 car la relation $\mathtt{cb} = \mathtt{bc}$ n'est pas dans la base de Gröbner. La présentation n'est pas non plus de type 2 car $\mathtt{cab} = \mathtt{a}^2\mathtt{b}$ ne fait pas partie de la R-complétion. Quant à la simplifiabilité à gauche, il suffit de remarquer qu'on a ajouté la relation $\mathtt{ba} = \mathtt{bc}$ et que dès lors on a $\mathtt{ba} \equiv \mathtt{bc}$ mais pas $\mathtt{a} \equiv \mathtt{c}$. □

5 SIMPLIFIABILITÉ

On a vu à la section I.6.1 qu'une application du retournement est de déterminer si le monoïde associé à une présentation R-complète est simplifiable à gauche. Dans le cas d'une présentation de monoïde R-complète, on sait en effet qu'il suffit d'examiner les relations de la forme $s \ldots = s \ldots$ pour déterminer la simplifiabilité à gauche du monoïde associé (proposition I.6.1). Étant donnée la forte ressemblance entre la construction de la G-complétion et de la R-complétion d'une présentation, il est naturel d'étudier l'information qu'apporte la G-complétion d'une présentation sur la simplifiabilité du monoïde associé.

Quand on considère des présentations G-complètes, le critère de la proposition I.6.1 reste nécessaire, mais n'est plus suffisant.

Proposition 5.1. (i) *Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde G-complète et réduite. Si $\mathcal{R}$ contient une relation de la forme $su = sv$ avec u, v des mots non vides de $\mathcal{S}^*$, alors le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ n'est pas simplifiable à gauche.*

(ii) *Il existe une présentation de monoïde G-complète $(\mathcal{S}; \mathcal{R})$ telle que $\mathcal{R}$ ne contienne*

aucune relation du type $su = sv$ avec u, v des mots non vides de $\mathcal{S}^*$, et pour laquelle le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ n'admet pas la simplification à gauche.

Démonstration. (i) Supposons que le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ soit simplifiable à gauche. Alors on a $u \equiv_{\mathcal{R}} v$ et $u = v$ n'est pas une relation de $\mathcal{R}$, sinon la présentation $\mathcal{R}$ ne serait pas réduit. Prouvons que ce n'est pas possible.

Puisqu'on a fixé un ordre compatible avec la concaténation dans le monoïde, l'inégalité $su > sv$ implique $u > v$. Cette dernière inégalité combinée avec l'équivalence $u \equiv v$ signifie que u ou v est réductible. Dès lors, supposons qu'il y ait une relation $w = w'$ de $\mathcal{R}$ avec w un sous-mot de u. Ceci signifie que la relation $su = sv$ n'était pas réduite, ce qui contredit l'hypothèse. Le même argument s'applique à v. Ainsi, il n'y a pas de relation $w = w'$ avec w un sous-mot de u ou v. Donc u et v sont nécessairement réduits et comme ils sont équivalents, ils sont égaux, ce qui contredit $u > v$.

(ii) Prenons le monoïde présenté par $(\mathtt{a}, \mathtt{b}, \mathtt{c};\ \mathtt{ca} = \mathtt{ba}, \mathtt{cb} = \mathtt{ba})$, muni de l'ordre deglex induit par $\mathtt{a} < \mathtt{b} < \mathtt{c}$. Cette présentation est G-complète. De $\mathtt{ca} = \mathtt{ba}$ et $\mathtt{cb} = \mathtt{ba}$ on déduit $\mathtt{ca} \equiv \mathtt{cb}$. Or on n'a pas $\mathtt{a} \equiv \mathtt{b}$ et donc le monoïde n'est pas simplifiable à gauche. □

La proposition 5.1 établit que pour qu'une présentation soit associée à un monoïde simplifiable à gauche, il est nécessaire qu'il n'y ait pas de relation $s\ldots = s\ldots$ et réciproquement, que même sans relation de ce type, il existe des présentations G-complètes associées à des monoïdes non simplifiables. Dans la preuve, les relations de la présentation $(\mathtt{a}, \mathtt{b}, \mathtt{c};\ \mathtt{ca} = \mathtt{ba}, \mathtt{cb} = \mathtt{ba})$ suggèrent que la simplifiabilité puisse être liée à la forme particulière de cette présentation, c'est-à-dire possédant deux relations $su = w$ et $sv = w$ avec $u \neq v$ et w ne commençant pas par un s. Ce n'est pas le cas :

Proposition 5.2. *Il existe une présentation G-complète $(\mathcal{S}; \mathcal{R})$ dont le monoïde associé $\langle \mathcal{S}; \mathcal{R} \rangle^+$ est non simplifiable à gauche et telle que $\mathcal{R}$ ne contienne pas de paire de relations $su = w$, $sv = w$ avec $u \neq v$ et w ne commençant pas par s.*

Démonstration. Soit la présentation

$$(\mathcal{S}; \mathcal{R}) = (\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{r}, \mathtt{s}, \mathtt{t};\ \mathtt{sba} = \mathtt{tca}, \mathtt{cab} = \mathtt{bb}, \mathtt{tbb} = \mathtt{rcb}, \mathtt{sa} = \mathtt{rc})$$

munie de l'ordre deglex induit par $\mathtt{a} < \mathtt{b} < \mathtt{c} < \mathtt{r} < \mathtt{t} < \mathtt{s}$. Par la proposition 2.18 cette présentation est G-complète. On a cependant, on a $\mathtt{sab} \equiv \mathtt{rcb}$ et $\mathtt{sbab} \equiv \mathtt{rcb}$ et donc $\mathtt{sbab} \equiv \mathtt{sab}$. Si le monoïde est simplifiable à gauche, alors on a $\mathtt{bab} \equiv \mathtt{ab}$. Or $\mathtt{bab}$ et $\mathtt{ab}$ sont tous deux réduits : comme ils sont non égaux, ils sont non équivalents. □

Contrairement au retournement, il n'apparaît donc pas clairement de caractérisation ou même de critère permettant de déterminer si une présentation de monoïde G-complète est associée à un monoïde simplifiable ou non.

CHAPITRE III

RETOURNEMENT ITÉRÉ

Dans ce chapitre, nous introduisons une relation moins fine que — mais basée sur — le retournement, permettant ainsi de détecter plus d'équivalences, notamment dans des cas de présentations de monoïdes R-incomplètes.

Le retournement de mot est un procédé de réécriture des mots simple à décrire et qui est bien adapté à l'utilisation d'un ordinateur, particulièrement lorsqu'à chaque étape il n'existe qu'une règle de réécriture — ce cas est dit complémenté. Un des intérêts du retournement est de résoudre — dans les bons cas — le problème du mot associé à une présentation. Toutefois, on a vu au chapitre I que le retournement ne permet pas de répondre au problème dans tous les cas, par exemple lorsque la présentation qu'on considère n'est pas R-complète ou bien lorsque la présentation est R-complète mais que les suites de retournement ne sont pas de longueur finie. Dans cette dernière situation, le retournement donne une semi-solution au problème du mot : toutes les équivalences sont détectées en un temps fini mais le processus de retournement peut ne pas terminer dans le cas contraire.

Dans les bons cas, on peut R-compléter une présentation (algorithme I.5.1) de telle sorte que le monoïde associé à la présentation R-complétée admet un problème du mot résoluble par retournement. Mais en général, on ne sait pas si une présentation est R-complète et on ne sait pas si la R-compléter est réalisable en un temps fini ou non.

Dans ce chapitre on définit un nouveau procédé de réécriture des mots, fondé sur le retournement de mot, et qu'on appelle *retournement itéré* : partant d'un mot w, on le retourne d'abord en $u_1 v_1^{-1}$ avec u_1, v_1 positifs, on permute les facteurs en $v_1^{-1} u_1$, qu'on retourne à son tour en $u_2 v_2^{-1}$ avec u_2, v_2 positifs, on permute les facteurs en $v_2^{-1} u_2$, et on recommence. On montre qu'il existe des présentations (R-incomplètes) telles que deux mots u et v représentent le même élément du monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ si et seulement si le retournement itéré du mot $u^{-1}v$ aboutit au mot vide. En appelant *degré* d'un retournement itéré le nombre de retournements réalisés, on montre :

> **Proposition :** *Le problème de mot du monoïde d'Heisenberg est résoluble par retournement itéré de degré* 2*. Le problème de mot du groupe d'Heisenberg est*

résoluble par retournement itéré de degré 3*.*

La présentation standard du monoïde d'Heisenberg fut la première pour laquelle on prouva que le problème de mot du monoïde nécessitait un retournement double. On donne dans ce chapitre d'autres exemples de présentation présentant cette même propriété. Par contre on ne connaît pas d'exemples de monoïde où un retournement plus que double est nécessaire.

Par ailleurs, on aborde le lien entre retournement et problème de mot du groupe et on montre

> **Proposition :** *Si le problème de mot du monoïde* $\langle \mathcal{S}; \mathcal{R} \rangle^+$ *est résoluble par retournement itéré de degré* d *(c'est-à-dire qu'on procède à* d *retournements successifs) et que* $\langle \mathcal{S}; \mathcal{R} \rangle^+$ *se plonge dans* $\langle \mathcal{S}; \mathcal{R} \rangle$*, alors le problème de mot du groupe* $\langle \mathcal{S}; \mathcal{R} \rangle$ *est résoluble par retournement itéré de degré* $d + 1$*.*

Le chapitre est organisé comme suit. Dans la section 1, nous définissons le retournement itéré et les notions rattachées. Nous montrons ensuite qu'un groupe possédant admettant une présentation dite RI-complète a un problème du mot soluble et on étend le résultat aux monoïdes, sous certaines conditions. Nous introduisons également un nombre — qu'on appelle le RI-degré — décrivant une propriété du retournement itéré et nous décrivons les présentations de RI-degré 1 et 2. Dans la section 2, nous donnons des exemples de présentations de RI-degré 3, dont la présentation standard d'Heisenberg fait partie. Finalement, dans la section 3 nous montrons qu'il existe également des présentations RI-incomplètes et en donnons des exemples.

1 RETOURNEMENT ITÉRÉ ET RI-COMPLÉTUDE

1.1 RETOURNEMENT ITÉRÉ

Rappelons deux définitions du chapitre I.

Définition 1.1 (présentation complémentée, forte convergence)**.** Une présentation de monoïde $(\mathcal{S}; \mathcal{R})$ est *complémentée* si, pour tout couple de lettres distinctes s, t de $\mathcal{S}$, il existe au plus une relation $s \ldots = t \ldots$. Le retournement associé à la présentation de monoïde complémentée $(\mathcal{S}; \mathcal{R})$ est *fortement convergent* — ou simplement, la présentation $(\mathcal{S}; \mathcal{R})$ est *fortement convergente* — si, pour tous mots u et v sur $\mathcal{S}$, il existe des mots u' et v' sur $\mathcal{S}$ tels qu'on ait $u^{-1}v \curvearrowright_{\mathcal{R}} v'u'^{-1}$.

Remarque 1.2. Il ne suffit pas qu'une présentation complémentée $(\mathcal{S}; \mathcal{R})$ possède, pour toute paire de lettres s, t de $\mathcal{S}$, au moins une relation $s \ldots = t \ldots$ pour qu'elle soit fortement convergente. Considérons la présentation de Baumslag-Solitar $(\mathtt{a}, \mathtt{b}; \mathtt{ba} = \mathtt{a}^2\mathtt{b})$; la suite de retournements issue du mot $\mathtt{b}^{-1}\mathtt{ab}$ est de longueur infinie. On a cependant la réciproque :

Fait 1.3. *Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde complémentée fortement convergente. Pour tous s,t de $\mathcal{S}$, il existe une relation $s\ldots = t\ldots$ dans $\mathcal{R}$.*

Démonstration. Soient deux lettres s et t de $\mathcal{S}$ et montrons qu'il existe une relation $s\ldots = t\ldots$. Comme $(\mathcal{S};\mathcal{R})$ est fortement convergente, il existe des mots u et v sur $\mathcal{S}$ vérifiant $s^{-1}t \curvearrowright_{\mathcal{R}} uv^{-1}$, ce qui, par définition du retournement, montre que $su = tv$ est une relation de $\mathcal{R}$. □

Définition 1.4 (présentation rectifiante)**.** On dit que la présentation $(\mathcal{S};\mathcal{R})$ est *rectifiante* si $(\mathcal{S};\mathcal{R})$ est une présentation de monoïde complémentée fortement convergente.

Des exemples de présentations rectifiantes sont les présentations d'Artin-Tits des groupes de tresses (voir p. 71), qui sont de plus R-complètes. Cette situation n'est pas générale : les présentations rectifiantes ne sont pas nécessairement R-complètes. Toutefois, dans certains cas — dont un exemple typique est la présentation d'Heisenberg (exemple 1.13) —, itérer le retournement pallie la R-incomplétude, c'est-à-dire que partant de deux mots u et v positifs et équivalents, une suite de retournements partant de $u^{-1}v$ s'achève par le mot vide.

Définition 1.5 (retournement itéré)**.** Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante et soit w un mot sur $\mathcal{S}\cup\mathcal{S}^{-1}$. La suite, finie ou infinie, de couples de mots positifs $(N_0(w),D_0(w))$, $(N_1(w),D_1(w))$, … est un *retournement itéré* de w si elle vérifie
- $w \curvearrowright_{\mathcal{R}} N_0(w)D_0(w)^{-1}$ ou $w = N_0(w)D_0(w)^{-1}$,
- pour $i\geq 0$, $D_i(w)^{-1}N_i(w) \curvearrowright_{\mathcal{R}} N_{i+1}(w)D_{i+1}(w)^{-1}$, et
- aucune suite plus longue ne vérifie les deux premiers points.

Par définition de la notion de présentation rectifiante, on a immédiatement le fait suivant.

Fait 1.6. *Sous les hypothèses de la définition 1.5, tout mot admet un retournement itéré et celui-ci est unique.*

Démonstration. L'unicité provient du fait que la présentation est complémentée. La forte convergence du retournement implique que, pour tout mot w de $(\mathcal{S}\cup\mathcal{S}^{-1})^*$, il existe deux mots u,v de $\mathcal{S}^*$ vérifiant $w \curvearrowright uv^{-1}$. □

Définition 1.7 (longueur)**.** Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante et soit w un mot sur $\mathcal{S}\cup\mathcal{S}^{-1}$. La *longueur* $\Delta(w)$ du retournement itéré de w est la longueur, c'est-à-dire le nombre d'éléments, de la suite $(N_0(w),D_0(w))$, $(N_1(w),D_1(w))$, … si elle est finie et ∞ sinon.

Notation. Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante. Soient w,w' des mots sur $(\mathcal{S}\cup\mathcal{S}^{-1})$. Pour $p\in\mathbb{N}^*$, la notation $w \curvearrowright_{\mathcal{R}}^{\boxed{p}} w'$ signifie qu'on a $\Delta(w)=p$ et $w' = N_{p-1}(w)D_{p-1}^{-1}(w)$. La notation $w \curvearrowright_{\mathcal{R}}^{\boxed{*}} w'$ signifie qu'il existe p de $\mathbb{N}^*$ pour lequel on a $w \curvearrowright_{\mathcal{R}}^{\boxed{p}} w'$.

Exemple 1.8. La présentation d'Artin-Tits du monoïde de tresses B_4^+ est

$$(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{bab} = \mathtt{aba}, \mathtt{ca} = \mathtt{ac}, \mathtt{cbc} = \mathtt{bcb})$$

et est donc rectifiante. On calcule facilement que le retournement itéré de Ca est la suite infinie constante $(\mathtt{a}, \mathtt{c})$, $(\mathtt{a}, \mathtt{c}), \ldots$ et donc on a $\Delta(\mathtt{Ca}) = \infty$. Pour le mot ABaAba, on obtient la suite finie $(\mathtt{b}, \mathtt{b})$, $(\varepsilon, \varepsilon)$ d'où on déduit $\Delta(\mathtt{ABaAba}) = 2$.

Remarque 1.9. Dans la définition du retournement itéré, on peut affaiblir les hypothèses et ne plus supposer la présentation $(\mathcal{S}; \mathcal{R})$ rectifiante mais seulement saturée, c'est-à-dire que pour toute paire s, t de $\mathcal{S}$ il existe une relation $s \ldots = t \ldots$ dans $\mathcal{R}$. Dans ce cas, la notion de retournement itéré existe encore, mais on perd l'unicité et des comportements très différents apparaissent sur des exemples simples. La présentation de monoïde $(\mathtt{a}, \mathtt{b}; \mathtt{ab}^2 = \mathtt{b}^2\mathtt{a}, \mathtt{ba}^2 = \mathtt{a}^2\mathtt{b})$ est complémentée et saturée. Soit w le mot AABaab. Nous allons construire des retournements itérés finis et infinis issus de w. Comme on a la relation $\mathtt{baa} = \mathtt{aab}$, on a le retournement itéré de longueur 1 $(\varepsilon, \varepsilon)$, c'est-à-dire $N_0(w) = D_0(w) = \varepsilon$. Mais, comme l'illustre la figure 1, on a aussi le retournement de longueur 2 $(\mathtt{b}, \mathtt{b})$, $(\varepsilon, \varepsilon)$.

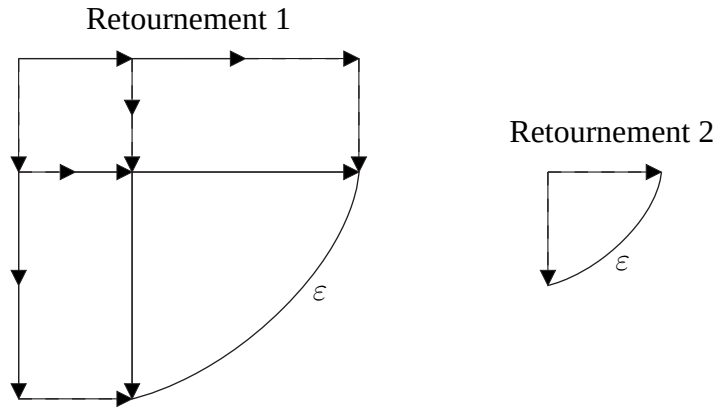


FIGURE 1 – Les flèches pleines représentent la lettre a, les tiretées représentent la lettre b. Dans le cas des présentations non complémentées, d'un même mot peuvent être construits plusieurs retournement itérés différents. Comme $\mathtt{baa} = \mathtt{aab}$ est une relation de la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{ab}^2 = \mathtt{b}^2\mathtt{a}, \mathtt{ba}^2 = \mathtt{a}^2\mathtt{b})$, on a le retournement (itéré) $\mathtt{AABaab} \curvearrowright \varepsilon$ de longueur 1. Le diagramme de gauche montre un autre retournement de AABaab menant à un retournement itéré de longueur 2.

Outre ces retournements itérés finis, le mot w admet des retournements itérés de longueurs infinies : le mot AABaab se retourne en babbaBBBAA, qui, à son tour, se retourne

en abaabAAABB. Or le mot AAABBabaab se retourne en le mot de départ AABaab, d'où on conclut que de w sont issus des retournements itérés arbitrairement grands (voir figure 2).

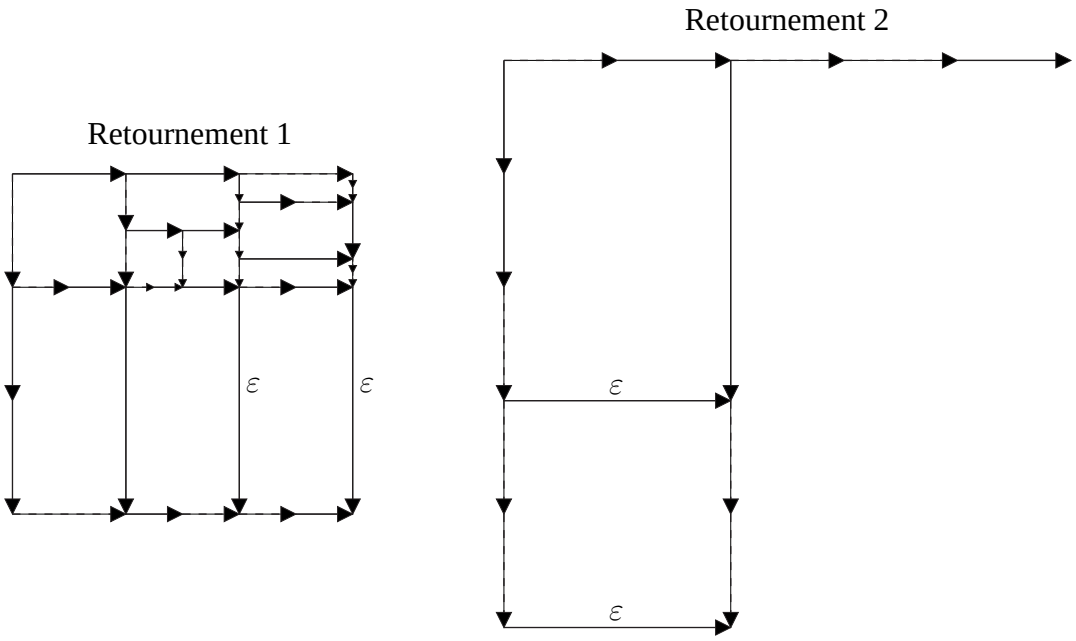


FIGURE 2 – Les flèches pleines représentent la lettre a, les tiretées la lettre b. Dans le cas des présentations non complémentées, d'un même mot peuvent être construits plusieurs retournement itérés différents. Comme $\mathtt{baa} = \mathtt{aab}$ est une relation de la présentation $(\mathtt{a}, \mathtt{b}; \mathtt{ab}^2 = \mathtt{b}^2\mathtt{a}, \mathtt{ba}^2 = \mathtt{a}^2\mathtt{b})$, on a le retournement (itéré) $\mathtt{AABaab} \curvearrowright \varepsilon$ de longueur 1. Le diagramme de gauche montre un autre retournement de AABaab menant à un retournement itéré de longueur infinie : à la deuxième étape de retournement (diagramme de droite), le retournement de BBBAAbabba conduit à retourner BBAbba. Comme les relations de la présentation sont symétriques en les lettres a et b, retourner BBAbba revient à retourner AABaab, le mot de départ.

On rappelle quelques notations introduites à la section I.1.1. Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde. On note $\equiv_{\mathcal{R}}$ la plus petite congruence sur $\mathcal{S}$ contenant $\mathcal{R}$ et on note $\equiv_{\mathcal{R}}^{\pm}$ la plus petite congruence sur l'ensemble $\mathcal{S} \cup \mathcal{S}^{-1}$ contenant $\mathcal{R}$ (donc $\equiv_{\mathcal{R}}$ aussi) et toutes les paires $\{ss^{-1}, \varepsilon\}$, $\{s^{-1}s, \varepsilon\}$ avec s dans $\mathcal{S}$.

Définition 1.10 (trivialité)**.** Soit $(\mathcal{S}; \mathcal{R})$ une présentation de monoïde. Soit w un mot sur $\mathcal{S} \cup \mathcal{S}^{-1}$. On dit que w est $\equiv_{\mathcal{R}}^{\pm}$*-trivial* si on a $w \equiv_{\mathcal{R}}^{\pm} \varepsilon$.

Exemple 1.11. Étant donnée une présentation de monoïde $(\mathcal{S}; \mathcal{R})$, si u est un mot sur $\mathcal{S} \cup \mathcal{S}^{-1}$, alors le mot uu^{-1} est $\equiv_{\mathcal{R}}^{\pm}$-trivial. Un cas plus intéressant de mot $\equiv_{\mathcal{R}}^{\pm}$-trivial est le mot

formé comme suit : soient u et v deux mots positifs et $\equiv_{\mathcal{R}}$-équivalents ; alors le mot $u^{-1}v$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial.

Définition 1.12 (RI-complétude, RI-degré)**.** Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante. La présentation $(\mathcal{S};\mathcal{R})$ est *RI-complète* si pour tout mot $\equiv^{\pm}_{\mathcal{R}}$-trivial w de $\mathcal{S}\cup\mathcal{S}^{-1}$ il existe un entier $p = p(w)$, le *RI-degré* de w, pour lequel on a $w \curvearrowright^{\boxed{p}}_{\mathcal{R}} \varepsilon$. Si la présentation $(\mathcal{S};\mathcal{R})$ est RI-complète, le *RI-degré*, ou simplement le *degré*, de $(\mathcal{S};\mathcal{R})$ est $\sup\{p(w); w \in (\mathcal{S}\cup\mathcal{S}^{-1})^*$ et $w \equiv^{\pm}_{\mathcal{R}} \varepsilon\}$.

L'exemple suivant montre que la notion de RI-complétude diffère de celle de R-complétude, à savoir qu'il existe des présentations RI-complètes non R-complètes.

Exemple 1.13. La présentation d'Heisenberg

$$(\mathcal{H}) \qquad (\mathtt{a},\mathtt{b},\mathtt{c};\mathtt{ab}=\mathtt{bac},\mathtt{ac}=\mathtt{ca},\mathtt{bc}=\mathtt{cb})$$

est rectifiante : posons $\mathcal{S}' = \{\mathtt{a},\mathtt{b}\}\cup\{\mathtt{c}^n,\mathtt{ac}^n; n\in\mathbb{N}\}$. On vérifie facilement que l'ensemble $\mathcal{S}'$ contient $\{\mathtt{a},\mathtt{b},\mathtt{c}\}$ et est clos par $\backslash$, et que $u,v\in\mathcal{S}'$ implique l'existence de $u\backslash v$. D'après la proposition I.2.11, le retournement associé à la présentation $\mathcal{H}$ est donc fortement convergent montrant que $\mathcal{H}$ est rectifiante. On sait que $\mathcal{H}$ est R-incomplète (proposition II.4.19) : l'équivalence $\mathtt{cba}\equiv\mathtt{ab}$ n'est pas prouvable par retournement sans avoir R-complété $\mathcal{H}$ préalablement. On montrera toutefois à la proposition 2.5 que la présentation d'Heisenberg est RI-complète de degré 3 : par exemple, de l'équivalence $\mathtt{cba}\equiv\mathtt{ab}$ on tire que le mot $\mathtt{ABCab}$ est $\equiv^{\pm}$-trivial et donc le retournement itéré de $\mathtt{ABCab}$ aboutit en au plus trois étapes au mot vide ε. On a tout d'abord la suite de retournements

$$\mathtt{AB[Ca]b} \curvearrowright \mathtt{A[Ba]Cb} \curvearrowright \mathtt{AacB[Cb]} \curvearrowright \mathtt{[Aa]c[Bb]C} \curvearrowright \mathtt{cC}.$$

Malgré l'équivalence $\mathtt{cba}\equiv\mathtt{ab}$, on n'a pas $(\mathtt{cba})^{-1}\mathtt{ab}\curvearrowright\varepsilon$ (la présentation $\mathcal{H}$ n'est pas R-complète). On vérifie cependant qu'on a $(\mathtt{cba})^{-1}\mathtt{ab}\curvearrowright^{\boxed{2}}\varepsilon$ puisque $\mathtt{Cc}$ se retourne en ε.

1.2 RI-COMPLÉTUDE

À partir des résultats classiques concernant le retournement, on montre une condition nécessaire à la RI-complétude puis on donne des conditions pour que le retournement itéré associé à la présentation $(\mathcal{S};\mathcal{R})$ résolve les problèmes du mot du monoïde $\langle\mathcal{S};\mathcal{R}\rangle^+$ et du groupe $\langle\mathcal{S};\mathcal{R}\rangle$.

Lemme 1.14. *Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante. Les conditions suivantes sont équivalentes.*

(i) *Le mot w est $\equiv^{\pm}_{\mathcal{R}}$-trivial ;*

(ii) *il existe un entier p tel que $N_p(w)D_p(w)^{-1}$ soit $\equiv^{\pm}_{\mathcal{R}}$-trivial ;*

(iii) pour tout entier p, le mot $N_p(w)D_p(w)^{-1}$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial.

Démonstration. Soit w un mot et considérons son retournement itéré. Posons $w_0 = w$ et pour $n > 0$, posons $w_n = D_{n-1}(w)^{-1}N_{n-1}(w)$. De même, on pose $w'_0 = N_0(w)D_0(w)^{-1}$ et pour $n > 0$, on pose $w'_n = N_n(w)D_n(w)^{-1}$. Pour montrer le lemme, il suffit de montrer qu'on a $w_n \equiv^{\pm} w'_n \equiv^{\pm} w_{n+1}$ pour $n \geq 0$. La première équivalence est donnée par la proposition I.1.7. Quant à la deuxième, on a $N_n(w)D_n(w)^{-1} \equiv^{\pm} \varepsilon$ d'où $N_n(w) \equiv^{\pm} D_n(w)$. On en déduit l'équivalence $D_n(w)^{-1}N_n(w) \equiv^{\pm} \varepsilon$ de laquelle on tire $N_n(w)D_n(w)^{-1} \equiv^{\pm} D_n(w)^{-1}N_n(w)$ soit $w'_n \equiv^{\pm} w_{n+1}$. □

D'après le lemme précédent, la $\equiv^{\pm}$-trivialité d'un mot est lisible dans le retournement itéré à tout rang. Mais cela ne fournit pas un moyen de détecter la $\equiv^{\pm}$-trivialité. Le lemme suivant donne un tel moyen dans le cas des présentations rectifiantes RI-complètes.

Lemme 1.15. *Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante RI-complète. Alors un mot w de $(\mathcal{S}\cup\mathcal{S}^{-1})^*$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial si et seulement si on a $w \curvearrowright^{\boxed{*}}_{\mathcal{R}} \varepsilon$.*

Démonstration. Soit w un mot de $(\mathcal{S}\cup\mathcal{S}^{-1})^*$. Comme $(\mathcal{S};\mathcal{R})$ est RI-complète, si w est $\equiv^{\pm}_{\mathcal{R}}$-trivial, alors il existe un entier p pour lequel on a $D_p(w) = N_p(w) = \varepsilon$. Réciproquement, si le retournement itéré finit par $N_p(w) = D_p(w) = \varepsilon$ alors le mot $N_p(w)D_p(w)^{-1}$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial et, par le lemme 1.14, w aussi. □

On donne maintenant une condition nécessaire à la RI-complétude.

Proposition 1.16. *Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante RI-complète. Alors quels que soient les mots u, v de $\mathcal{S}^*$, on a l'équivalence*

$$u \equiv^{\pm}_{\mathcal{R}} v \Leftrightarrow \exists w \in \mathcal{S}^*,\ (uw \equiv_{\mathcal{R}} vw).$$

Démonstration. On suppose que la présentation $(\mathcal{S};\mathcal{R})$ est RI-complète. Soient u, v des mots de $\mathcal{S}^*$ tels qu'il existe w dans $\mathcal{S}^*$ vérifiant $uw \equiv_{\mathcal{R}} vw$. On a donc $uw \equiv^{\pm}_{\mathcal{R}} vw$ et, par multiplication à droite par w^{-1}, on a $u \equiv^{\pm}_{\mathcal{R}} v$. Réciproquement, supposons qu'on a $u \equiv^{\pm}_{\mathcal{R}} v$ avec u, v deux mots de $\mathcal{S}^*$, autrement dit $u^{-1}v$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial. Comme $(\mathcal{S};\mathcal{R})$ est RI-complète, il existe un entier positif p satisfaisant $\Delta(u^{-1}v) = p$. Posons, pour $0 \leq i \leq p$, $u_i = D_i(w)$ et $v_i = N_i(w)$. D'après le diagramme de retournements de la figure 3 et la proposition I.1.5 , on a $uw \equiv_{\mathcal{R}} vw$ avec $w = v_0 \dots v_{p-1}$. □

1.3 SOLUTION AU PROBLÈME DU MOT

Lorsque le degré d'une présentation RI-complète $(\mathcal{S};\mathcal{R})$ est fini, le retournement itéré est un moyen simple de résoudre le problème du mot du groupe $\langle\mathcal{S};\mathcal{R}\rangle$.

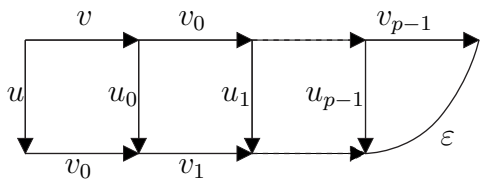


FIGURE 3 – Comme la présentation $(\mathcal{S};\mathcal{R})$ est RI-complète, le retournement itéré du mot $\equiv^{\pm}_{\mathcal{R}}$-trivial $u^{-1}v$ se termine par le mot vide ε. On lit sur le diagramme l'équivalence dans le monoïde $u \cdot v_0 \dots v_{p-1} \equiv v \cdot v_0 \dots v_{p-1}$.

Proposition 1.17. *Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante RI-complète de degré fini. Le retournement itéré fournit une solution au problème du mot du groupe $\langle \mathcal{S};\mathcal{R}\rangle$.*

Démonstration. Soit w un mot de $(\mathcal{S}\cup\mathcal{S}^{-1})^*$ et notons d le degré de $(\mathcal{S};\mathcal{R})$. Supposons qu'on ait $\Delta(w) = p$ avec $p \leq d$. Supposons $N_p(w) = D_p(w) = \varepsilon$. Du lemme 1.14, on déduit que le mot w est $\equiv^{\pm}_{\mathcal{R}}$-trivial et donc qu'il représente l'élément neutre de $\langle \mathcal{S};\mathcal{R}\rangle$. L'autre cas est qu'un seul des deux mots $N_p(w), D_p(w)$ est le mot vide. Dans ce cas le mot $D_p(w)^{-1}N_p(w)$ n'est pas $\equiv^{\pm}_{\mathcal{R}}$-trivial et donc w non plus. Supposons maintenant $\Delta(w) > d$. D'après le lemme 1.15, le mot w n'est pas $\equiv^{\pm}_{\mathcal{R}}$-trivial, donc ne représente pas l'élément neutre de $\langle \mathcal{S};\mathcal{R}\rangle$. □

Remarque 1.18. La proposition 1.17 ne se prolonge pas telle quelle au monoïde $\langle \mathcal{S};\mathcal{R}\rangle^+$: le fait que le retournement itéré d'un mot négatif-positif $u^{-1}v$ termine par le mot vide ne prouve pas en général l'équivalence $u \equiv v$. Autrement dit, le fait que deux mots sur $\mathcal{S}^*$ représentent le même élément du groupe $\langle \mathcal{S};\mathcal{R}\rangle$ n'implique pas qu'ils représentent le même élément du monoïde $\langle \mathcal{S};\mathcal{R}\rangle^+$. En effet, considérons la présentation rectifiante $(\mathtt{a},\mathtt{b},\mathtt{c};\mathtt{ab}=\mathtt{ba},\mathtt{bc}=\mathtt{cb},\mathtt{ab}=\mathtt{cb})$ et le mot w valant $\mathtt{Ac}$. Le retournement itéré de w mène en deux étapes au mot vide : le premier retournement est $\mathtt{Ac} \curvearrowright \mathtt{bB}$ et le deuxième $\mathtt{Bb} \curvearrowright \varepsilon$. Pourtant, on n'a pas $\mathtt{a} \equiv \mathtt{c}$ puisque qu'aucune relation de la présentation ne fait intervenir de mots d'une lettre. On donne toutefois un résultat partiel dans cette direction à la proposition 1.19.

Proposition 1.19. (i) *Supposons que $(\mathcal{S};\mathcal{R})$ est une présentation rectifiante RI-complète et que le monoïde $\langle \mathcal{S};\mathcal{R}\rangle^+$ est simplifiable à droite. Alors, pour tous les mots u, v sur $\mathcal{S}$, on a*

$$u \equiv_{\mathcal{R}} v \Leftrightarrow u^{-1}v \curvearrowright_{\mathcal{R}}^{\boxed{*}} \varepsilon.$$

(ii) *De plus, si $(\mathcal{S};\mathcal{R})$ est de degré $d+1$, alors on a, avec $k \leq d$,*

$$u \equiv_{\mathcal{R}} v \Leftrightarrow u^{-1}v \curvearrowright_{\mathcal{R}}^{\boxed{k}} \varepsilon.$$

Démonstration. De $u \equiv_{\mathcal{R}} v$, on déduit que $u^{-1}v$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial et comme $(\mathcal{S};\mathcal{R})$ est RI-complète, le retournement itéré de $u^{-1}v$ s'achève par $(\varepsilon,\varepsilon)$. Réciproquement, si le retournement itéré de $u^{-1}v$ s'achève par $(\varepsilon,\varepsilon)$, alors $u^{-1}v$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial. On en déduit $u \equiv^{\pm}_{\mathcal{R}} v$ puis,

par la proposition 1.16, qu'il existe un mot w de $\mathcal{S}^*$ vérifiant $uw \equiv vw$. Comme $\langle \mathcal{S}; \mathcal{R}\rangle^+$ est simplifiable à droite, on conclut par $u \equiv_{\mathcal{R}} v$.

Finalement, supposons que $(\mathcal{S}; \mathcal{R})$ est de degré $d+1$. De $\Delta(vu^{-1}) = \Delta(u^{-1}v) + 1$, on déduit que si la présentation itérée est de degré $d+1$ alors le retournement itéré de $u^{-1}v$ est au plus de longueur d. □

On déduit de la proposition 1.19 une nouvelle condition suffisante pour que le monoïde $\langle \mathcal{S}; \mathcal{R}\rangle^+$ se plonge dans son groupe de fractions $\langle \mathcal{S}; \mathcal{R}\rangle$.

Corollaire 1.20. *Soit $(\mathcal{S}; \mathcal{R})$ une présentation rectifiante RI-complète telle que le monoïde $\langle \mathcal{S}; \mathcal{R}\rangle^+$ soit simplifiable à droite. Alors $\langle \mathcal{S}; \mathcal{R}\rangle^+$ se plonge dans $\langle \mathcal{S}; \mathcal{R}\rangle$. En particulier, $\langle \mathcal{S}; \mathcal{R}\rangle^+$ est simplifiable à gauche.*

Démonstration. D'après la proposition 1.19, si la présentation $(\mathcal{S}; \mathcal{R})$ est RI-complète, alors pour deux mots u, v de $\mathcal{S}^*$, $u \equiv_{\mathcal{R}} v$ est équivalent à $u \equiv^{\pm}_{\mathcal{R}} v$. Ceci signifie que $\langle \mathcal{S}; \mathcal{R}\rangle^+$ se plonge dans $\langle \mathcal{S}; \mathcal{R}\rangle$. Or un monoïde se ploge dans son groupe de fractions si et seulement s'il vérifie les conditions de Ore [9], c'est-à-dire qu'il faut qu'il soit simplifiable et que deux éléments aient un multiple commun. On en déduit donc que $\langle \mathcal{S}; \mathcal{R}\rangle^+$ est simplifiable à gauche. □

On conclut par une solution au problème du mot du monoïde $\langle \mathcal{S}; \mathcal{R}\rangle^+$.

Corollaire 1.21. *Soit $(\mathcal{S}; \mathcal{R})$ une présentation rectifiante RI-complète de degré fini. Si le monoïde $\langle \mathcal{S}; \mathcal{R}\rangle^+$ est simplifiable à droite alors le retournement itéré fournit une solution au problème du mot de $\langle \mathcal{S}; \mathcal{R}\rangle^+$.*

Démonstration. Sous ces hypothèses, si u, v sont des mots sur $\mathcal{S}$, alors $u \equiv_{\mathcal{R}} v$ est équivalent à la $\equiv^{\pm}_{\mathcal{R}}$-trivialité de $u^{-1}v$. La démonstration est alors similaire à celle de la proposition 1.17. □

1.4 PRÉSENTATIONS DE PETIT RI-DEGRÉ

On identifie dans cette section les présentations rectifiantes RI-complètes de degré 1 et 2.

Proposition 1.22. *Aucune présentation rectifiante RI-complète n'est de degré 1.*

Démonstration. Supposons que $(\mathcal{S}; \mathcal{R})$ est une présentation rectifiante RI-complète de degré 1. Posons $w_{u,z,v} = u^{-1}zz^{-1}v$, avec u et v deux mots positifs équivalents et z un mot positif quelconque. Le mot $w_{u,z,v}$ est $\equiv^{\pm}_{\mathcal{R}}$-trivial car on a $u^{-1}zz^{-1}v \equiv^{\pm}_{\mathcal{R}} u^{-1}v \equiv^{\pm}_{\mathcal{R}} \varepsilon$, et puisque que $(\mathcal{S}; \mathcal{R})$ est RI-complète de degré 1, on a $w_{u,z,v} \curvearrowright_{\mathcal{R}} \varepsilon$ et $w_{z,v,z} \curvearrowright_{\mathcal{R}} \varepsilon$. De ces retournements on déduit $z^{-1}v \curvearrowright_{\mathcal{R}} \varepsilon$, pour tous z et v. De la proposition I.1.5 on déduit l'équivalence $z \equiv_{\mathcal{R}} v$ puis qu'il n'y a qu'une seule classe d'équivalence sous $\equiv_{\mathcal{R}}$ et donc

qu'un seul élément dans le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$. Si $\mathcal{S}$ n'a qu'un seul élément alors l'ensemble des relations $\mathcal{R}$ est vide et la présentation $(\mathcal{S}; \mathcal{R})$ présente le monoïde libre à un générateur, ce qui contredit que $\langle \mathcal{S}; \mathcal{R} \rangle^+$ ne possède qu'un élément. Supposons donc $|\mathcal{S}| \geq 2$. Soient s et t distincts de $\mathcal{S}$. Puisque $(\mathcal{S}; \mathcal{R})$ est rectifiante, il existe une unique relation $su = tv$, avec $u, v \in \mathcal{S}^*$. Comme $\langle \mathcal{S}; \mathcal{R} \rangle^+$ ne possède qu'un élément, le mot $s^{-1}t$ est $\equiv_{\mathcal{R}}^{\pm}$-trivial et comme $(\mathcal{S}; \mathcal{R})$ est RI-complète de degré 1, on a $s^{-1}t \curvearrowright_{\mathcal{R}} \varepsilon$, et donc $u = v = \varepsilon$. On en déduit que le monoïde $\langle \mathcal{S}; \mathcal{R} \rangle^+$ est le monoïde libre a un générateur, ce qui est impossible. Il n'y a donc pas de présentation rectifiante RI-complète de degré 1. □

Par construction du retournement itéré, on a le fait simple suivant :

Proposition 1.23. *Une présentation rectifiante est RI-complète de degré 2 si et seulement si elle est R-complète.*

2 DES PRÉSENTATIONS DE RI-DEGRÉ 3

Les présentations de RI-degré 3 sont les premières présentations pour lesquelles le retournement itéré diffère du retournement : il existe des équivalences de mots $u \equiv_{\mathcal{R}} v$ dans le monoïde $(\mathcal{S}; \mathcal{R})$ pour lesquelles le retournement itéré de $u^{-1}v$ termine par le mot vide contrairement au retournement simple.

2.1 EXEMPLE MOTIVANT : LA PRÉSENTATION D'HEISENBERG

La présentation d'Heisenberg

$$(\mathcal{H}) \qquad (\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ab} = \mathtt{bac}, \mathtt{ac} = \mathtt{ca}, \mathtt{bc} = \mathtt{cb}).$$

est rectifiante (exemple 1.13) et n'est pas R-complète (proposition II.4.19), ce qui montre qu'elle n'est pas de RI-degré 2 (proposition 1.23). On montre dans cette section que la présentation d'Heisenberg est RI-complète de degré 3 et ce qui donne une nouvelle résolution du problème du mot associé au groupe (resp. monoïde) d'Heisenberg.

Définition 2.1 (relation s-équilibrée)**.** Soient u et v deux mots sur $\mathcal{S}$. Pour tout s de $\mathcal{S}$, on dit que la relation $u = v$ est *s-équilibrée* si on a $\sharp_s(u) = \sharp_s(v)$.

Exemple 2.2. Les relations de la présentation d'Heisenberg sont $\mathtt{a}$-équilibrées, $\mathtt{b}$-équilibrées mais pas $\mathtt{c}$-équilibrées — pour cette dernière affirmation, il suffit de voir qu'on a $\mathtt{ab} \equiv_{\mathcal{H}} \mathtt{bac}$ mais pas $\sharp_{\mathtt{c}}(\mathtt{ab}) = \sharp_{\mathtt{c}}(\mathtt{bac})$.

Les deux lemmes suivants décrivent les mots produits par le retournement itéré associé à la présentation d'Heisenberg.

Lemme 2.3. *Soient N_l, D_l, N_r et D_r des mots positifs sur l'alphabet $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ tels qu'on ait $D_l \equiv_{\mathcal{H}} N_l$ et $D_l^{-1}N_l \curvearrowright_{\mathcal{H}} N_r D_r^{-1}$. Alors N_r et D_r ne contiennent pas la lettre* a*, autrement dit N_r et D_r sont des mots sur $\{\mathtt{b}, \mathtt{c}\}$.*

Démonstration. Supposons que N_r contienne au moins un a. Considérons celui le plus à gauche dans N_r, c'est-à-dire le seul a vérifiant $N_r = u\mathtt{a}v$, avec u un mot sans a et v un mot quelconque. Cette lettre a est produite par un retournement $\mathtt{c}^{-1}\mathtt{a}$ ou un retournement $\mathtt{b}^{-1}\mathtt{a}$; donc, dans le diagramme de retournement de $D_l^{-1}N_l$, au-dessus de ce a il y a un autre a (voir figure 4).

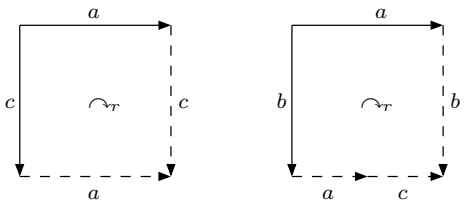


FIGURE 4 – Dans la présentation d'Heinsenberg $\mathcal{H}$, seules les relations $\mathtt{ca} = \mathtt{ac}$ et $\mathtt{ab} = \mathtt{bac}$ produisent une flèche horizontale étiquetée a.

Ce deuxième a est également produit par un des retournements $\mathtt{c}^{-1}\mathtt{a}$ ou $\mathtt{b}^{-1}\mathtt{a}$, et donc à nouveau un a horizontal apparaît. On en déduit qu'au sommet de la pile de retournements au-dessus du premier a il y a déjà un a et que ce a est donc dans N_l. On voit sur le diagramme de la figure 5 que le mot vertical w lu sur le bord gauche de la pile de retournements au-dessus du premier a est de la forme $\mathtt{c}^n\mathtt{b}^e\mathtt{c}^p$, avec $n \geq 0$, $e \in \{0, 1\}$, $p \geq 0$.

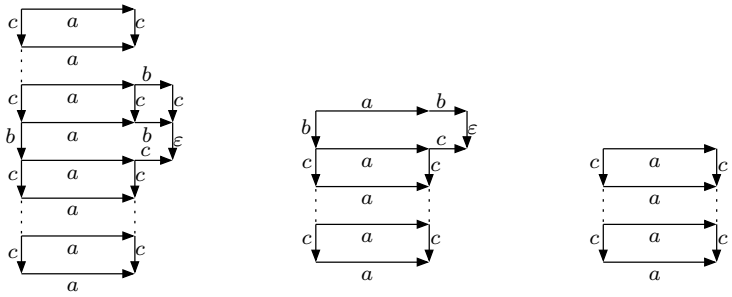


FIGURE 5 – Présentation d'Heisenberg. Au-dessus d'une flèche étiquetée a se dresse une pile de retournements. Tout mot de la forme $\mathtt{c}^n\mathtt{b}^e\mathtt{c}^p$ (avec $n \geq 0$, $e \in \{0, 1\}$, $p \geq 0$) peut apparaître sur le bord gauche de cette pile et ce mot la caractérise complètement.

Supposons maintenant qu'il y ait un b dans w et supposons que w s'écrive $\mathtt{c}^n\mathtt{b}\mathtt{c}^p$ pour n et p deux entiers naturels. Les diagrammes de la figure 6 montrent que soit w n'est pas produit par un retournement soit w est produit par le retournement de $(\mathtt{abc}^{n-1}\mathtt{bc}^p)^{-1}\mathtt{ba}$.

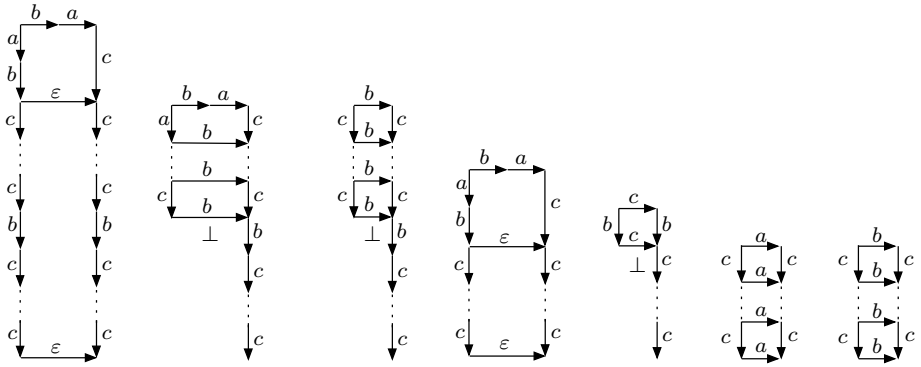


FIGURE 6 – Les différents diagrammes représentent tous les retournements possibles menant à la pile de retournements au-dessus du premier a de N_r.

Si w n'est pas produit par retournement, on a $D_l = w$ et donc $\sharp_{\mathtt{a}}(D_l) = \sharp_{\mathtt{a}}(w) = 0$. D'autre part, on a $\sharp\mathtt{a}(N_l) > 0$. Or les relations de la présentation $\mathcal{H}$ sont a-équilibrées, donc $N_l \equiv_{\mathcal{H}} D_l$ implique $\sharp_{\mathtt{a}}(D_l) = \sharp_{\mathtt{a}}(N_l)$, ce qui est une contradiction. On suppose donc que w est produit par le retournement de $(\mathtt{abc}^{n-1}\mathtt{bc}^p)^{-1}\mathtt{ba}$. Le diagramme de la figure 7 montre que $\mathtt{abc}^{n-1}\mathtt{bc}^p$ ne peut pas être le résultat d'un retournement, donc on en déduit $D_l = \mathtt{abc}^{n-1}\mathtt{bc}^p$.

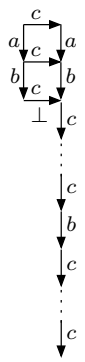


FIGURE 7 – Le diagramme montre que $\mathtt{abc}^{n-1}\mathtt{bc}^p$ ne peut pas être obtenu par retournement dans la présentation d'Heisenberg.

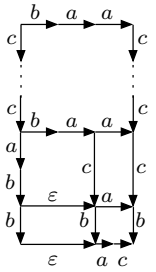


FIGURE 8 – L'équivalence $\mathtt{ba}^2 \cdot \mathtt{c}^{m+1}\mathtt{b} \equiv_{\mathcal{H}} \mathtt{c}^m\mathtt{ab}^2 \cdot \mathtt{ac}$ montre que $\overline{\mathtt{ba}^2}$ ne divise pas $\overline{\mathtt{c}^m\mathtt{ab}^2}$.

On en déduit que le mot $\mathtt{ba}^2$ est un préfixe de N_l et donc, comme on a l'équivalence $N_l \equiv_{\mathcal{H}} D_l$, on déduit que $\overline{\mathtt{ba}^2}$ divise $\overline{D_l}$ (on rappelle que si u est un mot, alors il représente l'élément $\overline{u}$ du monoïde). Or le diagramme de la figure 8 montre que $\overline{D_l}$ n'est pas divisible par $\overline{\mathtt{ba}^2}$. D'où, on conclut que le mot w ne contient pas la lettre b et donc que ce mot est de la forme $\mathtt{c}^n$, pour $n \geq 1$. Les diagrammes de la figure 6 montrent que si $\mathtt{c}^n$ pro-

vient d'un retournement, alors le bord le plus à gauche est $\mathtt{abc}^{n-1}$ ou encore $\mathtt{c}^n$. Comme $\mathtt{c}^n$ est isolé, c'est-à-dire que $\mathtt{c}^n$ est seul dans sa classe d'équivalence, on ne peut avoir $D_l = \mathtt{c}^n$ et donc on exclut ce cas. L'autre cas est similaire au cas $(\mathtt{abc}^{n-1}\mathtt{bc}^p)^{-1}\mathtt{ba} \curvearrowright w$ et on conclut à son impossibilité. Par suite, la supposition que N_r contenait la lettre $\mathtt{a}$ est fausse.

Il reste à montrer que D_r ne contient pas non plus de $\mathtt{a}$. D'après la proposition I.1.5 , le retournement $D_l^{-1}N_l \curvearrowright_{\mathcal{H}} N_rD_r^{-1}$ implique $D_lN_r \equiv_{\mathcal{H}} N_lD_r$ et donc, puisque que le monoïde d'Heisenberg admet la simplification à gauche, $N_r \equiv_{\mathcal{H}} D_r$. Comme les relations de la présentation d'Heisenberg sont $\mathtt{a}$-équilibrées, on déduit de cette dernière équivalence $\sharp_{\mathtt{a}}(N_r) = \sharp_{\mathtt{a}}(D_r)$, prouvant ainsi que D_r non plus ne contient pas de $\mathtt{a}$. □

Lemme 2.4. *Soient N_l, D_l, N_r et D_r des mots positifs sur l'alphabet $\{\mathtt{a},\mathtt{b},\mathtt{c}\}$ tels qu'on ait $D_l \equiv_{\mathcal{H}} N_l$ et $D_l^{-1}N_l \curvearrowright_{\mathcal{H}} N_rD_r^{-1}$. Alors N_r et D_r ne contiennent pas la lettre $\mathtt{b}$, autrement dit N_r, D_r sont des mots sur $\{\mathtt{a},\mathtt{c}\}$.*

La démonstration de ce lemme est identique à celle du lemme 2.3. Avec ces deux lemmes, on montre la RI-complétude de la présentation d'Heisenberg.

Proposition 2.5. *La présentation d'Heisenberg est RI-complète de degré 3.*

Démonstration. Le retournement associé à la présentation d'Heisenberg est fortement convergent (exemple 1.13) et donc, pour tout mot $\equiv_{\mathcal{H}}^{\pm}$-trivial w, il existe des mots N_l, D_l dans $\{\mathtt{a},\mathtt{b},\mathtt{c}\}^*$ vérifiant $w \curvearrowright_{\mathcal{H}} N_lD_l^{-1}$; de plus, $w \equiv_{\mathcal{H}}^{\pm} \varepsilon$ implique $N_l \equiv_{\mathcal{H}}^{\pm} D_l$ et, comme le monoïde d'Heisenberg se plonge dans son groupe de fractions, $N_l \equiv_{\mathcal{H}} D_l$. D'après les lemmes 2.3 et 2.4, les mots N_r et D_r satisfaisant $D_l^{-1}N_l \curvearrowright_{\mathcal{H}} N_rD_r^{-1}$ sont dans $\{\mathtt{c}\}^*$. De la proposition I.1.5 on déduit $D_lN_r \equiv_{\mathcal{H}} N_lD_r$ et par simplification à gauche, on trouve $N_r \equiv_{\mathcal{H}} D_r$. Mais comme N_r et D_r sont dans $\{\mathtt{c}\}^*$ et que tous les mots de $\{\mathtt{c}\}^*$ sont isolés, on a en fait $N_r = D_r$, donc finalement $D_r^{-1}N_r \curvearrowright_{\mathcal{H}} \varepsilon$. □

2.2 PRÉSENTATIONS À R-COMPLÉTION FINIE

À partir de la présentation d'Heisenberg, on construit par produit direct une présentation de RI-degré 3 et de R-complétion finie arbitrairement grande (proposition II.4.17). On donne dans cette section un exemple de présentation de RI-degré 3, dont la R-complétion nécessite l'ajout de plus d'une relation, et qui ne provient pas d'un produit direct.

Lemme 2.6. *La présentation de monoïde*

$$(\mathtt{a},\mathtt{b},\mathtt{c};\ \mathtt{ab}=\mathtt{ba},\ \mathtt{bc}=\mathtt{cb},\ \mathtt{ab}=\mathtt{cb}) \tag{1}$$

est rectifiante. De plus, si N_l et D_l sont deux mots sur $\{\mathtt{a},\mathtt{b},\mathtt{c}\}$ $\equiv$-équivalents, alors il existe un entier p de $[0, |N_l - \sharp_{\mathtt{b}}(N_l)|]$ vérifiant $D_l^{-1}N_l \curvearrowright \mathtt{b}^p\mathtt{b}^{-p}$.

Démonstration. Comme chacune de ses relations implique des mots de longueur 2, la présentation (1) est fortement convergente et donc rectifiante. Posons $\mathcal{S} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. Soient deux mots équivalents N_l et D_l sur $\mathcal{S}$ vérifiant $D_l^{-1}N_l \curvearrowright N_r D_r^{-1}$, avec N_r et D_r deux mots de $\mathcal{S}^*$. Comme les relations de (1) sont $\mathtt{b}$-équilibrées, on a $\sharp_{\mathtt{b}}(N_l) = \sharp_{\mathtt{b}}(D_l)$. Supposons qu'il y ait une lettre $\mathtt{a}$ dans le mot N_l et marquons-le $\dot{\mathtt{a}}$. Alors, dans le retournement de $D_l^{-1}N_l$ en $N_r D_r^{-1}$, trois cas se présentent : soit on a $\mathtt{a}^{-1}\dot{\mathtt{a}} \curvearrowright \varepsilon$, soit on a $\mathtt{c}^{-1}\dot{\mathtt{a}} \curvearrowright \mathtt{b}\mathtt{b}^{-1}$, soit on a $\mathtt{b}^{-1}\dot{\mathtt{a}} \curvearrowright \mathtt{a}\mathtt{b}^{-1}$. Dans les deux premiers cas, il n'y a plus de $\mathtt{a}$ dans la partie retournée. Dans le troisième cas, il reste un $\mathtt{a}$ positif. Mais comme les relations sont $\mathtt{b}$-équilibrées, il y a autant de lettres non-$\mathtt{b}$ dans N_l que dans D_l. Ainsi, chaque $\mathtt{a}$ de N_l est, lors du retournement de $D_l^{-1}N_l$, impliqué dans un retournement $\mathtt{c}^{-1}\mathtt{a} \curvearrowright \mathtt{b}\mathtt{b}^{-1}$ ou dans un retournement $\mathtt{a}^{-1}\mathtt{a} \curvearrowright \varepsilon$. On en déduit que N_r ne contient pas de $\mathtt{a}$. Par un raisonnement identique, on obtient que N_r ne contient pas non plus de $\mathtt{c}$ et que D_r ne contient que des $\mathtt{b}$. Enfin, par homogénéité de la présentation, on a $\sharp_{\mathtt{b}}(N_r) = \sharp_{\mathtt{b}}(D_r)$. □

On en déduit :

Corollaire 2.7. *La présentation* (1) *est de RI-degré 3 et la R-compléter nécessite l'ajout de trois relations.*

Démonstration. On a montré précédemment qu'il faut ajouter trois relations à la présentation (1) pour obtenir une présentation R-complète (proposition II.4.20, (iii)). De plus le lemme 2.6 implique que tout retournement itéré d'un mot $\equiv^{\pm}$-trivial est de longueur au plus 3 et se termine par $(\varepsilon, \varepsilon)$. □

2.3 R-COMPLÉTION INFINIE

Toutes les présentations RI-complètes vues jusqu'à maintenant ont des R-complétions finies : vides dans le cas des présentations de RI-degré 2 et arbitrairement grandes dans le cas des présentations de RI-degré 3.

Question 2.8. *Les présentations rectifiantes RI-complètes de degré 3 sont-elles les présentations R-incomplètes à R-complétion finie ?*

Le but de cette section est de répondre par la négative à cette question.

Lemme 2.9. *La présentation* $(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ba} = \mathtt{ab}, \mathtt{ca} = \mathtt{ac}, \mathtt{ca} = \mathtt{bb})$ *est rectifiante et RI-complète de degré 3.*

Avant de montrer le lemme, on introduit quelques outils et notations utiles à la preuve. Considérons le système de réécriture dont les règles sont

$$(\Sigma) \qquad \begin{array}{rcl} \mathtt{Bb} & \to & \varepsilon, \\ \mathtt{Cc} & \to & \varepsilon, \\ \mathtt{Bc} & \to & \mathtt{b}, \\ \mathtt{Cb} & \to & \mathtt{B}, \end{array}$$

auxquelles on adjoint les règles naturelles $x\varepsilon \to x$, pour $x \in \{\mathtt{B}, \mathtt{C}\}$, ainsi que $\varepsilon x \to x$, pour $x \in \{\mathtt{b}, \mathtt{c}\}$. En appliquant ces règles, on a par exemple la suite de réductions suivante (on note entre crochets le motif qu'on réduit pour passer au mot suivant)

$$\mathtt{BBBC[Bc]ccbc} \to \mathtt{BBB[Cb]ccbc} \to \mathtt{BBB[Bc]cbc} \to \mathtt{BB[Bb]cbc} \to \mathtt{B[Bc]bc} \to \mathtt{[Bb]bc} \to \mathtt{bc},$$

ou encore

$$\mathtt{BB[Bb]c} \to \mathtt{B[Bc]} \to \mathtt{[Bb]} \to \varepsilon.$$

Soit u un mot sur $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. On définit l'application $\mathfrak{b} : \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}^* \to \mathbb{N}$ par

$$\mathfrak{b}(u) = \sharp_{\mathtt{b}}(u) + 2\sharp_{\mathtt{c}}(u).$$

Lemme 2.10. *Soient u et v des mots sur $\{\mathtt{b}, \mathtt{c}\}$ vérifiant $\mathfrak{b}(u) = \mathfrak{b}(v)$. Alors la réduction maximale sous le système de réécriture Σ du mot $u^{-1}v$ est ε .*

Démonstration. Après une réduction par une des quatre premières règles de réécriture de Σ, le mot $u^{-1}v$ est réécrit en $u_1^{-1}v_1$ avec u_1 et v_1 deux mots positifs. Quelle que soit la règle appliquée pour cette réduction, on a $\mathfrak{b}(u) > \mathfrak{b}(u_1)$ et $\mathfrak{b}(u_1) = \mathfrak{b}(v_1)$: la première, la troisième et la quatrième règle font diminuer $\mathfrak{b}(u)$ et $\mathfrak{b}(v)$ de 1 et la deuxième de 2. On démontre donc le résultat par récurrence sur $\mathfrak{b}(u)$. La propagation de la récurrence est claire, il suffit de montrer l'initialisation.

Le cas $\mathfrak{b}(u) = 1$ correspond à $u = v = \mathtt{b}$ et on a $\mathtt{Bb} \to \varepsilon$. Au cas $\mathfrak{b}(u) = 2$ correspondent les différentes possibilités suivantes :

– on a $u = v = \mathtt{c}$, d'où $u^{-1}v = \mathtt{Cc}$ puis $\mathtt{Cc} \to \varepsilon$;

– on a $u = v = \mathtt{bb}$, d'où $u^{-1}v = \mathtt{BBbb}$ puis $\mathtt{B[Bb]b} \to \mathtt{Bb} \to \varepsilon$;

– on a $u = \mathtt{bb}$ et $v = \mathtt{c}$, d'où $u^{-1}v = \mathtt{BBc}$ puis $\mathtt{B[Bc]} \to \mathtt{Bb} \to \varepsilon$;

– on a $u = \mathtt{c}$ et $v = \mathtt{bb}$, d'où $u^{-1}v = \mathtt{Cbb}$ puis $\mathtt{[Cb]b} \to \mathtt{Bb} \to \varepsilon$. □

On est maintenant en mesure de prouver le lemme 2.9.

Démonstration du lemme 2.9. Soient N_l, D_l deux mots équivalents satisfaisant $D_l^{-1}N_l \curvearrowright N_r D_r^{-1}$ avec N_r et D_r deux mots positifs. Comme la lettre $\mathtt{a}$ commute avec toutes les autres, hormis le motif $\mathtt{Aa}$, chaque retournement d'un motif de deux lettres impliquant la lettre $\mathtt{a}$ (donc $\mathtt{Ab}$, $\mathtt{Ac}$, $\mathtt{Ba}$ et $\mathtt{Ca}$) préserve l'autre lettre.

Partant du mot négatif-positif $w_0 = D_l^{-1}N_l$, on effectue d'abord tous les retournements impliquant des $\mathtt{a}$, ce qui mène à un mot de la forme $\mathtt{a}^* w_1 \mathtt{a}^*$, où la notation x^* désigne un nombre quelconque de concaténations de x et w_1 est un mot négatif-positif écrit sur $\{\mathtt{b}, \mathtt{c}\}$. On effectue le seul retournement possible de w_1 suivi, le cas échéant, de tous les retournements possibles impliquant des $\mathtt{a}$. On obtient un mot $\mathtt{a}^* w_2 \mathtt{a}^*$ avec w_2 un mot négatif-positif écrit sur $\{\mathtt{b}, \mathtt{c}\}$. On itère ce processus. Le passage du mot w_n au mot w_{n+1} correspond à l'application d'une règle du système de réécriture Σ décrit plus haut. Comme les mots N_l et D_l sont équivalents, on a $\mathfrak{b}(N_l) = \mathfrak{b}(D_l)$ et, appliquant le lemme 2.10, on conclut que

les mots N_r et D_r sont dans $\{\mathtt{a}\}^*$. Finalement, l'équivalence $D_l N_r \equiv N_l D_r$ implique $|D_l N_r| = |N_l D_r|$, puis, comme les relations de la présentation préservent la longueur, $D_l \equiv N_l$ implique $|D_l| = |N_l|$ et donc $|N_r| = |D_r|$, ce qui revient à $N_r = D_r = \mathtt{a}^p$ pour un certain entier positif p. Le troisième retournement du retournement itéré retourne donc $\mathtt{a}^{-p}\mathtt{a}^p$, avec $p \geq 0$, en le mot vide ε . □

La proposition suivante répond par la négative à la question 2.8 :

Proposition 2.11. *Il existe une présentation rectifiante RI-complète de degré 3 dont la R-complétion est infinie.*

Démonstration. La présentation $(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ba} = \mathtt{ab}, \mathtt{ca} = \mathtt{ac}, \mathtt{ca} = \mathtt{bb})$ possède, d'après la proposition II.4.20, (ii), une R-complétion infinie. On conclut grâce au lemme 2.9. □

3 PRÉSENTATIONS RI-INCOMPLÈTES

On ne connaît pas à ce jour de présentation rectifiante RI-complète de degré supérieur à 3. Dans cette section, on montre, en donnant des exemples, que les présentations rectifiantes et non R-complètes ne sont pas RI-complètes en général. Finalement on montre, pour les présentations vérifiant une certaine hypothèse de finitude, à savoir que la clôture par l'opération $\setminus$ de l'alphabet considéré est fini, que la longueur du retournement itéré est soit inférieure à une borne explicite, soit infini.

3.1 DES COMPORTEMENTS DIVERS

Si une présentation $(\mathcal{S}; \mathcal{R})$ est RI-incomplète, cela signifie qu'il existe un mot $w \equiv^{\pm}_{\mathcal{R}}$-trivial tel que soit le retournement itéré est de longueur finie et ne termine pas par $(\varepsilon, \varepsilon)$, soit le retournement itéré de w est de longueur infinie. Les deux situations se produisent.

Exemple 3.1. Soit la présentation

(2) $\qquad (\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}; \mathtt{ab} = \mathtt{bac}, \mathtt{bc} = \mathtt{cbd}, \mathtt{ab} = \mathtt{cbd}, \mathtt{da} = \mathtt{ad}, \mathtt{db} = \mathtt{bd}, \mathtt{dc} = \mathtt{cd}).$

Les deux relations $\mathtt{ab} = \mathtt{bac}$ et $\mathtt{ab} = \mathtt{cbd}$ impliquent $\mathtt{cbd} \equiv \mathtt{bac}$. Le mot $(\mathtt{bac})^{-1}\mathtt{cbd}$ est donc $\equiv^{\pm}$-trivial. Itérons le retournement à partir de ce mot :

$$\begin{aligned} (\mathtt{bac})^{-1}\mathtt{cbd} &\curvearrowright \mathtt{bd}(\mathtt{bdc})^{-1}, \\ (\mathtt{bd})^{-1}\mathtt{bdc} &\curvearrowright \mathtt{c}. \end{aligned}$$

Le retournement itéré de $(\mathtt{bac})^{-1}\mathtt{cbd}$ termine par (ε, c) et donc la présentation (2) est R-incomplète.

La présentation suivante montre qu'il est possible que le retournement itéré d'un mot $\equiv^{\pm}$-trivial ne termine pas.

Exemple 3.2. Soit la présentation

$$(\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d};\mathtt{ab}=\mathtt{bc},\mathtt{bc}=\mathtt{cbd},\mathtt{ac}=\mathtt{cbd},\mathtt{da}=\mathtt{ad},\mathtt{db}=\mathtt{bd},\mathtt{dc}=\mathtt{cd}). \tag{3}$$

Le mot $\mathtt{c}^{-1}\mathtt{a}\mathtt{a}^{-1}\mathtt{d}$ se retourne en $\mathtt{bdd}(\mathtt{ac})^{-1}$. Du lemme I.1.6 on déduit $\mathtt{dac} \equiv_{\mathcal{R}} \mathtt{cbdd}$ et donc la $\equiv^{\pm}_{\mathcal{R}}$-trivialité de $(\mathtt{cbd}^2)^{-1}\mathtt{dac}$. En itérant le retournement, on obtient :

$$\begin{aligned}(\mathtt{cbd}^2)^{-1}\mathtt{dac} &\curvearrowright_{\mathcal{R}} \mathtt{c}(\mathtt{bd})^{-1}\\ (\mathtt{bd})^{-1}\mathtt{c} &\curvearrowright_{\mathcal{R}} \mathtt{c}(\mathtt{bd}^2)^{-1}\\ (\mathtt{bd}^2)^{-1}\mathtt{c} &\curvearrowright_{\mathcal{R}} \mathtt{c}(\mathtt{bd}^3)^{-1}.\end{aligned}$$

On voit par récurrence que le n^{e} retournement est $(\mathtt{bd}^{n-1})^{-1}\mathtt{c} \curvearrowright \mathtt{c}(\mathtt{bd}^n)^{-1}$. On en déduit que le retournement itéré de $(\mathtt{cbd}^2)^{-1}\mathtt{dac}$ est de longueur infinie. Comme le mot $(\mathtt{cbd}^2)^{-1}\mathtt{dac}$ est $\equiv^{\pm}$-trivial, la présentation (3) est RI-incomplète.

3.2 BORNES SUPÉRIEURES

Si $(\mathcal{S};\mathcal{R})$ est une présentation RI-incomplète, il se peut que le retournement itéré d'un mot $\equiv^{\pm}_{\mathcal{R}}$-trivial soit infini (exemple 3.2). Nous montrons maintenant que dans certains cas de présentations RI-incomplètes, soit la longueur du retournement itéré d'un mot w est inférieure à une certaine borne dépendant de w, soit le retournement itéré de w est infini.

Notation. Soit la présentation de monoïde $(\mathcal{S};\mathcal{R})$ et soit X un ensemble de mots contenant $\mathcal{S}$. Si w est un mot sur $\mathcal{S}$, alors on note $|w|_X$ le nombre minimal p de mots $u_1,\dots,u_p$ de X intervenant dans une décomposition en produit $u_1\dots u_p$ de w. On pose $|\varepsilon|_X = 0$. Si w est un mot sur $(\mathcal{S}\cup\mathcal{S}^{-1})$, alors w se décompose de manière unique en un produit $w_1^{e_1}\dots w_p^{e_p}$ avec chaque mot w_i positif, $e_i = \pm 1$ et deux e_i successifs sont différents. On pose dans ce cas $|w|_X = \sum_{i=1}^{p}|w_i|_X$. Si $(\mathcal{S};\mathcal{R})$ est complémentée, on note $\hat{\mathcal{S}}$ la clôture par $\backslash_{\mathcal{R}}$ de $\mathcal{S}$.

Exemple 3.3. Soit la présentation standard d'Artin-Tits $(\mathtt{a},\mathtt{b};\mathtt{bab}=\mathtt{aba})$ et posons $\mathcal{S} = \{\mathtt{a},\mathtt{b}\}$. On calcule la clôture $\hat{\mathcal{S}}$ de $\mathcal{S}$ par $\backslash_{\mathcal{R}}$ et on trouve $\hat{\mathcal{S}} = \{\varepsilon,\mathtt{a},\mathtt{b},\mathtt{ba},\mathtt{ab}\}$. On a donc $|\mathtt{a}|_{\hat{\mathcal{S}}} = |\mathtt{b}|_{\hat{\mathcal{S}}} = |\mathtt{ab}|_{\hat{\mathcal{S}}} = |\mathtt{ba}|_{\hat{\mathcal{S}}} = 1$. Puis on a $|\mathtt{aa}|_{\hat{\mathcal{S}}} = |\mathtt{bb}|_{\hat{\mathcal{S}}} = 2$, etc. Finalement calculons $|\mathtt{baabBAbbabBaaa}|_{\hat{\mathcal{S}}}$:

$$|\mathtt{baabBAbbabBaaa}|_{\hat{\mathcal{S}}} = \underbrace{|\mathtt{baab}|_{\hat{\mathcal{S}}}}_{2} + \underbrace{|\mathtt{ab}|_{\hat{\mathcal{S}}}}_{1} + \underbrace{|\mathtt{bbab}|_{\hat{\mathcal{S}}}}_{3} + \underbrace{|\mathtt{b}|_{\hat{\mathcal{S}}}}_{1} + \underbrace{|\mathtt{aaa}|_{\hat{\mathcal{S}}}}_{3} = 10.$$

Si w est un mot et X un ensemble, on dit que $|w|_X$ est la X-*longueur* de w. Jusqu'à présent, la seule longueur dont on disposait sur les mots était le nombre de lettres ; or le nombre de lettres varie par retournement, autrement dit, si on a $w \curvearrowright w'$, on n'a pas en général $|w| = |w'|$ — ou même $|w| \geq |w'|$. La $\hat{\mathcal{S}}$-longueur est mieux adaptée au retournement :

Lemme 3.4. *Soit $(\mathcal{S};\mathcal{R})$ une présentation de monoïde et soient w, w' deux mots sur $(\mathcal{S} \cup \mathcal{S}^{-1})^*$. Alors $w \curvearrowright_{\mathcal{R}} w'$ implique $|w|_{\hat{\mathcal{S}}} \geq |w'|_{\hat{\mathcal{S}}}$.*

Démonstration. On ne montre que le cas où le mot w est négatif-positif, le cas général étant une juxtaposition de retournements de mots négatifs-positifs. Posons $w = u^{-1}v$ avec u, v des mots de $\mathcal{S}^*$ de $\hat{\mathcal{S}}$-longueur p et q. On note u', v' les deux mots sur $\mathcal{S}$ de $\hat{\mathcal{S}}$-longueurs p' et q' vérifiant $w \curvearrowright_{\mathcal{R}} v'u'^{-1}$. On montre par récurrence sur $p+q$ qu'on a $p \geq p'$ et $q \geq q'$.

Supposons $p + q = 2$. Le seul cas est $w = u^{-1}v$ avec u, v positifs de $\hat{\mathcal{S}}$-longueur 1. Comme $\hat{\mathcal{S}}$ est clos par retournement, les mots positifs u' et v' sont de $\hat{\mathcal{S}}$-longueur 1 au plus. On suppose maintenant $p + q = n$. Un des deux mots u et v, disons v, est de $\hat{\mathcal{S}}$-longueur supérieure à 1. Soit $\tilde{v}$ un préfixe de v de $\hat{\mathcal{S}}$-longueur $p-1$ et soit z le mot vérifiant $v = \tilde{v}z$. Posons $n = p + q$. Soit $\tilde{v}'$ le mot positif satisfaisant $u^{-1}\tilde{v} \curvearrowright_{\mathcal{R}} \tilde{v}'u'^{-1}$. Par hypothèse de récurrence, $|u^{-1}\tilde{v}|_{\hat{\mathcal{S}}} = n-1$ implique $|\tilde{v}'|_{\hat{\mathcal{S}}} \leq q-1$ et $|u'^{-1}|_{\hat{\mathcal{S}}} \leq p$. Puis, de $p < n$ on déduit par hypothèse de récurrence $u'^{-1}z \curvearrowright_{\mathcal{R}} z'u''^{-1}$, avec z', u'' des mots sur $\mathcal{S}$ et $|z'|_{\hat{\mathcal{S}}} \leq 1$. En combinant ces deux retournements, on conclut qu'on a $p' \leq p$ et $q' \leq q$. □

Proposition 3.5. *Soit $(\mathcal{S};\mathcal{R})$ une présentation rectifiante. Supposons que la clôture $\hat{\mathcal{S}}$ de $\mathcal{S}$ par $\backslash_{\mathcal{R}}$ est finie. Soit w un mot de $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ de $\hat{\mathcal{S}}$-longueur p. Alors on a soit $\Delta(w) \leq (|\hat{\mathcal{S}}| - 1)^p$, soit $\Delta(w) = \infty$.*

Démonstration. Par le lemme 3.4, si w est un mot sur $(\mathcal{S} \cup \mathcal{S}^{-1})$ de $\hat{\mathcal{S}}$-longueur p, alors pour tout i, la $\hat{\mathcal{S}}$-longueur de $D_i(w)^{-1}N_i(w)$ est inférieure à p. Or il y a au plus $(|\hat{\mathcal{S}}| - 1)^p$ mots de $\hat{\mathcal{S}}$-longueur p. Donc soit le retournement itéré de w est de longueur (finie) inférieure à $(|\hat{\mathcal{S}}| - 1)^p$, soit le retournement itéré de w est périodique, donc infini. □

Remarque 3.6. Supposons que w s'écrive uv^{-1} avec u, v des mots de $\mathcal{S}$ et qu'on a en plus $|u|_{\hat{\mathcal{S}}} = |v|_{\hat{\mathcal{S}}}$. Comme les retournements des mots $u^{-1}v$ et $v^{-1}u$ sont symétriques, l'égalité de la proposition 3.5 devient $\Delta(w) \leq \lceil \frac{(|\hat{\mathcal{S}}|-1)^p}{2} \rceil$ où $\lceil x \rceil$ désigne la partie entière supérieure de x.

Une présentation $(\mathcal{S};\mathcal{R})$ pour laquelle calculer la clôture $\hat{\mathcal{S}}$ de $\mathcal{S}$ est simple est le cas où toutes les relations $u = v$ de $(\mathcal{S};\mathcal{R})$ vérifient $|u| \leq 2$ et $|v| \leq 2$. Dans ce cas, on a $\hat{\mathcal{S}} = \mathcal{S} \cup \{\varepsilon\}$ et donc $\hat{\mathcal{S}}$ est finie si $\mathcal{S}$ est finie.

Exemple 3.7. Considérons la présentation

$$(\mathtt{a}, \mathtt{b}, \mathtt{c}; \mathtt{ab} = \mathtt{bc}, \mathtt{ba} = \mathtt{c}^2, \mathtt{ac} = \mathtt{cb}).$$

La clôture $\hat{\mathcal{S}}$ par $\backslash$ de $\mathcal{S}$ est $\mathcal{S} \cup \{\varepsilon\}$. Posons $w = \mathtt{CABacb}$. D'après la proposition 3.5, comme w est de longueur 6, on a au plus 3^6 retournements à effectuer. Le premier retournement donne `cccBCA` et le deuxième `cB`; ceci signifie que la troisième étape consiste à retourner le mot `Bc`, de longueur 2. D'après la remarque 3.6, les $\lceil \frac{3^2}{2} \rceil$ premiers termes du retournement itéré de `Bc` suffisent. Le calcul montre que le retournement itéré de `Bc` est périodique de période 3 et donc qu'on a $\Delta(w) = \infty$.

3.3 PRÉSENTATION RI-INCOMPLÈTE À RETOURNEMENTS ITÉRÉS FINIS

Si $(\mathcal{S};\mathcal{R})$ est une présentation de RI-degré inférieur ou égal à 3 le retournement itéré d'un mot $\equiv^{\pm}_{\mathcal{R}}$-trivial termine par $(\varepsilon,\varepsilon)$ est au plus de longueur 3 étapes. Nous ne connaissons pas à ce jour de présentation de RI-degré 4 ou plus, et donc la question suivante se pose : existe-t-il une présentation pour laquelle des retournements itérés de mots $\equiv^{\pm}$-triviaux se terminent en plus de trois étapes par $(\varepsilon,\varepsilon)$?

Dans cette section, on donne une présentation non RI-complète qui répond affirmativement à la question précédente.

Proposition 3.8. *Il existe une présentation $(\mathcal{S};\mathcal{R})$ satisfaisant l'énoncé suivant :*

(4) *Pour $4 \leq i \leq 12$, il existe un mot w_i sur $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ $\equiv^{\pm}_{\mathcal{R}}$-trivial avec $\Delta(w_i) = i$ et $N_i(w_i) = D_i(w_i) = \varepsilon$.*

Démonstration. Montrons qu'une présentation vérifiant l'énoncé (4) est

(5) $(\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d};\mathtt{adc}=\mathtt{bdc},\mathtt{aa}=\mathtt{cd},\mathtt{ad}=\mathtt{db},\mathtt{bca}=\mathtt{cda},\mathtt{bc}=\mathtt{da},\mathtt{cba}=\mathtt{dcb})$.

Soit w_4 le mot `bBCdcA`. Le retournement itéré de w_4 est

$$(\mathtt{ba},\mathtt{ab}),\ (\mathtt{caa},\mathtt{dca}),\ (\mathtt{dca},\mathtt{dca}),\ (\varepsilon,\varepsilon).$$

Posons $w_5 =$ `cbBCdcAB`, $w_6 =$ `BCCbad`, $w_7 =$ `CCCbcb`, $w_8 =$ `acBCACad`, $w_9 =$ `acDcbCCC`, $w_{10} =$ `dccACaCaCA`, $w_{11} =$ `dbaCBcdcbCDADB` et $w_{12} =$ `cacacbccDDDDBBCB`. C'est une simple — mais longue — vérification de voir qu'on a $\Delta(w_i) = i$ et $N_i(w_i) = D_i(w_i) = \varepsilon$ pour tout i. □

Remarque 3.9. La présentation de la preuve est la plus petite possible en le sens qu'on n'a pas trouvé de présentation sur trois lettres pour laquelle il existe un retournement itéré de mot $\equiv^{\pm}$-trivial de longueur supérieure à 3. De plus, nous n'avons pas trouvé de mots $\equiv^{\pm}$-triviaux dont la longueur du retournement itéré dépassait 12. Trouver le mot w_{12} de la preuve (dont le retournement itéré est de longueur 12) a nécessité plusieurs dizaines de millions d'étapes de retournements et pour trouver un mot $\equiv^{\pm}$-trivial dont le retournement itéré est de longueur supérieure à 13, on a calculé les retournements itérés de plus de vingt millions de mots $\equiv^{\pm}$-triviaux.

Puisqu'il existe des retournements itérés de longueurs supérieures à 3, la présentation 4 n'est pas R-complète. Elle n'est pas non plus RI-complète :

Proposition 3.10. *La présentation* (5) *est RI-incomplète.*

Démonstration. Le calcul du retournement itéré de $\mathtt{Ca}$ montre qu'on a $\Delta(\mathtt{Ca}) = \infty$. Pour montrer que la présentation (5) n'est pas RI-complète, il suffit de montrer que $\mathtt{Ca}$ est $\equiv^{\pm}$-trivial. La relation $\mathtt{adc} = \mathtt{bdc}$ implique $\mathtt{a} \equiv^{\pm} \mathtt{b}$, d'où de la relation $\mathtt{ad} = \mathtt{db}$ on tire $\mathtt{ad} \equiv^{\pm} \mathtt{da}$ et de $\mathtt{bc} = \mathtt{da}$ on déduit $\mathtt{ac} \equiv^{\pm} \mathtt{da}$. En combinant ces résultats, on trouve $\mathtt{ac} \equiv^{\pm} \mathtt{ad}$, puis $\mathtt{c} \equiv^{\pm} \mathtt{d}$. Finalement, de la relation $\mathtt{cba} = \mathtt{dcb}$ on obtient d'abord $\mathtt{dba} \equiv^{\pm} \mathtt{dca}$ puis $\mathtt{b} \equiv^{\pm} \mathtt{c}$. Les équivalences $\mathtt{a} \equiv^{\pm} \mathtt{b} \equiv^{\pm} \mathtt{c} \equiv^{\pm} \mathtt{d}$ impliquent qu'un mot est $\equiv^{\pm}$-trivial dès que la somme des exposants est nulle. Le mot $\mathtt{Ca}$ est donc bien $\equiv^{\pm}$-trivial. □

On conclut ce chapitre sur la question ouverte suivante :

Question 3.11. *Existe-t-il une présentation RI-complète de degré supérieur à 3 ?*

Partie B

Retournement : cas des mots de tresses

CHAPITRE IV

DISTANCE COMBINATOIRE

Dans ce chapitre, nous étudions la distance combinatoire entre mots de tresse et en particulier établissons des critères afin de pouvoir la calculer à partir de diagrammes de van Kampen — et donc de diagrammes de retournement.

Étant donnés deux mots de tresse équivalents u et v, on ne connaît pas de procédé général pour calculer la distance combinatoire entre u et v, notée $\mathrm{dist}(u, v)$, c'est-à-dire, partant de u, le nombre minimal de relations à appliquer pour obtenir v. Une méthode pour majorer $\mathrm{dist}(u, v)$ est de trouver un diagramme de van Kampen pour (u, v), c'est-à-dire un pavage du plan représentant une suite de relations à appliquer pour passer de u à v, un type particulier de tel diagramme étant un diagramme de retournement.

Le point de départ consiste à associer à tout mot de tresse u une suite $\mathrm{P}(u)$ d'éléments de $\{1, \dots, n\}^2 \times \{1, \dots, |u|\}$ et à minorer $\mathrm{dist}(u, v)$ par une fonction explicite de $\mathrm{P}(u)$ et $\mathrm{P}(v)$. D'une part on en déduit

> **Proposition :** *Pour $n \geq 3$, il existe des mots de tresse positifs à n brins u_n et v_n vérifiant $\mathrm{dist}(u_n, v_n) \geq n^4/8$.*

D'autre part, on en déduit plusieurs critères permettant d'établir qu'un diagramme de van Kampen pour (u, v), notons-le $\mathcal{K}$, — ou un diagramme de retournement — est optimal, c'est-à-dire que le nombre de pavés de $\mathcal{K}$ égale $\mathrm{dist}(u, v)$.

Dans le cas des mots de tresse, on montre qu'il existe une façon de nommer chacun des pavés d'un diagramme de van Kampen $\mathcal{K}$ pour des mots équivalents u et v, d'où on tire le premier critère d'optimalité :

> **Critère 1 :** *Si tous les pavés d'un diagramme de van Kampen $\mathcal{K}$ portent un nom différent, alors $\mathcal{K}$ est optimal.*

Dans la section 3, on introduit dans tout diagramme de van Kampen $\mathcal{K}$ associé à des mots de tresse équivalents u, v des courbes, appelées *séparatrices*, réalisant une partition des arêtes de $\mathcal{K}$. On prouve alors un nouveau critère d'optimalité, reformulation du premier dans le langage des séparatrices :

Critère 2 : *Si les séparatrices d'un diagramme de van Kampen $\mathcal{K}$ se croisent au plus une fois, alors $\mathcal{K}$ est optimal.*

Si u, v sont des mots de tresse équivalents, les deux critères ci-dessus établissent un moyen de calculer $\mathrm{dist}(u, v)$ ou, au pire, majorer $\mathrm{dist}(u, v)$, moyennant la connaissance d'un diagramme de van Kampen pour (u, v). Le retournement du mot $u^{-1}v$, avec u, v des mots de tresse, fournit un tel diagramme : partant du diagramme de retournement de $u^{-1}v$, on obtient un diagramme de van Kampen pour (u, v) en identifiant les sommets reliés par des ε-arêtes. Ce lien entre les deux types de diagrammes nous permet de prouver un critère d'optimalité pour les diagrammes de retournement :

Critère 3 : *Si un diagramme de retournement $\mathcal{D}$ ne contient aucune ε-arête, alors $\mathcal{D}$ est optimal.*

Dans la section 1, on rappelle la notion de tresse, de diagramme de tresse et de tresse simple. On montre dans cette section une minoration quartique en le nombre de brins n de la plus grande distance combinatoire entre deux expressions d'une tresse à n brins. Dans la section 2, on définit dans le cadre des tresses la notion de diagramme de van Kampen et on établit un critère sur les pavés pour qu'un diagramme de van Kampen réalise la distance combinatoire, autrement dit, pour qu'il soit optimal. Dans la section 3, on définit la notion de séparatrice et on reformule le critère concernant les pavés en termes de séparatrices. Dans la dernière section, on rapproche la notion connue de diagramme de retournement de celle de diagramme de van Kampen et on établit un critère d'optimalité dans le vocabulaire du retournement.

1 TRESSES

Dans cette section, nous rappelons les définitions standard concernant les tresses, notamment celle de tresse simple. Puis, en considérant un mot de tresse comme une suite de permutations de brins, on donne une nouvelle minoration de la distance combinatoire entre deux mots représentant une tresse simple.

1.1 DIAGRAMMES DE TRESSE

Pour $n \geq 2$, la présentation standard d'Artin-Tits est

$$(\mathcal{A}_n) \qquad \left(\sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{pour } |j-i| = 1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \text{pour } |j-i| \geq 2 \end{array} \right).$$

On appelle *n-tresse*, ou plus simplement *tresse*, un élément du groupe de tresses à n brins B_n, de présentation $(\mathcal{A}_n)$. On appelle *n-mot de tresse* un mot représentant une tresse. Un n-mot de tresse est ainsi un élément du groupe libre sur $n-1$ générateurs $\sigma_1, \dots \sigma_{n-1}$.

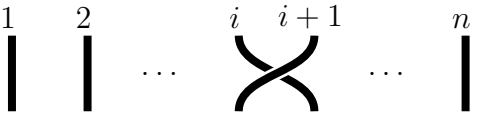
Définition 1.1 (monoïde de tresses B_n^+)**.** On note B_n^+ le monoïde présenté par $(\mathcal{A}_n)$.

C'est un résultat standard que le monoïde B_n^+ se plonge dans B_n [16].

Définition 1.2 (tresse positive)**.** On appelle *tresse positive* une tresse du monoïde B_n^+.

Remarque 1.3. Tout mot écrit uniquement en des puissances positives des générateurs σ_i représente une tresse positive. Inversement, un mot contenant des puissances négatives peut représenter une tresse positive : la tresse représentée par $\sigma_2^{-1}\sigma_1\sigma_2\sigma_1$ est positive. En effet, le mot $\sigma_2^{-1}\sigma_1\sigma_2\sigma_1$ est équivalent à $\sigma_2^{-1}\sigma_2\sigma_1\sigma_2$ et donc à $\sigma_1\sigma_2$.

À chaque lettre σ_i, on associe le diagramme D_{σ_i}

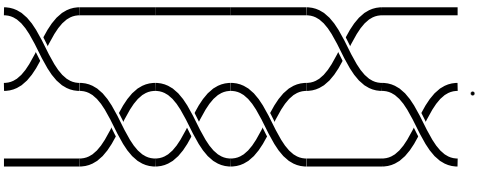


Définition 1.4 (diagramme de tresse)**.** À tout mot u positif, on associe le *diagramme de tresse* D_u composé par l'empilement (du haut vers le bas) des diagrammes D_{σ_i} correspondant aux lettres de u.

Remarque 1.5. Pour des questions de place, on pourra représenter le diagramme D_u à l'horizontale, la lecture se faisant alors de la gauche vers la droite.

On appelle p^{e} *brin*, ou *brin* p, d'un diagramme D_u le brin initialement à la p^{e} position à partir de la gauche en haut du diagramme (resp. à partir du bas à gauche du diagramme) si le diagramme est présenté verticalement (resp. horizontalement).

Exemple 1.6. Le diagramme du mot de tresse $\sigma_2\sigma_1^3\sigma_2\sigma_1$ est



1.2 TRESSES SIMPLES

Définition 1.7. Une tresse b est simple si b est positive et s'il existe un diagramme de tresse représentant b tel que chaque brin croise au plus une fois tout autre brin.

Remarque 1.8. Une n-tresse simple a au plus $n(n-1)/2$ croisements puisque tout brin ne peut croiser qu'une fois au plus tout autre brin (voir la figure 2).

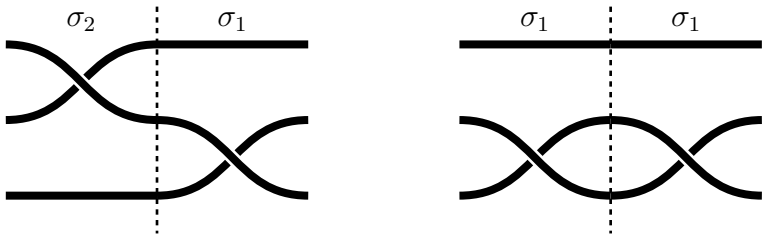


FIGURE 1 – Le diagramme de gauche représente une tresse simple : chacun des brins croise une fois au plus tout autre brin. Le diagramme de droite représente une tresse qui n'est pas simple : les brins 1 et 2 de la tresse se croisent deux fois.

Exemple 1.9. La tresse représentée par $\sigma_2\sigma_1$ est simple alors que la tresse représentée par σ_1^2 ne l'est pas (figure 1). L'exemple 1.6 présente une tresse qui n'est pas simple car les brins 1 et 3 se croisent plus d'une fois. La tresse Δ_4 est la plus grande tresse simple sur quatre brins : tous les brins se croisent une fois exactement (figure 2).

Remarque 1.10. Par la suite, on dira *mot (de tresse) simple* pour *mot représentant une tresse simple*.

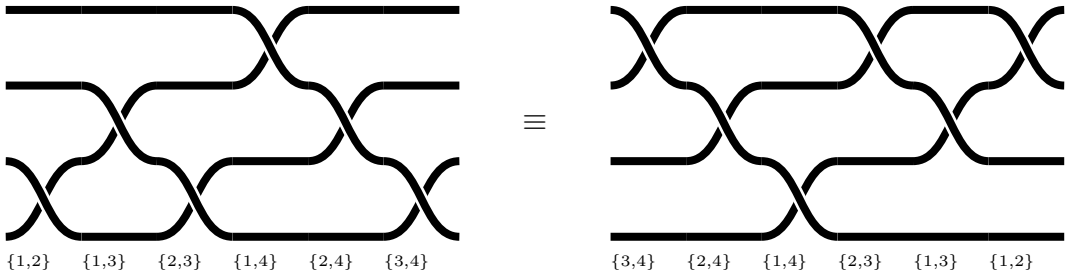


FIGURE 2 – Deux diagrammes de tresse représentant des expressions de l'élément de Garside Δ_4, la tresse simple la plus complexe sur quatre brins. Tous les brins se croisent exactement une fois. Le diagramme de gauche représente le mot u_4, donné par $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ et celui de droite, v_4, donné par $\sigma_3\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3$. Sous chaque croisement est indiqué son nom.

Notation. On note S_n l'ensemble des n-mots simples. On rappelle que la notation $|.|_{S_n}$ est définie à la section III.3.2.

1.3 MOTS DE PERMUTATION

Un mot de tresse décrit une tresse en explicitant chaque croisement en termes locaux : la lettre σ_i du mot de tresse $u\sigma_i v$ signifie qu'il faut croiser les brins sortant en position i

et $i+1$ du diagramme D_u avant d'effectuer les croisements décrits dans v. On donne dans cette section une réécriture d'un mot de tresse fournissant une description globale de la tresse en explicitant pour chaque croisement les noms des (deux) brins concernés.

Notation. On note $[\![1,n]\!]$ l'ensemble $\{1,\dots,n\}$ et $[\![1,n]\!]^{(k)}$ l'ensemble de toutes les parties de $[\![1,n]\!]$ dont le cardinal est k.

Définition 1.11 (nom de croisement)**.** Soit u un n-mot positif et soit t un entier de $[\![1,|u|]\!]$. Le *nom* du t^{e} croisement de D_u est le couple $(\{p,q\},\mu)$ de $[\![1,n]\!]^{(2)} \times [\![1,|u|_{S_n}]\!]$ si le t^{e} croisement de D_u concerne les brins p et q et que c'est la μ^{e} fois que ces deux brins se croisent.

Remarque 1.12. Dans le cas où u est un mot simple, on considère que le nom d'un croisement consiste uniquement en une paire $\{p,q\}$ (au lieu de $(\{p,q\},1)$).

Définition 1.13 (mot de permutation)**.** Pour tout n-mot positif u, le *n-mot de permutation* $\mathrm{P}(u)$ est la suite des noms des croisements du diagramme D_u.

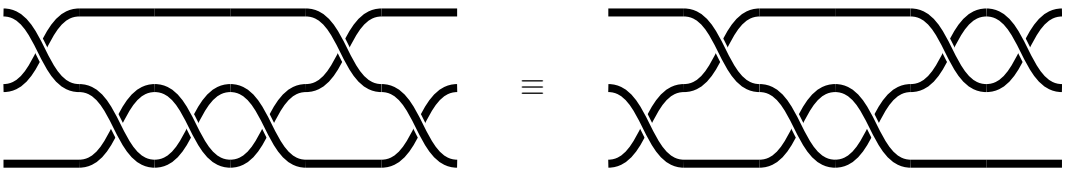


FIGURE 3 – Deux diagrammes de tresse représentant la même tresse. Sous chaque croisement est indiqué son nom. Ce dernier est formé de deux entiers correspondant aux brins qui se croisent, et d'un troisième entier indiquant le nombre de fois que ces deux brins se sont déjà croisés.

Exemple 1.14. Notons $\sigma_{j,i}$ le mot $\sigma_{j-1}\sigma_{j-2}\dots\sigma_{i+1}\sigma_i$ pour $j > i$ et le mot vide pour $j \leq i$. Soit u_n le mot $\sigma_{1,1}\sigma_{2,1}\dots\sigma_{n-1,1}$. Le mot u_n est simple et représente l'élément de Garside Δ_n (voir [15]). Par récurrence on calcule $\mathrm{P}(u_n)$ et on trouve

$$\mathrm{P}(u_n) = (\{1,2\},\{1,3\},\{2,3\},\dots,\{n-2,n-1\},\{1,n\},\dots,\{n-1,n\}).$$

Une autre écriture v_n de Δ_n, obtenue en lisant le diagramme de tresse de u_n en sens inverse, est $\sigma_{n-1,1}\sigma_{n-1,2}\dots\sigma_{n-1,n-2}$. On trouve alors

$$\mathrm{P}(v_n) = (\{n-1,n\},\dots,\{2,n\},\{1,n\},\{n-2,n-1\},\dots\{2,3\},\{1,3\},\{1,2\})$$

c'est-à-dire la suite $\mathrm{P}(u_n)$ écrite à l'envers.

Remarque 1.15. Par construction, les brins p et q de la tresse représentée par u se croisent dans le diagramme de tresse D_u si et seulement si le couple $(\{p,q\},1)$ apparaît dans $\mathrm{P}(u)$. Deux mots u et v équivalents représentent la même tresse donc leurs diagrammes comportent les mêmes croisements de brins, et donc les mots de permutation $\mathrm{P}(u)$ et $\mathrm{P}(v)$ contiennent les mêmes noms de croisements.

Plus précisément, on a le lemme suivant :

Lemme 1.16. *Soient u et v deux mots équivalents. Alors $\mathrm{P}(u)$ est une anagramme de $\mathrm{P}(v)$, c'est-à-dire qu'un nom de croisement apparaît dans $\mathrm{P}(u)$ si et seulement s'il apparaît dans $\mathrm{P}(v)$.*

1.4 DISTANCE COMBINATOIRE

En observant les changements qu'impliquent les relations sur les mots de permutation, on établit une minoration de la distance combinatoire entre des mots équivalents u et v en comparant les mots de permutation $\mathrm{P}(u)$ et $\mathrm{P}(v)$.

Notation. On note $[\![1,n]\!]^{(2,2)}$ l'ensemble des parties de $[\![1,n]\!]^{(2)}$ dont le cardinal est 2, c'est-à-dire l'ensemble des paires de paires distinctes.

Notation. Une relation de tresse est de *type I* si elle est de la forme $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ pour un certain i, et de *type II* si elle est de la forme $\sigma_i\sigma_j = \sigma_j\sigma_i$ pour des entiers i,j.

Définition 1.17. Soient u,v deux n-mots de tresse équivalents. On note $I_3(\mathrm{P}(u),\mathrm{P}(v))$ le nombre de triplets $\{(\{p,q\},\mu_1),(\{p,r\},\mu_2),(\{q,r\},\mu_3)\}$ tels que l'ordre de$(\{p,q\},\mu_1)$, $(\{p,r\},\mu_2)$, $(\{q,r\},\mu_3)$ n'est pas le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. On note $I_{2,2}(\mathrm{P}(u),\mathrm{P}(v))$ le nombre de paires $\{(\{p,q\},\mu_1),(\{p',q'\},\mu_2)\}$ telles que $(\{p,q\},\mu_1)$ et $(\{p',q'\},\mu_2)$ n'apparaissent pas le même ordre dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$.

Proposition 1.18. *Pour tous n-mots équivalents u,v, on a*

$$\mathrm{dist}(u,v) \geq I_3(\mathrm{P}(u),\mathrm{P}(v)) + I_{2,2}(\mathrm{P}(u),\mathrm{P}(v)).$$

Démonstration. On considère d'abord le cas $\mathrm{dist}(u,v)=1$, c'est-à-dire, le cas où on obtient v en appliquant une relation de tresse à u. Supposons en premier que v est obtenu à partir de u en appliquant une relation de type I, disons $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$. Alors il existe un unique triplet T_0, disons $\{(\{p,q\},\mu_1),(\{p,r\},\mu_2),(\{q,r\},\mu_3)\}$, tel que le mot de permutation $\mathrm{P}(v)$ est obtenu à partir de $\mathrm{P}(u)$ en remplaçant la sous-suite de noms $((\{p,q\},\mu_1),(\{p,r\},\mu_2),(\{q,r\},\mu_3))$ par $((\{q,r\},\mu_3),(\{p,r\},\mu_2),(\{p,q\},\mu_1))$ (voir figure 4). Donc l'ordre des trois noms de croisement n'est pas le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. D'un autre côté, tout autre triplet T de noms de $[\![1,n]\!]^{(2)}\times[\![1,|u|_{S_n}]\!]$ a au plus deux noms en commun avec T_0 et donc l'ordre des trois noms de T est le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. On a

donc $I_3(\mathrm{P}(u), \mathrm{P}(v)) = 1$ dans ce cas. De plus, toute paire de noms de $[\![1, n]\!]^{(2)} \times [\![1, |u|_{S_n}]\!]$ contient au plus un des trois noms $(\{p, q\}, \mu_1)$, $(\{p, r\}, \mu_2)$, $(\{q, r\}, \mu_3)$ et donc l'ordre de cette paire est le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. On en déduit l'égalité $I_{2,2}(\mathrm{P}(u), \mathrm{P}(v)) = 0$ dans ce cas.

Supposons maintenant qu'on applique une relation de type II, disons $\sigma_i\sigma_j = \sigma_j\sigma_i$, pour transformer u en v. Il existe alors une unique paire P_0, disons $\{(\{p, q\}, \mu_1), (\{p', q'\}, \mu_2)\}$, telle que le mot de permutation $\mathrm{P}(v)$ est obtenu à partir de $\mathrm{P}(u)$ en remplaçant la sous-suite $((\{p, q\}, \mu_1), (\{p', q'\}, \mu_2))$ par $((\{p', q'\}, \mu_2), (\{p, q\}, \mu_1))$ (figure 5). Donc l'ordre des deux noms considérés n'est pas le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. D'un autre côté, toute autre paire de noms P de $[\![1, n]\!]^{(2)} \times [\![1, |u|_{S_n}]\!]$ a au plus un nom en commun avec P_0, et donc les deux noms de P apparaissent dans le même ordre dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. On a dans ce cas l'égalité $I_{2,2}(\mathrm{P}(u), \mathrm{P}(v)) = 1$. De plus, tout triplet de noms de $[\![1, n]\!]^{(2)} \times [\![1, |u|_{S_n}]\!]$ ne peut engendrer qu'un des deux noms $(\{p, q\}, \mu_1)$ et $(\{p', q'\}, \mu_2)$. Donc l'ordre de ces trois noms est le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$, d'où l'égalité $I_3(\mathrm{P}(u), \mathrm{P}(v)) = 0$.

Dans chacun des deux cas, la quantité $I_3(\mathrm{P}(u), \mathrm{P}(v)) + I_{2,2}(\mathrm{P}(u), \mathrm{P}(v))$ varie de 1 lorsqu'un on applique une relation de tresse. Ceci implique le résultat. □

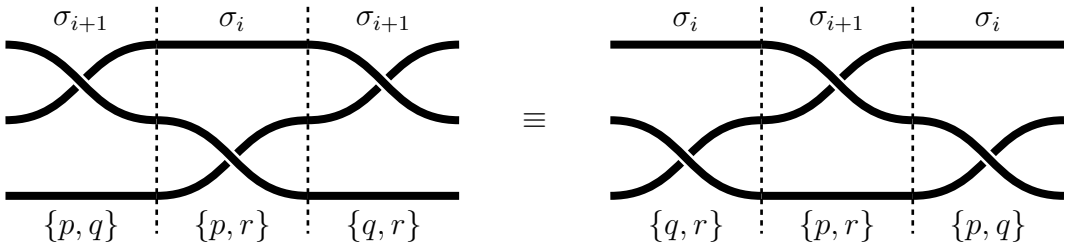


FIGURE 4 – Le passage du mot $\sigma_{i+1}\sigma_i\sigma_{i+1}$ au mot $\sigma_i\sigma_{i+1}\sigma_i$ a pour effet de transposer deux éléments du mot de permutation associé à $\sigma_{i+1}\sigma_i\sigma_{i+1}$: on remplace $(\{p, q\}, \{p, r\}, \{q, r\})$ par $(\{q, r\}, \{p, r\}, \{p, q\})$.

On déduit de la proposition 1.18 une minoration de la plus grande distance combinatoire entre n-mots simples.

Corollaire 1.19. *Pour tout n, il existe des n-mots simples vérifiant*

$$\mathrm{dist}(u, v) \geq \frac{1}{8}n^4 + O(n^3).$$

Remarque 1.20. Dans le cas des n-mots simples, au triplet d'entiers $\{p, q, r\}$ dans $[\![1, n]\!]^{(3)}$ correspond le triplet de noms $\{(\{p, q\}, 1), (\{p, r\}, 1), (\{q, r\}, 1)\}$. De manière similaire, à la paire de paires d'entiers $\{\{p, q\}, \{p', q'\}\}$ dans $[\![1, n]\!]^{(2,2)}$ correspond la paire de noms $\{(\{p, q\}, 1), (\{p', q'\}, 1)\}$. Cette correspondance justifie par la suite l'utilisation de ces deux écritures simplifiées.

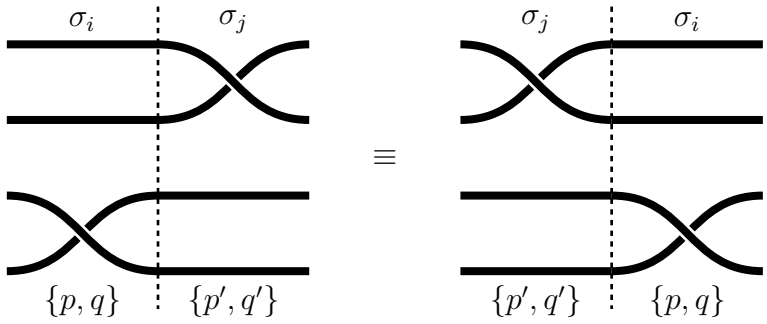


FIGURE 5 – Le passage du mot $\sigma_i\sigma_j$ au mot $\sigma_j\sigma_i\sigma_i$ a pour effet de transposer deux éléments du mot de permutation associé à $\sigma_i\sigma_j$: on remplace $\{p,q\}$, $\{p',q'\}$ par $\{p',q'\}$, $\{p,q\}$.

Démonstration. Considérons les mots u_n et v_n de l'exemple 1.14. On a remarqué plus haut que la suite $\mathrm{P}(u_n)$ est la suite $\mathrm{P}(v_n)$ écrite à l'envers. Ainsi tout triplet de $[\![1,n]\!]^{(3)}$ contribue 1 à I_3, donnant

$$I_3(\mathrm{P}(u_n),\mathrm{P}(v_n)) = \sharp([\![1,n]\!]^{(3)}) = \binom{n}{3}.$$

De manière identique, toute paire de paires $\{\{p,q\},\{p',q'\}\}$ dans $[\![1,n]\!]^{(2,2)}$ contribue 1 à $I_{2,2}$, donnant

$$I_{2,2}(\mathrm{P}(u_n),\mathrm{P}(v_n)) = \sharp([\![1,n]\!]^{(2,2)}) = \frac{1}{2}\binom{n}{2}\binom{n-2}{2} = 3\binom{n}{4}. \qquad \square$$

Remarque 1.21. Appelons *largeur* d'un mot de tresse u le nombre $\sigma_M - \sigma_m + 1$, avec σ_M (resp. σ_m) le générateur de plus haut (resp. bas) indice apparaissant dans u. Le corollaire montre que la distance combinatoire entre deux mots de tresse simples peut croître quartiquement en la largeur de u. Dans le chapitre V, on étudie l'incidence de la longueur.

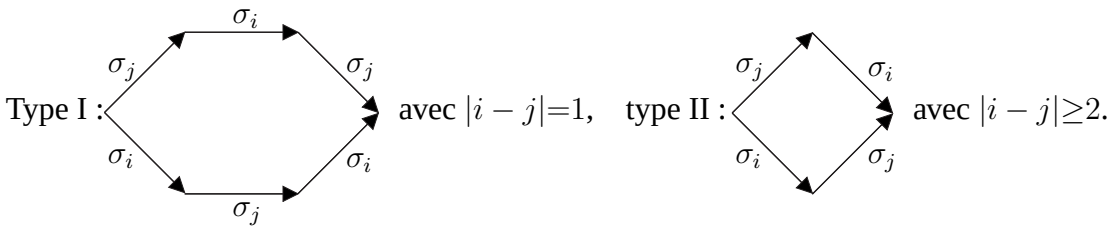
2 DIAGRAMMES DE VAN KAMPEN

Si deux mots u et v représentent la même tresse, il existe, par définition, une suite de relations à appliquer successivement pour passer de u à v. On introduit dans cette section une représentation graphique de cette suite de relations, appelée diagramme de van Kampen, et on établit un critère pour que le diagramme $\mathcal{K}$ entre les mots u et v soit optimal en le sens que la suite de relations représentée par $\mathcal{K}$ soit de longueur minimale, c'est-à-dire pour que le diagramme $\mathcal{K}$ donne la distance combinatoire entre u et v.

2.1 DIAGRAMMES DE VAN KAMPEN

On définit dans cette section la notion de diagramme de van Kampen dans le cas particulier des mots de tresse.

Définition 2.1 (diagramme de van Kampen)**.** Soient u, v des mots de tresse positifs. Un *diagramme de van Kampen* pour (u, v) est un diagramme $\mathcal{K}$ pavant une région connexe et simplement connexe du plan à l'aide des pavés des deux types suivants, de telle sorte que le bord de $\mathcal{K}$ consiste en deux chemins dont les étiquettes forment respectivement u et v (figure 6) :



Remarque 2.2. Ces deux chemins, en raison de l'orientation des arêtes des pavés, sont issus du sommet *source* — le seul du diagramme qui n'est le but d'aucune arête — et terminent par le sommet *puits* — le seul qui n'est la source d'aucune arête.

On a le résultat standard suivant.

Proposition 2.3 ([7])**.** *Soient u, v deux mots. Il existe un diagramme de van Kampen pour (u, v) si et seulement si on peut passer de u à v par des relations de tresse.*

2.2 OPTIMALITÉ D'UN DIAGRAMME DE VAN KAMPEN

Si u, v sont des mots de tresse positifs, alors il existe un diagramme de van Kampen pour (u, v) si et seulement si les mots u et v sont équivalents (proposition 2.3). Parce que chaque pavé correspond à une relation, compter le nombre de pavés du diagramme fournit une borne supérieure à la distance combinatoire entre u et v. On donne ici un critère pour qu'un diagramme de van Kampen réalise la distance combinatoire.

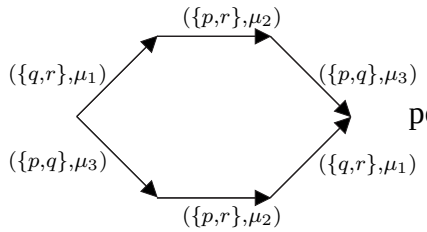
Définition-Proposition 2.4 (nom d'une arête)**.** *Soit $\mathcal{K}$ un diagramme de van Kampen pour les mots u et v. Soit a une arête de $\mathcal{K}$ et σ son étiquette. Alors il existe un chemin γ de la source de $\mathcal{K}$ jusqu'à son puits passant par a. Soit w_γ le mot que forment les étiquettes des arêtes par lesquelles passe γ. Le* nom *de l'arête a, indépendant du mot w_γ, est le nom du croisement qu'implique σ dans D_{w_γ}.*

Démonstration. Soient s_1 et s_2 respectivement les source et but de l'arête a. Par construction de $\mathcal{K}$, il existe un chemin de la source jusqu'à s_1 et un chemin de s_2 jusqu'au puits.

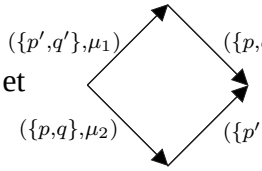
En reliant ces deux chemins par a, on obtient un chemin γ de la source de $\mathcal{K}$ vers son puits, et on note w_γ le mot formé par les étiquettes de γ dans le diagramme. Le mot w_γ est équivalent à u puisque le sous-diagramme de $\mathcal{K}$ bordé par γ et le chemin étiqueté u est un diagramme de van Kampen pour u et w_γ (proposition 2.3). On attribue ensuite à a son nom dans $\mathrm{P}(w_\gamma)$ (définition 1.13 et remarque 1.15).

Soient γ et δ deux chemins passant par l'arête a. Les deux mots w_γ et w_δ correspondants sont équivalents. Pour montrer que le nom de a ne dépend pas du chemin choisi, il suffit de considérer qu'on peut passer de w_γ à w_δ par application d'une seule relation de tresse. Si on applique la relation après a, cela signifie que les chemins γ et δ sont identiques jusqu'à a, et donc les noms des arêtes également. Si la relation a lieu avant a, on observe que les positions des brins après un motif $\sigma_i\sigma_{i+1}\sigma_i$ ou $\sigma_{i+1}\sigma_i\sigma_{i+1}$ sont les mêmes, et on tient un raisonnement identique pour une relation de type II (figures 4 et 5). □

Remarque 2.5. Il est clair qu'en nommant les arêtes ainsi, seulement deux types de pavés apparaissent dans un diagramme de van Kampen, à savoir



pour le type I, et



pour le type II.

Cette remarque permet de nommer de manière univoque les pavés d'un diagramme de van Kampen.

Définition 2.6 (nom d'un pavé)**.** Soient u, v des mots de tresse positifs et soit $\mathcal{K}$ un diagramme de van Kampen pour (u, v). Le *nom* d'un pavé du diagramme $\mathcal{K}$ est défini par l'ensemble des noms des arêtes qui le bordent, c'est-à-dire

– pour un pavé de type I, c'est un triplet $\{(\{p, q\}, \mu_1), (\{p, r\}, \mu_2), (\{q, r\}, \mu_3)\}$;

– pour un pavé de type II, c'est une paire $\{(\{p, q\}, \mu_1), (\{p', q'\}, \mu_2)\}$.

Remarque 2.7. Dans le cas des mots simples (voir remarque 1.20), les noms des pavés sont du type $\{p, q, r\}$ ou $\{\{p, q\}, \{p', q'\}\}$.

Définition 2.8 (diagramme de van Kampen optimal)**.** Soient u, v des mots de tresse positifs. Un diagramme de van Kampen $\mathcal{K}$ pour (u, v) est *optimal* si le nombre de pavés de $\mathcal{K}$ égale la distance combinatoire entre u et v.

Le critère d'optimalité d'un diagramme de van Kampen s'énonce alors comme suit.

Proposition 2.9. *Soient u et v deux mots de tresse équivalents et soit $\mathcal{K}$ un diagramme de van Kampen pour (u, v) dans lequel tous les noms de pavés sont différents. Alors $\mathcal{K}$ est optimal.*

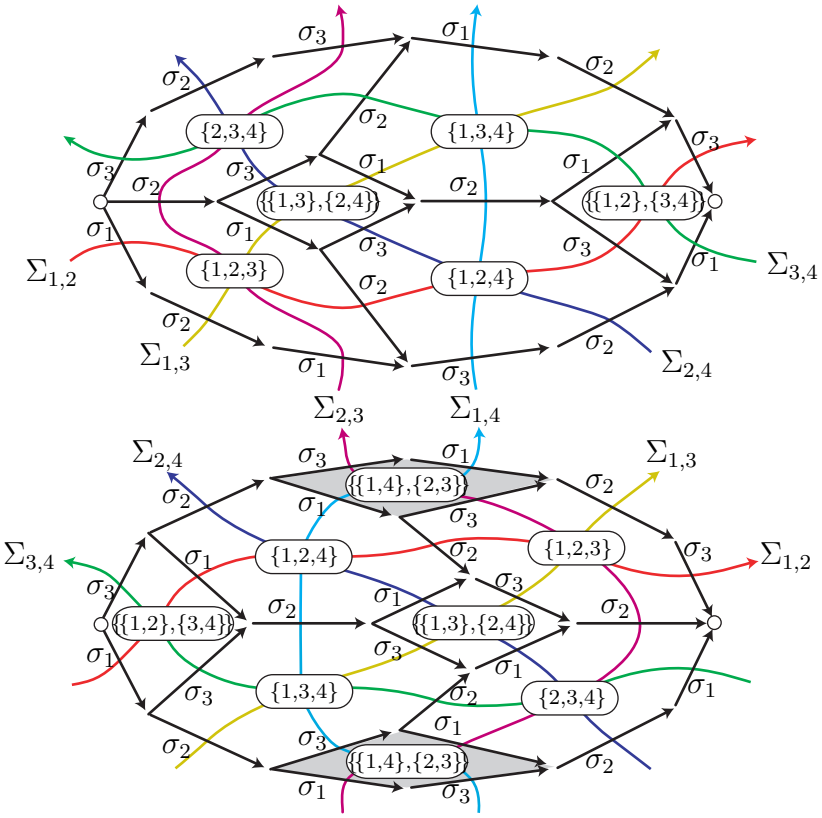


FIGURE 6 – Deux diagrammes de van Kampen pour les mots $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3$ et $\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$: le pavage par des pavés hexagonaux (de type I) et quadrilatéraux (de type II) montre que les deux mots représentent la même tresse. Chacun des pavés porte un nom dépendant des séparatrices (les courbes $\Sigma_{p,q}$) qui s'y croisent. Dans le diagramme du haut, tous les pavés portent un nom différent et le diagramme est optimal : le nombre de pavés réalise la distance combinatoire, qui est donc égale à 6. Dans le diagramme du bas, le pavé $\{\{1,4\},\{2,3\}\}$ apparaît deux fois et le diagramme n'est pas optimal.

Démonstration. La preuve de la proposition 1.18 montre que, si $\mathcal{K}$ contient exactement un pavé nommé $\{(\{p,q\},\mu_1),(\{p,r\},\mu_2),(\{q,r\},\mu_3)\}$, alors l'ordre d'apparition des noms $(\{p,q\},\mu_1)$, $(\{p,r\},\mu_2)$, $(\{q,r\},\mu_3)$ n'est pas le même dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. Donc, si $\mathcal{K}$ contient N pavés de type I — de noms différents deux à deux par hypothèse —, alors on a $I_3(\mathrm{P}(u),\mathrm{P}(v)) \geq N$. De même, si le diagramme $\mathcal{K}$ contient exactement un pavé nommé $\{(\{p,q\},\mu_1),(\{p',q'\},\mu_2)\}$, alors l'ordre des noms $(\{p,q\},\mu_1)$ et $(\{p',q'\},\mu_2)$ est différent dans $\mathrm{P}(u)$ et $\mathrm{P}(v)$. Donc, si $\mathcal{K}$ contient N' pavés de type II — de noms différents deux à deux par hypothèse —, alors on a $I_{2,2}(\mathrm{P}(u),\mathrm{P}(v)) \geq N'$. De la proposition 1.18 on déduit $\mathrm{dist}(u,v) \geq N + N'$ et du fait que $\mathcal{K}$ est un diagramme de van Kampen $\mathrm{dist}(u,v) \leq N + N'$. □

3 SÉPARATRICES

Dans cette section, on établit une particularité des diagrammes de van Kampen pour les mots de tresse, disons u et v : on peut relier les arêtes de même nom par une courbe reliant le bord étiqueté u au bord étiqueté v, en ne croisant jamais deux fois un même chemin reliant la source au puits. On établit alors un critère d'optimalité pour les diagrammes de van Kampen en termes de séparatrices.

Définition 3.1 (fragment de séparatrice)**.** (Figure 7) Soit $\mathcal{K}$ un diagramme de van Kampen. Un *fragment de* $(\{p,q\},\mu)$*-séparatrice* d'un pavé de $\mathcal{K}$ est une courbe (intérieure au pavé) reliant les milieux des arêtes nommées $(\{p,q\},\mu)$, si elles existent.

Remarque 3.2. Cette définition posant des problèmes d'unicité, dans la suite, on ne considère les fragments qu'à isotopie près.

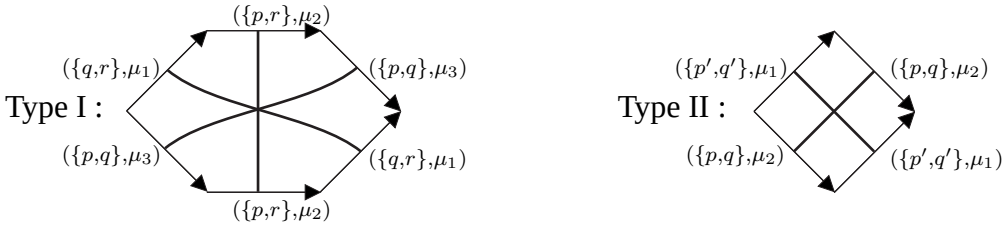


FIGURE 7 – Fragments de séparatrices pour les pavés de type I et II dans un diagramme de van Kampen : un fragment de séparatrice relie deux arêtes de même nom à l'intérieur d'un pavé.

Définition 3.3 (séparatrice)**.** (Figure 6) Soient u, v deux mots de tresse positifs et soit $\mathcal{K}$ un diagramme de van Kampen pour (u,v). La $(\{p,q\},\mu)$-séparatrice est la courbe formée de tous les fragments de $(\{p,q\},\mu)$-séparatrice.

Notation. On note $\Sigma^{\mu}_{p,q}$ la $(\{p,q\},\mu)$-séparatrice et, si les mots considérés sont simples, pour chaque paire $\{p,q\}$, il n'y a qu'une seule séparatrice, qu'on note $\Sigma_{p,q}$.

On reformule le critère d'optimalité de la proposition 2.9 en termes de séparatrices.

Proposition 3.4. *Soient u, v deux n-mots de tresse positifs et équivalents et soit $\mathcal{K}$ un diagramme de van Kampen pour (u,v) tel que deux séparatrices distinctes se croisent au plus une fois. Alors $\mathcal{K}$ est optimal.*

Démonstration. Par construction, pour tout triplet $\{p,q,r\}$ et toute paire $\{\mu_1,\mu_2\}$, les seuls endroits où $\Sigma^{\mu_1}_{p,q}$ et $\Sigma^{\mu_2}_{p,r}$ peuvent se croiser est à l'intérieur de pavés de type I nommés $\{(\{p,q\},\mu_1), (\{p,r\},\mu_2), (\{q,r\},\mu_3)\}$ avec μ_3 un entier, et réciproquement, les trois séparatrices d'un pavé de type I se croisent deux à deux (figure 7). De même, pour toute

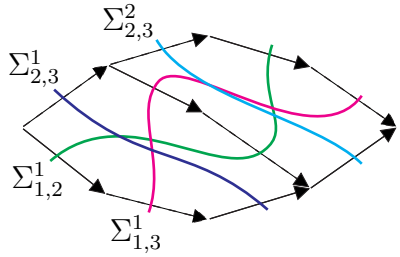


FIGURE 8 – Diagramme de van Kampen pour $(\sigma_2\sigma_2\sigma_1\sigma_1, \sigma_1\sigma_2\sigma_1\sigma_1)$. Les arêtes pleines (resp. tiretées) représentent σ_1 (resp. σ_2). Les séparatrices relient les arêtes de même nom ; contrairement au cas d'une tresse simple (figure 6), deux brins peuvent se croiser plusieurs fois : ici les brins 2 et 3 se croisent deux fois, ce dont témoignent les séparatrices $\Sigma^1_{2,3}$ et $\Sigma^2_{2,3}$.

paire de paires $\{\{p,q\},\{p',q'\}\}$, le seul endroit où peuvent se croiser $\Sigma^{\mu_1}_{p,q}$ et $\Sigma^{\mu_2}_{p',q'}$ est à l'intérieur d'un pavé de type II nommé $\{(\{p,q\},\mu_1),(\{p',q'\},\mu_2)\}$, et, réciproquement, les deux séparatrices d'un tel pavé se croisent.

Ainsi, le nombre de fois que deux séparatrices $\Sigma^{\mu_1}_{p,q}$ et $\Sigma^{\mu_2}_{p',q'}$ se croisent est exactement le nombre de pavés de type I nommés $\{(\{p,q\},\mu_1),(\{p,r\},\mu_2),(\{q,r\},\mu_3)\}$ avec $\mu_3 \leq |u|_{S_n}$, si l'ensemble $\{p,q,p',q'\}$ a trois éléments, et le nombre de pavés de type II nommés $\{(\{p,q\},\mu_1),(\{p',q'\},\mu_2)\}$ sinon. On en déduit que tous les pavés de $\mathcal{K}$ portent un nom différent. Il ne reste plus qu'à appliquer la proposition 2.9. □

4 DIAGRAMMES DE RETOURNEMENT

4.1 LIEN AVEC LES DIAGRAMMES DE VAN KAMPEN

On a décrit au chapitre I les diagrammes de retournement : partant de deux mots de tresse positifs u, v, on retourne $u^{-1}v$ en $v'u'^{-1}$ avec u', v' deux mots de tresse positifs. Alors le diagramme de retournement de $u^{-1}v$ est un diagramme de van Kampen (particulier) pour les mots uv' et vu' : en plus des pavés de type I (à six arêtes) et des pavés de type II (à quatre arêtes), il peut y avoir des pavés de type III (à deux arêtes + une ε-arête) correspondant aux retournements de sous-mots $\sigma_i^{-1}\sigma_i$ en ε.

Si un diagramme de retournement contient une ε-arête, alors on obtient un diagramme de van Kampen en identifiant, pour chaque pavé de type III, les arêtes liées par l'ε-arête. On a alors, par construction :

Fait 4.1. *Si u, v, u', v' sont des mots de tresse positifs vérifiant $u^{-1}v \curvearrowright v'u'^{-1}$, alors le diagramme de retournement de $u^{-1}v$ fournit un diagramme de van Kampen pour (uv', vu').*

Démonstration. Si le diagramme de retournement de $u^{-1}v$ contient des pavés de type III, on les supprime en identifiant les arêtes liées par les ε-arêtes. Ensuite, il suffit de voir, par la

proposition I.1.5, que les mots uv' et vu' sont équivalents et que chaque pavé du diagramme de retournement de $u^{-1}v$ est soit un pavé de type I, soit un pavé de type II. □

Définition 4.2 (hexagone, carré, digone)**.** Soit $\mathcal{D}$ un diagramme de retournement. Un pavé de type I de $\mathcal{D}$ est appelé *hexagone*. Un pavé de type II de $\mathcal{D}$ est un *carré* et un pavé de type III de $\mathcal{D}$ est un *digone*.

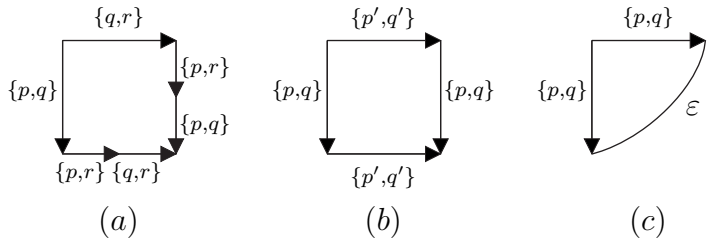


FIGURE 9 – Le pavé (a) est un hexagone et correspond à un pavé de type I. Le pavé (b) est un carré et correspond à un pavé de type II. Le pavé (c) est un digone et correspond à un pavé de type III.

La notion de séparatrice est la même pour les diagrammes de retournement que celle définie à la section 3 pour les diagrammes de van Kampen, et pour les digones, cela revient à tracer une courbe entrant horizontalement dans le digone et ressortant verticalement (figure 10).

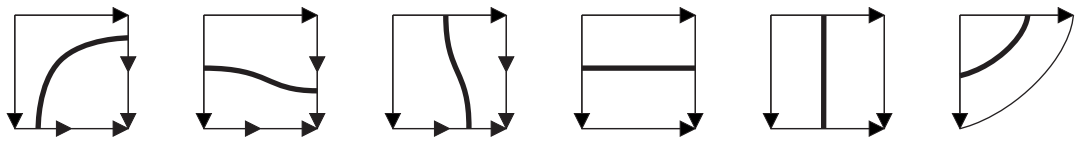


FIGURE 10 – Les courbes en trait gras sont les fragments des différentes séparatrices. Une séparatrice relie deux arêtes si elles portent le même nom (figure 9). Un hexagone est traversé par trois séparatrices, un carré par deux et un digone par une.

4.2 DIAGRAMMES DE RETOURNEMENT OPTIMAUX

Les diagrammes de retournement sont essentiellement des diagrammes de van Kampen, et on peut s'y ramener en supprimant les digones — voir la section précédente. Ainsi, pour u, v des mots de tresse positifs, le diagramme de retournement $\mathcal{D}$ de $u^{-1}v$ donne une méthode pour passer du mot uv' au mot équivalent vu' avec u', v' les mots uniques mots de tresse positifs vérifiant $u^{-1}v \curvearrowright v'u'^{-1}$; partant de uv', le nombre de relations à appliquer pour obtenir vu' est le nombre de pavés dans le diagramme de van Kampen correspondant

— qui vaut la somme des nombres de carrés et d'hexagones de $\mathcal{D}$ — , qui est donc, par définition, minoré par la distance combinatoire $\mathrm{dist}(uv', vu')$.

Dans cette section, on donne une condition sur le diagramme de retournement de $u^{-1}v$ pour que le diagramme de van Kampen pour (uv', vu') soit optimal, c'est-à-dire qu'il réalise la distance combinatoire entre uv' et vu'.

Notation. Soient u, v des mots de tresse positifs et soit $\mathcal{D}$ le diagramme de retournement de $u^{-1}v$. On note $\mathrm{dist}_{\curvearrowright}(u, v)$ la somme des nombres d'hexagones et de carrés de $\mathcal{D}$.

Définition 4.3 (diagramme de retournement optimal)**.** Soient u, v, u', v' des mots de tresse positifs vérifiant $u^{-1}v \curvearrowright v'u'^{-1}$. On dit que le diagramme de retournement $\mathcal{D}$ de $u^{-1}v$ est *optimal* si le diagramme de van Kampen obtenu à partir de $\mathcal{D}$ est optimal, c'est-à-dire si on a $\mathrm{dist}_{\curvearrowright}(u, v) = \mathrm{dist}(uv', vu')$.

Remarque 4.4. D'après ce qui précède, on a $\mathrm{dist}(uv', vu') \leq \mathrm{dist}_{\curvearrowright}(u, v)$ puisque tout diagramme de retournement donne un diagramme de van Kampen.

Nous montrons maintenant le critère d'optimalité annoncé.

Proposition 4.5. *Soient u, v des mots de tresse positifs. Supposons que le diagramme de retournement $\mathcal{D}$ de $u^{-1}v$ ne contienne pas de digone. Alors $\mathcal{D}$ est optimal.*

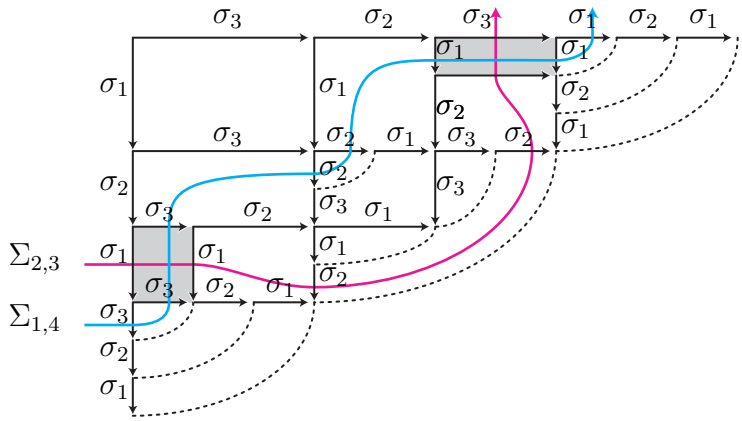


FIGURE 11 – Diagramme de retournement pour $\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1$. En identifiant les sommets aux extrémités des ε-arêtes, on retrouve le diagramme de van Kampen du bas de la figure 6. La non-optimalité du diagramme est claire : les séparatrices $\Sigma_{1,4}$ et $\Sigma_{2,3}$ se croisent deux fois (carrés grisés).

Démonstration. Notons $\mathcal{D}$ le diagramme de retournement de $u^{-1}v$. D'après l'orientation qu'on a donnée aux séparatrices, toute arête verticale de $\mathcal{D}$ est traversée par une séparatrice

de la gauche vers la droite et toute arête verticale est traversée par une séparatrice du bas vers le haut. De plus, on remarque que seuls les digones font passer l'orientation d'une séparatrice de horizontale à verticale, et que seuls les hexagones peuvent changer l'orientation d'une séparatrice de verticale à horizontale. On observe aussi que si deux séparatrices se croisent dans un polygone, alors en entrant dans le polygone, elles sont toutes les deux verticales ou l'une est verticale et l'autre horizontale.

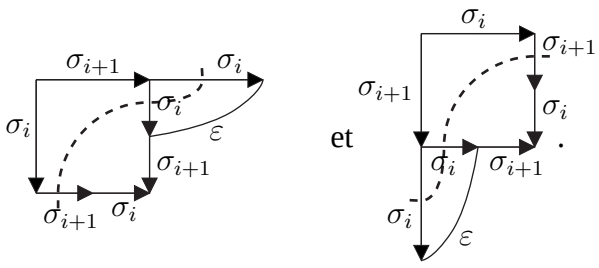
Supposons maintenant que deux séparatrices Σ, Σ' se croisent au moins deux fois dans $\mathcal{D}$. On distingue deux cas, selon que les noms des séparatrices impliquent trois ou quatre noms de brins. D'abord, supposons qu'il existe des entiers p, q, r (et μ, μ') satisfaisant $\Sigma = \Sigma^{\mu}_{p,q}$ et $\Sigma' = \Sigma^{\mu'}_{p,r}$. Alors Σ et Σ' se croisent nécessairement dans un hexagone nommé $\{(\{p,q\},\mu),(\{p,r\},\mu'),(\{q,r\},\mu'')\}$ pour un certain entier μ''. Soit H_1 (resp. H_2) le premier (resp. deuxième) hexagone dans lequel Σ et Σ' se croisent. Soit Σ et Σ' sortent de H_1 horizontalement soit l'une des deux sort verticalement. Dans le premier cas, comme il n'y a qu'une des deux séparatrices qui peut rentrer horizontalement dans H_2 c'est que l'autre change d'orientation entre H_1 et H_2, ce qui témoigne de la présence d'un digone. Dans le second cas, quitte à permuter les rôles des séparatrices, on suppose que Σ (resp. Σ') est horizontale (resp. verticale) en sortant de H_1. Alors Σ reste en dessous de Σ' (plus loin de v) jusqu'à entrer dans H_2. Ainsi, la seule possibilité est que Σ' soit horizontale à l'entrée (par la gauche) de H_2 et que Σ soit verticale à l'entrée (par le bas) de H_2. Ceci n'est possible que si l'orientation de Σ est modifiée de horizontale à verticale, c'est-à-dire si Σ traverse un digone entre H_1 et H_2.

Supposons maintenant qu'il existe des entiers p, q, p', q' (et μ, μ') satisfaisant $\Sigma = \Sigma^{\mu}_{p,q}$ et $\Sigma' = \Sigma^{\mu'}_{p',q'}$. Alors les séparatrices Σ et Σ' se croisent nécessairement dans des carrés nommés $\{(\{p,q\},\mu),(\{p',q'\},\mu')\}$. Soit C_1 (resp. C_2) le premier (resp. le deuxième) carré dans lequel C_1 et C_2 se croisent. Quitte à permuter les rôles de Σ et Σ', on peut supposer qu'à la sortie de C_1 Σ est horizontale et Σ' est verticale. Alors, comme pour le cas des hexagones, Σ reste en dessous de Σ' jusqu'au carré C_2. Ceci implique que Σ' est horizontal en entrant dans C_2 et que Σ est verticale, ceci signifiant que Σ a traversé un digone entre C_1 et C_2.

On a montré que deux séparatrices se croisent au moins deux fois dans $\mathcal{D}$ seulement si $\mathcal{D}$ contient un digone. On en déduit que deux séparatrices se croisent au plus une fois dans $\mathcal{D}$ et on applique la proposition 3.4. □

Remarque 4.6. La proposition 4.5 s'appuie sur le fait que deux séparatrices ne peuvent se croiser deux fois s'il n'y a pas de digones : pour se croiser à nouveau, chacune des séparatrices doit changer d'orientation, ce qui nécessite un digone (et un hexagone). Mais, lorsqu'un digone est convenablement accolé à un hexagone, une séparatrice passant par l'hexagone et le digone ne change pas d'orientation — dans le cas hexagone-puis-digone, la séparatrice est verticale avant l'hexagone et après le digone et dans le cas digone-puis-hexagone, la séparatrice est horizontale avant le digone et après l'hexagone —, ce qu'on

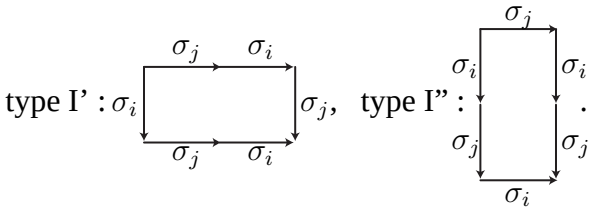
voit sur



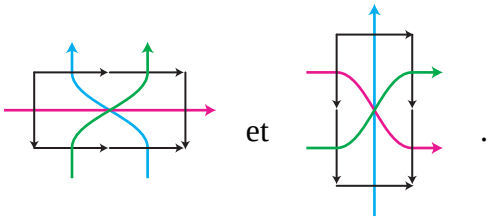
Dans une suite de retournement, ces situations correspondent à la présence d'un sous-mot de la forme $\sigma_i^{-1}\sigma_{i+1}\sigma_i$, pour lequel on a $[\sigma_i^{-1}\sigma_{i+1}]\sigma_i \curvearrowright \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}[\sigma_i^{-1}\sigma_i] \curvearrowright \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}$, ou de la forme $\sigma_i^{-1}\sigma_{i+1}^{-1}\sigma_i$, se retournant en $[\sigma_i^{-1}\sigma_i]\sigma_{i+1}\sigma_i^{-1}\sigma_{i+1}^{-1} \curvearrowright \sigma_{i+1}\sigma_i^{-1}\sigma_{i+1}^{-1}$.

Ces deux dernières suites de retournement motivent l'introduction de deux nouveaux types d'hexagones.

Définition 4.7. Pour $|i-j|=1$, les hexagones de types I' et I" sont :



Remarque 4.8. Une séparatrice traversant un hexagone de type I' ou I" ne change pas d'orientation : on a



Définition 4.9 (diagramme compact)**.** Soient i,j deux entiers vérifiant $|i-j|=1$. Un diagramme de retournement est dit *compact* si tout sous-mot $\sigma_i^{-1}\sigma_j\sigma_i$ (resp. $\sigma_i^{-1}\sigma_j^{-1}\sigma_i$) borde un hexagone de type I' (resp. type I").

Remarque 4.10. Il existe un unique diagramme de retournement partant d'un mot w et dont les pavés sont de types I, II et III. Ce n'est pas le cas lorsqu'on utilise également les hexagones de types I' et I" car un digone peut être accolé à deux hexagones en même temps (figure 12).

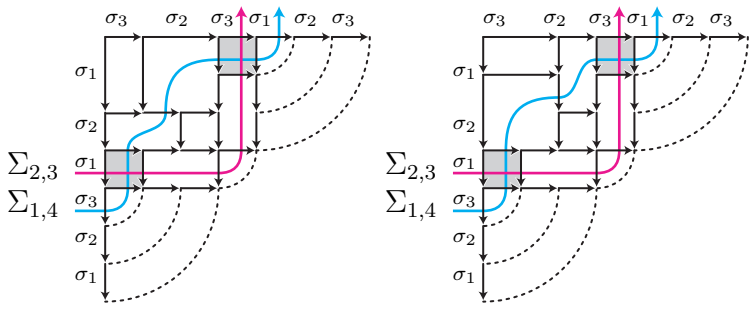


FIGURE 12 – Deux diagrammes de retournement compacts correspondant au diagramme de retournement non compact de la figure 11.

Le même argument que pour la proposition 4.5 donne :

Proposition 4.11. *Soient u, v des mots de tresse positifs. Supposons que $\mathcal{D}$ soit un diagramme de retournement de $u^{-1}v$ compact et sans digone. Alors $\mathcal{D}$ est optimal.*

Démonstration. Les hexagones de types I' et I" ne changent pas l'orientation des séparatrices (remarque 4.8), et donc leur présence dans un diagramme de retournement n'altère pas l'argument utilisé dans la preuve de la proposition 4.5. □

On verra à la section V.2.1 une application de la proposition 4.11, où un exemple y sera développé.

CHAPITRE V

COMPLEXITÉS DU RETOURNEMENT

Dans ce chapitre, on établit des bornes concernant deux quantités attachées au retournement des mots de tresse : d'un mot $u^{-1}v$ de longueur ℓ, avec u, v des mots de tresse positifs, est issue une suite de retournement ; on appelle 1-*complexité* la longueur du mot terminal et 2-*complexité* la longueur de la suite de retournement. Le but de ce chapitre est d'encadrer ces deux complexités en fonction de ℓ.

Nous distinguons deux cas : dans un premier temps, nous traiterons le cas des mots de tresse écrits sur un nombre fini de générateurs et le cadre de l'étude sera donc BW_n ; dans un deuxième temps, nous traiterons le cas des mots écrits sur une infinité de générateurs et le cadre de l'étude sera BW_∞. Dans le cas où la largeur est fixée, c'est-à-dire que le nombre de générateurs est fini, les résultats sont connus [12] et on remontre que la 1-complexité (resp. 2-complexité) est linéaire (resp. quadratique).

Lorsque l'indice des mots de tresses n'est pas fixé, pratiquement aucun résultat n'est connu concernant les 1- et 2-complexités du retournement. On commence par améliorer une borne cubique de [12] :

> **Proposition :** *Pour tout ℓ suffisamment grand, il existe un mot de longueur ℓ dont la 2-complexité est supérieure à $(4\ell^4)/3$.*

On ramène l'étude des complexités dans le cas arbitrairement large au cas de largeur finie en observant que les complexités n'augmentent pas indéfiniment avec la largeur des mots : les mots larges et courts n'ont pas une complexité supérieure à celle de mots moins larges et de même longueur. On montre :

> **Proposition :** *Les mots de longueur ℓ et de 1-complexité (resp. 2-complexité) maximale sont de largeur inférieure à 2ℓ.*

Ce résultat suffit pour montrer que la 1-complexité est au plus cubique. Le reste du chapitre est dévolu à obtenir une majoration de la 2-complexité.

Le défaut de connaissance du nombre d'ε-retournements rend la majoration de la 2-complexité délicate. On introduit un cas particulier de retournement, le retournement paci-

fique, qui ne comporte pas d'étape de suppression de lettres. Chaque opération du retournement pacifique laisse une trace lisible dans le mot retourné. On montre que tout mot w' issu par retournement pacifique de w, un n-mot de longueur ℓ, est de longueur inférieure à $C_n\ell$, où C_n ne dépend que de n. On écrit alors tous les mots de la suite de retournement pacifique issue de w dans une grille $C_n\ell \times C_n\ell$ et on montre que si w se retourne pacifiquement en w', alors on a $\mathrm{UL}(w') > \mathrm{UL}(w)$, où UL est une fonction à valeurs entières majorée par l'aire de la grille. On en déduit une borne supérieure pour la 2-complexité, améliorant un résultat de [14] de plusieurs ordres de grandeur :

Proposition : *Les mots de longueur ℓ ont une 2-complexité inférieure à $3^{4\ell}\ell^2$.*

On ne sait pas évaluer correctement le nombre de digones d'un diagramme de retournement. En conséquence, on a une mauvaise connaissance des éventuelles répétitions d'hexagones, c'est-à-dire d'hexagones portant le même nom. En raisonnant avec les séparatrices du diagramme, on montre que si deux hexagones portent le même nom, alors ils font partie d'un sous-diagramme particulier, qu'on appelle *motif répétiteur*, et qu'on décrit. En particulier, on montre qu'il n'y a qu'un nombre fini de sous-diagrammes possibles :

Proposition : *Si un diagramme de retournement $\mathcal{D}$ contient deux hexagones de même nom, alors $\mathcal{D}$ contient un motif répétiteur d'une des trois familles* A, B *ou* $\overline{\mathrm{B}}$.

Finalement, l'expérience nous menant à conjecturer qu'un diagramme de retournement ne peut pas contenir beaucoup de motifs répétiteurs (conjecture 6.12), on énonce :

Proposition : *Supposons que la conjecture 6.12 est vérifiée. Alors la 2-complexité d'un mot $u^{-1}v$ de longueur ℓ, avec u, v simples, est quartique en ℓ.*

Le chapitre est organisé comme suit. Dans la section 1, on donne des équivalents asymptotiques pour les 1- et 2-complexités dans le cas particulier où la largeur des mots est fixée. À partir de la section 2, les mots ne sont plus de largeur fixée. Dans la section 2, on montre qu'il existe des mots de 2-complexité quartique en leur longueur. Dans la section 3, on montre qu'à longueur donnée, les mots larges ne sont pas plus complexes. Dans la section 4, on décrit le retournement pacifique et on borne supérieurement la 2-complexité du retournement. Dans la section 5, on utilise les séparatrices pour améliorer la borne de la partie 4 et pour décrire les répétitions d'hexagones. À la section 6, on définit les motifs répétiteurs et on établit des bornes supérieures pour la 2-complexité.

1 MOTS DE LARGEUR FIXÉE

La complexité du retournement d'un mot dépend de sa largeur (le nombre de brins tressés) et de sa longueur (le nombre de croisements de brins). Mais, à largeur fixée, la décomposition d'un mot de tresse w en produits de mots simples — qui sont en nombre fini — permet de majorer les 1- et 2-complexités de w en fonction de sa longueur ℓ uniquement.

1.1 NOTIONS PRÉLIMINAIRES

Comme la présentation standard d'Artin-Tits ($\mathcal{A}_n$) est complémentée, de tout n-mot de tresse w est issu une unique suite de retournement. De plus, comme le retournement des mots de tresses est fortement convergent, toute suite de retournement maximale se termine par un mot uv^{-1} avec u, v positifs. On a alors la définition suivante :

Définition 1.1 (1-complexité)**.** Soit w un mot de tresse. On appelle 1-*complexité* de w, et on note $\mathrm{L}_1(w)$, la longueur du mot uv^{-1} vérifiant $w \curvearrowright uv^{-1}$ avec u, v positifs. On pose $\mathrm{L}_1(\ell, n) = \sup\{\mathrm{L}_1(w); w\ n\text{-mot de longueur } \ell\}$.

On définit une deuxième notion de complexité.

Définition 1.2 (2-complexité)**.** Soit w un mot de tresse. On appelle 2-*complexité* de w, et on note $\mathrm{L}_2(w)$, la longueur de la suite de retournement maximale issue de w, c'est-à-dire de la suite de retournement terminant par un mot uv^{-1} avec u, v positifs. On pose $\mathrm{L}_2(\ell, n) = \sup\{\mathrm{L}_2(w); w\ n\text{-mot de longueur } \ell\}$.

Remarque 1.3. Pour u, v deux mots positifs, et en notant $d(u^{-1}v)$ le nombre de digones dans le diagramme de retournement de $u^{-1}v$, on a $\mathrm{dist}_{\curvearrowright}(u, v) + d(u^{-1}v) = \mathrm{L}_2(u^{-1}v)$ (voir la section IV.4.2).

Proposition 1.4 ([13])**.** *L'ensemble des n-mots simples S_n est clos par $\backslash$. Autrement dit, si u, v sont des n-mots simples, alors les deux n-mots u', v' vérifiant $u^{-1}v \curvearrowright v'u'^{-1}$ sont simples.*

Proposition 1.5 ([13])**.** *L'ensemble des n-mots simples S_n est fini.*

1.2 BORNES INFÉRIEURES ET SUPÉRIEURES

Lemme 1.6. *Soient u, v des mots positifs. Posons $i(n) = \max\{\mathrm{L}_2(x^{-1}y); x, y \in S_n\}$ et $e(n) = n(n-1)/2$. Alors on a*

$$\mathrm{L}_2(u^{-1}v) \leq i(n)|u|_{S_n}|v|_{S_n} \quad \textit{et} \quad \mathrm{L}_1(u^{-1}v) \leq e(n)(|u|_{S_n} + |v|_{S_n}).$$

Démonstration. D'après la proposition 1.4, le retournement de $u^{-1}v$ nécessite au plus $|u|_{S_n}|v|_{S_n}|$ retournements du type $x^{-1}y \curvearrowright y'x'^{-1}$ avec x, y, x', y' des mots simples. Or l'ensemble des n-simples est fini (prop. 1.5), donc la quantité $i(n)$ est finie et, par définition, chacun des mots $x^{-1}y$ est de 2-complexité inférieure à $i(n)$, d'où la majoration de $\mathrm{L}_2(u^{-1}v)$. D'après le lemme III.3.4, pour tout mot w vérifiant $u^{-1}v \curvearrowright w$, on a $|u^{-1}v|_{S_n} \geq |w|_{S_n}$. De plus, la longueur maximale d'un n-mot simple est $n(n-1)/2$ (chacun des n brins croise exactement une fois les $n-1$ autres brins). On en déduit la majoration annoncée. □

Remarque 1.7. Aucune majoration fine de $i(n)$, le nombre maximal de retournements élémentaires requis pour retourner $u^{-1}v$ avec u, v deux n-mots simples, n'est connue à ce jour. Toutefois, d'après le corollaire IV.1.19 sur la minoration de la distance combinatoire, $i(n)$ croît au moins quartiquement avec n, ce qu'on montre à la proposition 2.1 dans le cas spécifique du retournement.

Exemple 1.8. Soient les familles de mots de tresses $(u_p)_{p\geq 1}$ et $(v_p)_{p\geq 1}$. Pour $p \geq 1$, on pose $u_p = \sigma_1^p$ et $v_p = \sigma_3^p$. Pour $i \geq 1$, le mot σ_i^2 n'est pas simple donc, pour $p \geq 1$, on en déduit $|u_p|_{S_4} = |v_p|_{S_4} = p$. Du retournement $\sigma_1^{-1}\sigma_3 \curvearrowright_r \sigma_3\sigma_1^{-1}$ on déduit, pour $p \geq 1$, que le retournement complet $u_p^{-1}v_p \curvearrowright_r v_p u_p^{-1}$ nécessite p^2 étapes, soit $|u_p|_{S_4}.|v_p|_{S_4}$, et le mot terminal est de longueur $2p$, soit $|u_p|_{S_4} + |v_p|_{S_4}$.

Le lemme dit que si les mots u et v sont de longueur ℓ, alors le nombre maximal d'étapes que requiert le retournement du mot $u^{-1}v$ est dans $O(\ell^2)$ et la longueur du mot terminal est dans $O(\ell)$. Il reste à étendre ce résultat pour les mots qui ne sont pas négatifs-positifs.

Proposition 1.9. *Soit w un n-mot de tresse. On a les majorations*

$$\mathrm{L}_2(w) \leq I|w|_{S_n}^2 \quad \textit{et} \quad \mathrm{L}_1(w) \leq E|w|_{S_n},$$

où I et E ne dépendent pas de w.

Démonstration. Posons $w = w_1^{e_1} \dots w_p^{e_p}$ la décomposition de w de la section III.3.2. Pour tout i, on a $e_i e_{i+1} = -1$. On montre la majoration de $\mathrm{L}_2(w)$ par récurrence sur p. Le cas $p = 2$ correspond au lemme 1.6, où on a posé $I = i(n)$. Supposons $p > 2$. Le cas $e_p = -1$ est clair : on a $\mathrm{L}_2(w) = \mathrm{L}_2(w_1^{e_1} \dots w_{p-1}^{e_{p-1}}) \leq I|w_1^{e_1} \dots w_{p-1}^{e_{p-1}}|_{S_n}^2 \leq I|w|_{S_n}^2$. On suppose maintenant $e_p = 1$. Posons $w_1' = w_1^{e_1} \dots w_{p-2}^{e_{p-2}}$ et $w_2' = w_{p-1}^{-1}w_p$. On a alors $\mathrm{L}_2(w) \leq |w_1'|_{S_n}^2 + |w_2'|_{S_n}^2 + |w_1'|_{S_n}|w_2'|_{S_n} \leq (|w_1'|_{S_n} + |w_2'|_{S_n})^2 \leq |w|_{S_n}^2$.

La majoration de $\mathrm{L}_1(w)$ est celle du lemme 1.6, où on a posé $E = e(n)$. □

De la proposition 1.9 et du fait que, pour tout n-mot w, on a l'inégalité $|w|_{S_n} \leq |w|$, on déduit immédiatement le corollaire suivant.

Corollaire 1.10. *On a $\mathrm{L}_2(\ell, n) \in O(\ell^2)$ et $\mathrm{L}_1(\ell, n) \in O(\ell)$.*

Finalement, en combinant, les majorations obtenues au corollaire 1.10 aux minorations de l'exemple 1.8, on obtient les équivalences asymptotiques suivantes.

Proposition 1.11. *Pour $n \geq 3$, on a*

$$\mathrm{L}_1(\ell, n) \in \Theta(\ell) \quad \textit{et} \quad \mathrm{L}_2(\ell, n) \in \Theta(\ell^2).$$

2 BORNES INFÉRIEURES

Dans cette section et les suivantes, on ne restreint plus le nombre de brins et on cherche à évaluer les 1- et 2-complexités de mots de tresse arbitrairement larges. Ainsi, les mots de tresse dont on calcule les complexité représentent des éléments du monoïde B_∞^+ présenté par

$$(\mathcal{A}_\infty) \qquad \left(\sigma_1, \sigma_2, \dots \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{pour } |j-i| = 1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \text{pour } |j-i| \geq 2 \end{array} \right).$$

À la différence du cas où la largeur est fixée, les simples ne sont plus en nombre fini et les majorations de la proposition 1.9 n'ont plus d'intérêt : le supremum du nombre d'étapes de retournement pour retourner $u^{-1}v$, avec u, v des simples, n'est pas fini, tout comme le supremum des longueurs des mots simples. On montre dans cette section que les équivalences asymptotiques de la proposition 1.11 ne sont plus valables lorsque n n'est pas fixé.

2.1 2-COMPLEXITÉ QUARTIQUE

Proposition 2.1. *Pour tout ℓ il existe des mots u, v de longueur ℓ satisfaisant*

$$\mathrm{L}_1(u^{-1}v) \geq 2\ell^2 \quad \textit{et} \quad \mathrm{L}_2(u^{-1}v) \geq \ell^4,$$

pour ℓ suffisamment grand.

Avant de montrer la proposition, on montre un lemme préparatoire. On rappelle que $w \curvearrowright^{(k)} w'$ signifie qu'il existe une suite de retournement de longueur k de w à w'.

Lemme 2.2. *Pour $i, p \geq 1$, on pose $a_{i,p} = \sigma_{i+p-1}\sigma_{i+p-2}...\sigma_i$, $b_{i,p} = \sigma_i\sigma_{i+1}...\sigma_{i+p-1}$, $c_{i,p} = a_{i,p}a_{i+1,p}$, et $d_{i,p} = b_{i+1,p}b_{i,p}$. Alors, pour tous i, p, on a*

$$(1) \qquad b_{i,p}^{-1}\, a_{i+1,p} \curvearrowright^{(N_p)} a_{i,p+1}\, b_{i,p+1}^{-1},$$

$$(2) \qquad {d_{i,p}}^{-1}\, c_{i+2,p} \curvearrowright^{(N'_p)} c_{i,p+2}\, d_{i,p+2}^{-1},$$

avec $N_p = p^2 + p - 1$ et $N'_p = 4p^2 + 8p - 3$.

Démonstration. Pour (1) on raisonne par récurrence sur p. Le cas $p = 1$ est

$$b_{i,1}^{-1}\, b_{i+1,1} \curvearrowright^{(1)} a_{i,2}\, b_{i,2}^{-1},$$

ou, autrement dit, $\sigma_i^{-1}\sigma_{i+1} \curvearrowright^{(1)} \sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\sigma_i^{-1}$. Supposons $p \geq 2$. En utilisant l'hypothèse de récurrence une fois, plus une étape de type I et une étape de type III — ou une étape I'

à la place — et $2p-2$ étapes de type II, on obtient

$$\begin{aligned}
b_{i,p}^{-1}\, a_{i+1,p} = \quad & \sigma_{i+p-1}^{-1}\, [b_{i,p-1}^{-1}\, \sigma_{i+p}]\, a_{i+1,p-1} \\
\curvearrowright^{(p-1)} \quad & \sigma_{i+p-1}^{-1}\, \sigma_{i+p}\, [b_{i,p-1}^{-1}\, a_{i+1,p-1}] \\
\curvearrowright^{(N_{p-1})} \quad & [\sigma_{i+p-1}^{-1}\, \sigma_{i+p}]\, a_{i,p}\, b_{i,p}^{-1} \\
\curvearrowright^{(1)} \quad & \sigma_{i+p}\, \sigma_{i+p+1}\, \sigma_{i+p}^{-1}\, [\sigma_{i+p+1}^{-1}\, a_{i+1,p}]\, b_{i,p}^{-1} \\
\curvearrowright^{(1)} \quad & \sigma_{i+p}\, \sigma_{i+p+1}\, [\sigma_{i+p}^{-1}\, a_{i+1,p-1}]\, b_{i,p}^{-1} \\
\curvearrowright^{(p-1)} \quad & \sigma_{i+p}\, \sigma_{i+p+1}\, a_{i+1,p-1}\, \sigma_{i+p}^{-1}\, b_{i,p}^{-1} = a_{i,p+1}\, b_{i,p+1}^{-1}.
\end{aligned}$$

On en déduit $N_p = N_{p-1} + 2p = p^2 + p - 1$.

Les calculs pour (2) sont illustrés à la figure 1. En utilisant (1) quatre fois, plus $4p+1$ étapes de type II, on obtient

$$\begin{aligned}
d_{i,p}^{-1}\, c_{i+2,p} = \quad & b_{i,p}^{-1}\, [b_{i+1,p}^{-1}\, a_{i+2,p}]\, a_{i+3,p} \\
\curvearrowright^{(N_p)} \quad & b_{i,p}^{-1}\, a_{i+1,p+1}\, b_{i+1,p+1}^{-1}\, a_{i+3,p} \\
= \quad & [b_{i,p}^{-1}\, \sigma_{i+p+1}]\, a_{i+1,p}\, b_{i+1,p+1}^{-1}\, a_{i+3,p} \\
\curvearrowright^{(p)} \quad & \sigma_{i+p+1}\, [b_{i,p}^{-1}\, a_{i+1,p}]\, b_{i+1,p+1}^{-1}\, a_{i+3,p} \\
\curvearrowright^{(N_p)} \quad & \sigma_{i+p+1}\, a_{i,p+1}\, b_{i,p+1}^{-1}\, b_{i+1,p+1}^{-1}\, a_{i+3,p} \\
= \quad & a_{i,p+2}\, b_{i,p+1}^{-1}\, b_{i+2,p}^{-1}\, [\sigma_{i+1}^{-1}\, a_{i+3,p}] \\
\curvearrowright^{(p)} \quad & a_{i,p+2}\, b_{i,p+1}^{-1}\, [b_{i+2,p}^{-1}\, a_{i+3,p}]\, \sigma_{i+1}^{-1} \\
\curvearrowright^{(N_p)} \quad & a_{i,p+2}\, b_{i,p+1}^{-1}\, a_{i+3,p+1}\, b_{i+3,p+1}^{-1}\, \sigma_{i+1}^{-1} \\
= \quad & a_{i,p+2}\, b_{i+1,p}^{-1}[\, \sigma_i^{-1}\, \sigma_{i+p+2}\, a_{i+2,p}]\, b_{i+2,p+2}^{-1} \\
\curvearrowright^{(p+1)} \quad & a_{i,p+2}\, [b_{i+1,p}^{-1}\, \sigma_{i+p+2}]\, a_{i+2,p}\, \sigma_i^{-1}\, b_{i+1,p+1}^{-1} \\
\curvearrowright^{(p)} \quad & a_{i,p+2}\, \sigma_{i+p+2}\, [b_{i+1,p}^{-1}\, a_{i+2,p}]\, \sigma_i^{-1}\, b_{i+1,p+1}^{-1} \\
\curvearrowright^{(N_p)} \quad & a_{i,p+2}\, \sigma_{i+p+2}\, a_{i+1,p+1}\, b_{i+1,p+1}^{-1}\, \sigma_i^{-1}\, b_{i+1,p+1}^{-1} = c_{i,p+2}\, d_{i,p+2}^{-1}.
\end{aligned}$$

La somme donne $N'_p = 4p^2 + 8p - 3$. □

On peut maintenant prouver la proposition 2.1.

Démonstration de la proposition 2.1. (Figure 2.) On pose

$$u_\ell = \sigma_{2\ell}\sigma_{2\ell-2}...\sigma_2 \quad \text{et} \quad v_\ell = \sigma_1\sigma_3...\sigma_{2\ell-1},$$

et on considère le retournement de $u_\ell^{-1}v_\ell$. On distingue trois suites d'étapes. Premièrement, $\ell(\ell-2)/2$ étapes de type II mènent à

$$\sigma_2^{-1}\, \sigma_1\, \sigma_4^{-1}\, \sigma_3\, ...\, \sigma_{2\ell}^{-1}\, \sigma_{2\ell-1}.$$

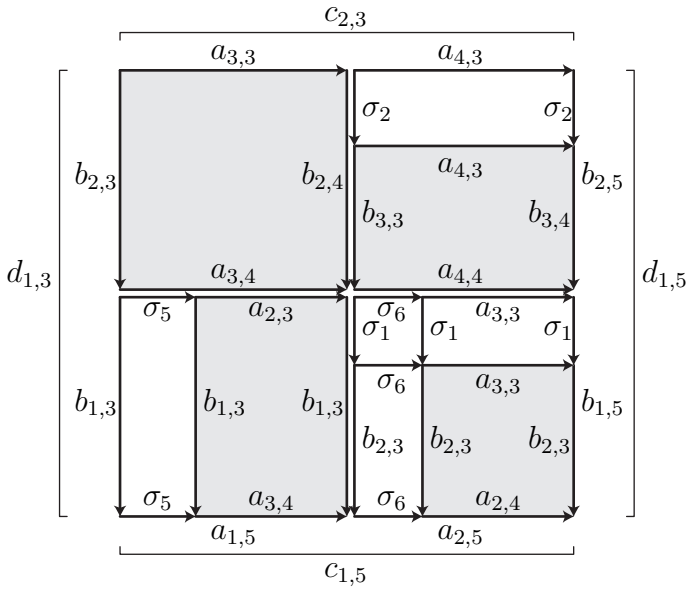


FIGURE 1 – Démonstration de la relation 2, ici avec $i = 1$ et $p = 3$; les rectangles gris correspondent à la relation 1.

Puis, ℓ étapes de type I mènent à $\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}\ \sigma_3\sigma_4\sigma_3^{-1}\sigma_4^{-1}\ \ldots\ \sigma_{2\ell-1}\sigma_{2\ell}\sigma_{2\ell-1}^{-1}\sigma_{2\ell}^{-1}$, qu'on réécrit sous la forme

$$c_{1,1}\ d_{2,1}^{-1}\ c_{3,1}\ d_{4,1}^{-1}\ \ldots\ c_{2\ell-1,1}\ d_{2\ell,1}^{-1}.$$

Ensuite, on applique (2) à répétition : avec $\ell - 1$ applications, on obtient

$$c_{1,1} \cdot c_{1,3}\ d_{2,3}^{-1}\ c_{3,3}\ d_{4,3}^{-1}\ \ldots\ c_{2\ell-3,3}\ d_{2\ell-2,3}^{-1} \cdot d_{2\ell,1}^{-1};$$

puis avec $\ell - 2$ applications supplémentaires, on arrive à

$$c_{1,1}\ c_{1,3} \cdot c_{1,5}\ d_{2,5}^{-1}\ c_{3,5}\ d_{4,3}^{-1}\ \ldots\ c_{2\ell-5,5}\ d_{2\ell-4,5}^{-1} \cdot d_{2\ell-2,3}^{-1}\ d_{2\ell,1}^{-1},$$

et ainsi de suite. Finalement, après avoir utilisé (2) $\ell(\ell-1)/2$ fois, on obtient

$$c_{1,1}\ c_{1,3}\ldots c_{1,2\ell+1}\ d_{2,2\ell-1}^{-1}\ d_{4,2\ell-3}^{-1}\ \ldots\ d_{2\ell-2,3}^{-1}\ d_{2\ell,1}^{-1},$$

qui est de longueur $2\ell(\ell-1)$, montrant que la 1-complexité de $u_\ell^{-1}v_\ell$ est quadratique en ℓ. De plus, en sommant toutes les étapes, on montre que la 2-complexité de $u_\ell^{-1}v_\ell$, c'est-à-dire la longueur de la suite de retournement maximale issue de $u_\ell^{-1}v_\ell$, est $(8\ell^4 - 23\ell^2 + 9\ell + 12)/6$. □

Remarque 2.3. On ne connaît pas de mots dont la 2-complexité soit supérieure à celle donnée par les mots u_ℓ et v_ℓ de la preuve de la proposition 2.1. Il est remarquable que ces mots soient des mots simples (au sens de la définition IV.1.7).

Remarque 2.4. En faisant passer la borne inférieure de cubique à quartique, la proposition 2.1 améliore d'un ordre de grandeur la dernière minoration connue [12, p. 13] de la 2-complexité au pire : le retournement des mots $(\sigma_1\sigma_3\dots\sigma_{2\ell-1})^{-1}\sigma_2\sigma_4\dots\sigma_{2\ell}$ est de 2-complexité $(8\ell^3-9\ell^2+4\ell)/3$ — et de 1-complexité quadratique.

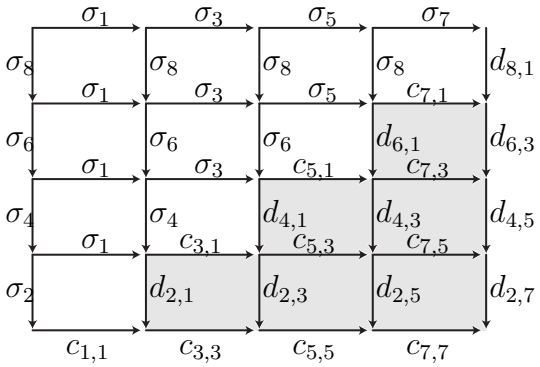


FIGURE 2 – (Démonstration de la proposition 2.1.) Diagramme de retournement simplifié dans le cas, ici pour $\ell = 4$; chaque rectangle grisé correspond à une relation (2), leur nombre est quadratique en la longueur du mot initial.

ℓ	2	4	8	16
$\mathrm{L}_1(w_\ell)$	4	24	112	480
$\mathrm{L}_2(w_\ell)$	1	11	288	5230

TABLE 1 – Dans le cas de mots de tresse de largeur non bornée, le nombre d'étapes de retournement L_2 peut dépasser la borne quadratique (du cas borné) et croître quartiquement. La longueur du mot terminal L_1 peut avoir une croissance quadratique — alors qu'elle est linéaire dans le cas n fixé (section 1). Ici le mot w_ℓ est le mot $u_\ell^{-1}v_\ell$ donné dans la preuve de la proposition 2.1 par $u_\ell = \sigma_{2\ell}\sigma_{2\ell-2}...\sigma_2$ et $v_\ell = \sigma_1\sigma_3...\sigma_{2\ell-1}$.

De ce calcul, on tire deux corollaires :

Corollaire 2.5. *Pour $\ell \geq 1$, posons $u_\ell = \sigma_{2\ell}\sigma_{2\ell-2}\dots\sigma_2$ et $v_\ell = \sigma_1\sigma_3\dots\sigma_{2\ell-1}$. Le diagramme de retournement de $u_\ell^{-1}v_\ell$ est optimal et on a $\mathrm{dist}_\curvearrowright(u_\ell, v_\ell) \in \Theta(\ell^4)$.*

Démonstration. D'après les calculs du lemme 2.2 et de la proposition 2.1, le diagramme de retournement de $u_\ell^{-1}v_\ell$ est compact et sans digones. Donc d'après la proposition IV.4.11, le diagramme est optimal. De plus, le nombre de pavés de type I' est quadratique en ℓ et il n'y a ni pavés de type I" ni pavés de type III, d'où l'équivalent asymptotique. □

Notation. On pose $\mathrm{L}_1(\ell) = \sup\{\mathrm{L}_1(\ell, n); n \in \mathbb{N}\}$ et $\mathrm{L}_2(\ell) = \sup\{\mathrm{L}_2(\ell, n); n \in \mathbb{N}\}$.

Corollaire 2.6. *On a les minorations asymptotiques*

$$\mathrm{L}_1(\ell) \in \Omega(\ell^2) \quad \textit{et} \quad \mathrm{L}_2(\ell) \in \Omega(\ell^4).$$

2.2 ESTIMATIONS PAR ORDINATEUR

Le retournement d'un mot (de tresse) est une opération aisément réalisable sur ordinateur. Le calcul des 1- et 2-complexités est donc simple à réaliser.

Expérimentalement, on ne trouve pas de familles de mots dont la 2-complexité dépasse la borne quartique établie plus haut. Sans obligatoirement chercher de familles, on peut toutefois pour chaque longueur de mots, chercher celui (ou ceux) de complexité maximale. En raison du trop grand nombre de mots, la recherche des pires cas (par exhaustion) est rapidement impossible : au-delà de la longueur 14, nous n'avons pas retourné tous les mots.

Grâce aux premiers cas, on est en mesure de décrire un sous-ensemble de l'ensemble des mots dans lequel on conjecture trouver les mots de 2-complexité maximale.

Conjecture 2.7. *Soient u, v deux mots dont la somme des longueurs est 2ℓ. Alors les mots u et v maximisant $\mathrm{L}_2(u^{-1}v)$ satisfont les contraintes suivantes :*

- *u et v sont positifs ;*
- *u et v sont de longueur ℓ ;*
- *tous les générateurs d'indice pair (resp. impair) sont dans u (resp. v) ;*
- *chaque générateur d'indice compris entre 1 et 2ℓ apparaît exactement une fois ;*
- *pour $i \leq \ell$, si la i^e lettre de u est σ_j, alors la i^e lettre de v est $\sigma_{\ell+1-j}$.*

Remarque 2.8. Notons $E_{2\ell}$ l'ensemble des mots $u^{-1}v$ vérifiant les conditions de la conjecture 2.7. On a procédé à la recherche exhaustive de l'ensemble $E_{2\ell}$ jusqu'à $\ell = 10$ (voir tableau 2). Pour chaque ℓ, le mot de $E_{2\ell}$ de 2-complexité maximale a été comparé à un grand nombre (plusieurs millions) de mots de longueur 2ℓ de $\mathrm{BW}_\infty \setminus E_{2\ell}$: pour $2\ell \leq 20$, le maximum est toujours trouvé dans $E_{2\ell}$.

3 MAJORATION DE LA 1-COMPLEXITÉ

Le but de cette section est de montrer que les 1- et 2-complexités des mots de tresse de longueur ℓ atteignent leurs maxima sur des mots dont la largeur est au plus 2ℓ, ce qui traduit le fait intuitif que des croisements sur des brins éloignés n'interfèrent pas.

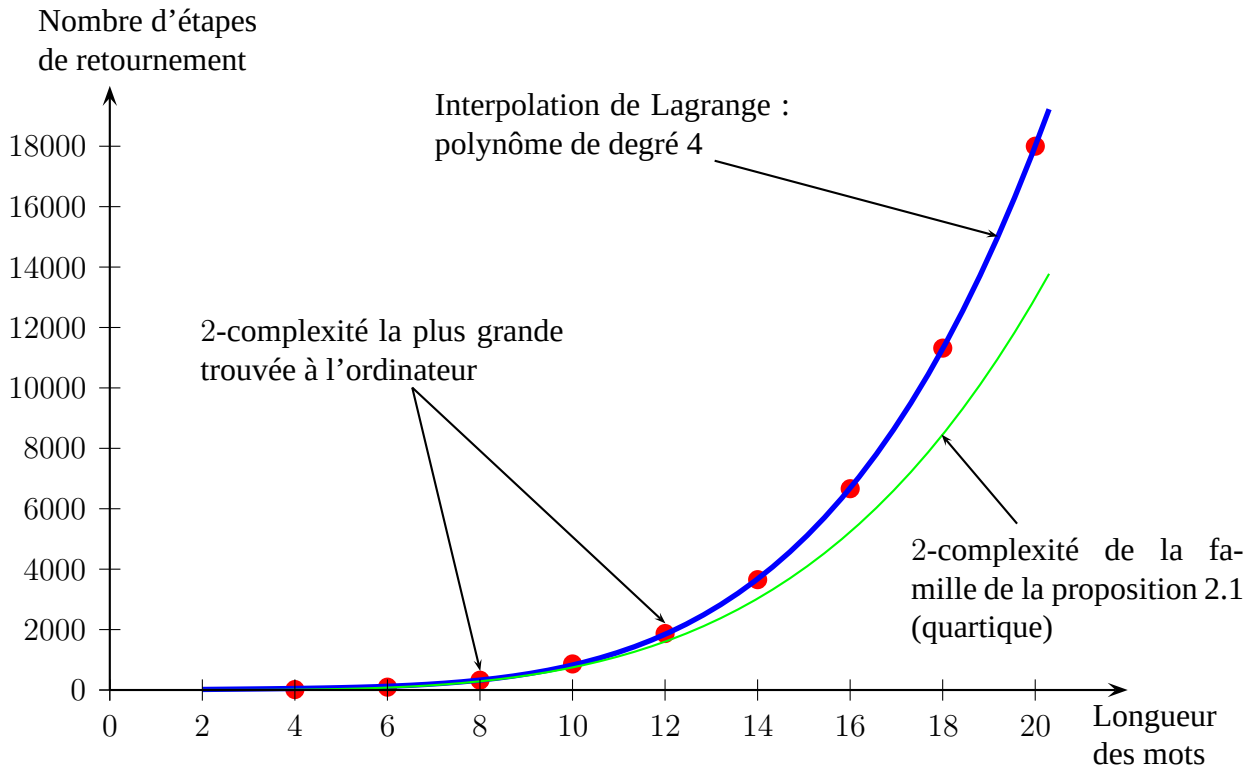


FIGURE 3 – (Tableau 2). On obtient par ordinateur les mots de 2-complexité la plus élevée possible jusqu'à la longueur 20 (points). Leur répartition suggère qu'il n'existe pas de famille de mots dont la complexité croîtrait plus vite qu'un polynôme de degré 4 (courbe épaisse). La 2-complexité des mots de la proposition 2.1 a une croissance quartique (courbe fine).

2ℓ	E	Mot de plus grande 2-complexité	LM	L_2
4	✓	$(\sigma_2\sigma_4)^{-1}\sigma_3\sigma_1$	✓	18
6	✓	$(\sigma_2\sigma_4\sigma_6)^{-1}\sigma_5\sigma_3\sigma_1$	✓	97
8	✓	$(\sigma_4\sigma_2\sigma_8\sigma_6)^{-1}\sigma_5\sigma_7\sigma_1\sigma_3$	✓	328
10	✓	$(\sigma_6\sigma_8\sigma_{10}\sigma_2\sigma_4)^{-1}\sigma_5\sigma_3\sigma_1\sigma_9\sigma_7$	✓	859
12	✓	$(\sigma_6\sigma_4\sigma_2\sigma_{10}\sigma_{12}\sigma_8)^{-1}\sigma_7\sigma_9\sigma_{11}\sigma_3\sigma_1\sigma_5$	✓	1870
14		$(\sigma_6\sigma_8\sigma_4\sigma_2\sigma_{12}\sigma_{14}\sigma_{10})^{-1}\sigma_9\sigma_7\sigma_{11}\sigma_{13}\sigma_3\sigma_1\sigma_5$	✓	3649
16		$(\sigma_{10}\sigma_8\sigma_{12}\sigma_{14}\sigma_{16}\sigma_2\sigma_4\sigma_6)^{-1}\sigma_7\sigma_9\sigma_5\sigma_3\sigma_1\sigma_{15}\sigma_{13}\sigma_{11}$	✓	6660
18		$(\sigma_8\sigma_{10}\sigma_6\sigma_4\sigma_2\sigma_{16}\sigma_{18}\sigma_{14}\sigma_{12})^{-1}\sigma_{11}\sigma_9\sigma_{13}\sigma_{15}\sigma_{17}\sigma_3\sigma_1\sigma_5\sigma_7$	✓	11313
20		$(\sigma_{12}\sigma_{10}\sigma_{14}\sigma_{16}\sigma_{18}\sigma_{20}\sigma_2\sigma_4\sigma_6\sigma_8)^{-1}\sigma_9\sigma_{11}\sigma_7\sigma_5\sigma_3\sigma_1\sigma_{19}\sigma_{17}\sigma_{15}\sigma_{13}$	✓	18000

TABLE 2 – 2-complexités (L_2) les plus élevées par longueur (ℓ). Pour les petites longueurs, la recherche exhaustive (E) fut possible. Pour les longueurs supérieures à 14, on a testé l'ensemble des mots décrits à la conjecture 2.7. On indique si le mot ayant la plus grande complexité est de largeur maximale (LM), autrement dit si ses largeur et longueur coïncident.

3.1 NOTIONS PRÉLIMINAIRES

Définition 3.1 (support)**.** On appelle *support* du mot de tresse u, et on note $\mathrm{Supp}(u)$, l'ensemble $\{i\ ;\ \sigma_i^{\pm 1}$ est une lettre de $u\}$.

Définition 3.2 (ensemble connexe, composante connexe)**.** Soit E une partie finie de $\mathbb{N}$. On dit que E est *connexe* si E vérifie $\max(E) - \min(E) = \#E - 1$. Soient I et F des ensembles satisfaisant les inclusions $I \subset F \subset \mathcal{P}(\mathbb{N})$. On dit que I est une *composante connexe de* F si I est un sous-ensemble connexe maximal de F, c'est-à-dire que s'il existe un ensemble J contenant I alors on a $I = J$.

Exemple 3.3. Soit E l'ensemble $\{0, 1, 2, 3, 4\}$. L'ensemble E est connexe. En effet, on a $\max(E) - \min(E) = 4 - 0 = 4 = \#E - 1$. L'ensemble $E\backslash\{1\}$ n'est pas connexe car il a deux composantes connexes, qui sont $\{0\}$ et $\{2, 3, 4\}$.

Notation. Soit E un ensemble. On note $\mathrm{C}(E)$ l'ensemble des composantes connexes de E. Soit w un mot de BW_∞. On note $\mathrm{C}(u)$ pour $\mathrm{C}(\mathrm{Supp}(u))$.

Remarque 3.4. Deux composantes I et J connexes distinctes d'un ensemble E sont disjointes. On ordonne alors $\mathrm{C}(E)$ par $<$ en posant $I < J \Leftrightarrow \exists i \in I, \exists j \in J,\ i < j$.

Notation. On note $\mathrm{C}_i(w)$ la i^{e} composante connexe de w pour l'ordre $<$. Soit w un mot de BW_∞. On note $\mathrm{WC}_i(w)$, le sous-mot maximal de support $\mathrm{C}_i(w)$ parmi tous les mots obtenus à partir de w en n'appliquant que des relations de type II, c'est-à-dire des relations de la forme $\sigma_i\sigma_j = \sigma_j\sigma_i$ avec $|j - i| \geq 2$, et uniquement entre lettres dont les indices sont dans des composantes connexes différentes.

Exemple 3.5. Soit w le mot $\sigma_4\sigma_2\sigma_1^{-1}\sigma_5\sigma_2$. On a $\mathrm{Supp}(w) = \{1,2,4,5\}$, $\mathrm{C}_1(w) = \{1,2\}$ et $\mathrm{C}_2(w) = \{4,5\}$. Par application de relations de type II, on obtient $\sigma_2\sigma_1^{-1}\sigma_2\sigma_4\sigma_5$ et donc $\mathrm{WC}_1(w) = \sigma_2\sigma_1^{-1}\sigma_2$ et $\mathrm{WC}_2(w) = \sigma_4\sigma_5$.

Définition 3.6 (opération sh)**.** Le *décalé à droite d'un mot* w est le mot $\mathrm{sh}(w)$ dans lequel chaque lettre σ_i de w a été remplacée par σ_{i+1}. On dit que w est un décalé de w' s'il existe un entier positif p satisfaisant $\mathrm{sh}^p(w') = w$, avec $\mathrm{sh}^p(w') = \mathrm{sh}(\mathrm{sh}^{p-1}(w'))$ et $\mathrm{sh}^1(w') = \mathrm{sh}(w')$.

Lemme 3.7. *Pour tout mot* w *de* BW_∞*, on a* $\mathrm{L}_1(w) = \mathrm{L}_1(\mathrm{sh}(w))$ *et* $\mathrm{L}_2(w) = \mathrm{L}_2(\mathrm{sh}\, w)$.

Démonstration. Il suffit de remarquer que pour i et j positifs, on a

$$\sigma_i\sigma_{i+1}\sigma_i \equiv \sigma_{i+1}\sigma_i\sigma_{i+1} \Leftrightarrow \mathrm{sh}(\sigma_i\sigma_{i+1}\sigma_i) \equiv \mathrm{sh}(\sigma_{i+1}\sigma_i\sigma_{i+1})$$

et

$$\sigma_i\sigma_j \equiv \sigma_j\sigma_i \Leftrightarrow \mathrm{sh}(\sigma_i\sigma_j) \equiv \mathrm{sh}(\sigma_j\sigma_i).$$

□

Lemme 3.8. *Soient* w, w' *des mots de* BW_∞ *ayant chacun deux composantes connexes. On suppose qu'on a* $\mathrm{WC}_1(w) = \mathrm{WC}_1(w')$ *et que* $\mathrm{WC}_2(w')$ *est un décalé de* $\mathrm{WC}_2(w)$*. Alors on a* $\mathrm{L}_1(w) = \mathrm{L}_1(w')$ *et* $\mathrm{L}_2(w) = \mathrm{L}_2(w')$.

Démonstration. C'est une application directe du lemme 3.7. □

Remarque 3.9. Le lemme permet de restreindre l'étude de la complexité du retournement aux seuls mots dont la distance entre les composantes connexes est 2.

3.2 BORNES SUPÉRIEURES

On obtient immédiatement le lemme suivant.

Lemme 3.10. *Pour* $\ell > 2$*, on a*

$$\mathrm{L}_1(\ell) = \mathrm{L}_1(\ell, 2\ell).$$

Démonstration. Soit un mot w de longueur ℓ dans BW_∞. Posons $n = \max(\mathrm{Supp}(w)) + 1$. On en déduit $w \in \mathrm{BW}_n$. D'après le lemme 3.8, on peut supposer que les composantes connexes de u sont à distance 2. D'après le lemme 3.7, quitte à décaler w, on peut supposer $\min(\mathrm{Supp}(w)) = 1$. Or le mot le plus large qu'on puisse former dans lequel apparaît σ_1, qui soit de longueur ℓ et pour lequel les composantes connexes sont à distance 2 est de largeur $2\ell - 1$, par exemple le mot $\sigma_1\sigma_3 \ldots \sigma_{2\ell-1}$. On peut dès lors supposer que w est dans $\mathrm{BW}_{2\ell}$, d'où on obtient $\mathrm{L}_1(\ell) \leq \mathrm{L}_1(\ell, 2\ell)$. Or, par définition de $\mathrm{L}_1(\ell)$, on a aussi $\mathrm{L}_1(\ell) \geq \mathrm{L}_1(\ell, 2\ell)$, d'où en fait $\mathrm{L}_1(\ell) = \mathrm{L}_1(\ell, 2\ell)$. □

Remarque 3.11. Plus le nombre de brins qu'on s'autorise à croiser augmente, plus la 1-complexité augmente puisque toute tresse dans laquelle n brins se croisent peut toujours être vue comme tresse sur p brins, $p \geq n$, dans laquelle les $p - n$ derniers brins ne sont pas tressés. Donc, pour tout entier positif ℓ, la suite $(\mathrm{L}_1(\ell, n))_{n\geq 3}$ est croissante. Le lemme précédent montre qu'en réalité cette suite est stationnaire dès le rang 2ℓ.

Proposition 3.12. *Pour tout entier positif ℓ, la suite $(\mathrm{L}_1(\ell, n))_{n\geq 3}$ est stationnaire à partir du rang $2\ell - 1$.*

Démonstration. D'après la remarque 3.11 et le lemme 3.10, il s'agit de voir qu'on a l'égalité $\mathrm{L}_1(\ell, 2\ell - 1) = \mathrm{L}_1(\ell, 2\ell)$. Considérons donc les mots de longueur ℓ. Par le lemme 3.7, on se restreint aux mots contenant σ_1. Les mots de longueur ℓ de $\mathrm{BW}_{2\ell}$ qui ne sont pas dans $\mathrm{BW}_{2\ell-1}$ sont les mots de largeur $2\ell - 1$. Ces mots possèdent une copie de chaque générateur (ou de son inverse) d'indice impair et sont donc de la forme $\sigma_1^{\pm 1}\sigma_3^{\pm 1}\ldots\sigma_{2\ell-1}^{\pm 1}$ (à permutation des lettres près). Pour tout mot w de cette forme, on a $\mathrm{L}_1(w) = \ell$, ce qui n'est pas le maximum qu'on peut obtenir avec un mot de longueur ℓ (voir par exemple la famille de mots présentée à la proposition 2.1). On en déduit $\mathrm{L}_1(\ell, 2\ell - 1) \geq \mathrm{L}_1(\ell, 2\ell)$, ce qui achève la preuve. □

Remarque 3.13. La proposition établit qu'en termes de complexité du retournement, les mots de longueur ℓ sont les plus complexes dès qu'ils sont dans $\mathrm{BW}_{2\ell-1}$.

À la proposition 1.9 on a borné supérieurement — et explicitement en fonction de n — la 1-complexité des mots de BW_n, pour un n fixé. En reliant ce résultat et la remarque 3.13, on borne supérieurement $\mathrm{L}_1(\ell)$.

Proposition 3.14. *Pour tout entier positif ℓ, on a*

$$\mathrm{L}_1(\ell) \leq \ell.\left(\frac{(2\ell-1)(2\ell-2)}{2} - 1\right).$$

Démonstration. D'après le lemme 3.12, on a $\mathrm{L}_1(\ell) = \mathrm{L}_1(\ell, 2\ell - 1)$ puis en appliquant la proposition 1.9 avec $n = 2\ell - 1$, pour tout mot w de longueur ℓ, on obtient

$$\mathrm{L}_1(w) \leq e(2\ell - 1)|w|_{S_{2\ell-1}}.$$

La première remarque est qu'on a $|w|_{S_{2\ell-1}} \leq \ell$. La deuxième remarque est que la valeur $n(n-1)/2$ donnée à $e(n)$ au lemme 1.6 peut être affinée pour la raison suivante : pour donner une valeur à $e(n)$ on a majoré la taille des mots $u\backslash v$, pour u et v simples, par la longueur de l'élément de Garside Δ_n, à savoir $n(n-1)/2$; or les mots $u\backslash v$ qu'on obtient ne représentent pas Δ_n mais sont des préfixes stricts d'expressions de Δ_n. En combinant ces deux remarques, on obtient le résultat annoncé. □

On pourrait encore améliorer la borne de quelques unités en étudiant avec un peu de soin les retournements des mots de longueur ℓ et de largeur $2\ell - 2$, puis $2\ell - 3$, etc. En fait, nous pensons que le résultat suivant est vrai :

Conjecture 3.15. *Pour tout entier positif ℓ, la suite $(\mathrm{L}_1(\ell, n))_{n\geq 3}$ est stationnaire à partir du rang $\ell + 1$.*

Remarque 3.16. Montrer cette conjecture améliorerait la borne de la proposition 3.14 d'un facteur 4. Ceci n'est pas le meilleur résultat espéré : on ne connaît aucune famille de mots dont la 1-complexité croît plus vite que quadratiquement alors que la borne de la proposition 3.14 est cubique.

Plus que le résultat de cette conjecture donc, ce que l'expérience mène à croire est la conjecture suivante :

Conjecture 3.17. *On a*

$$\mathrm{L}_1(\ell) \in \Theta(\ell^2).$$

Remarque 3.18. En réalité, la façon qu'on a de borner supérieurement la 1-complexité du retournement fait intervenir une borne intermédiaire : on commence par borner supérieurement la 1-complexité de $u^{-1}v$, où u et v sont des simples, puis, s'appuyant sur le fait que tout mot se décompose en produit de simples d'une part et que $u\backslash v$ et $v\backslash u$ sont des simples d'autre part, on énonce une borne supérieure pour la 1-complexité du retournement d'un mot quelconque. La borne pour les simples est quadratique et est optimale : la suite $(\mathrm{L}_1(u_\ell^{-1}v_\ell))_{\ell\geq 1}$, avec, pour $\ell \geq 1$, $u_\ell = \sigma_1 \dots \sigma_{2\ell-1}$ et $v_\ell = \sigma_2 \dots \sigma_{2\ell}$, croît quadratiquement avec ℓ. C'est donc en établissant la deuxième borne que le calcul est trop grossier ; la majoration qu'on donne pour le cas d'un mot quelconque part du principe que le « pire global » est une juxtaposition de « pires locaux ». Cette approche ne tient pas compte du fait qu'on ne peut — apparemment — pas cumuler uniquement des cas localement les pires. Il s'agirait donc, pour améliorer significativement la borne cubique de la proposition 3.14, de mieux comprendre les relations entre les différents retournements de simples qu'implique le retournement d'un mot quelconque.

4 MAJORATION DE LA 2-COMPLEXITÉ : RETOURNEMENT PACIFIQUE

Contrairement aux méthodes employées pour les résultats de minoration et de majoration des 1- et 2-complexités obtenus jusqu'à maintenant, ce sont des considérations géométriques et non plus seulement combinatoires qui nous permettent dans cette section de calculer une borne supérieure simplement exponentielle.

Partant d'un mot $u^{-1}v$ avec u et v positifs, on a montré à la proposition 3.14 que la longueur du mot terminal était au plus cubique en la longueur de $u^{-1}v$. Cette borne n'est pas

suffisante pour majorer le nombre d'étapes de retournements : il se pourrait que les mots intermédiaires, c'est-à-dire les mots de la suite de retournement issue de $u^{-1}v$, croissent fortement, ce qui nécessiterait un grand nombre d'étapes de retournement, avant de décroître d'autant, ce phénomène étant *a priori* rendu possible par l'ajout de lettres dans un mot intermédiaire lors d'un retournement utilisant une relation de type I ou la suppression de lettres dans un mot intermédiaire lors d'un ε-retournement.

Dans cette section, nous introduisons une version modifiée du retournement, qui garde une trace des ε-retournements, et qui permet de majorer la longueur de la suite de retournement issue de $u^{-1}v$, c'est-à-dire la 2-complexité de $u^{-1}v$.

4.1 GRILLE DE RETOURNEMENT

Le premier résultat donne une majoration de la longueur des mots d'une suite de retournement.

Proposition 4.1. *[17, Proposition 3(i)] Soit w un n-mot de tresse de longueur ℓ. Tout mot obtenu depuis w par retournement est de longueur au plus $C_n\ell$ avec $C_n = \frac{1}{2}3^n$.*

Définition 4.2. On appelle *grille de retournement* $G(\ell, n)$ la grille de $C_n\ell \times C_n\ell$ mailles carrées, où C_n est donné à la proposition 4.1.

Définition 4.3. Un n-mot w est *écrit* dans une grille de retournement $G(\ell, n)$ si
- on a $|w| \leq C_n\ell$,
- w a une lettre par côté de maille avec la règle qu'une lettre positive (resp. négative) est écrite sur un segment horizontal (resp. vertical),
- la première lettre de w est sur le côté gauche de $G(\ell, n)$ et la dernière est sur le bord supérieur de $G(\ell, n)$ (voir la figure 4).

D'après la proposition 4.1, tout mot issu du retournement d'un n-mot de tresse w de longueur ℓ est inscriptible dans la grille de retournement $G(\ell, n)$.

Remarque 4.4. Le but est que, partant d'un n-mot w de longueur ℓ, chacun des retournements successifs produise un mot qui progresse dans la grille, c'est-à-dire que le nombre de mailles dans la région au-dessus à gauche d'un mot augmente lorsqu'on le retourne. Ce faisant, le nombre d'étapes de retournement de w est majoré par le nombre de mailles de $G(\ell, n)$, à savoir $(C_n\ell)^2$.

4.2 LIMITE DU RETOURNEMENT

Notation. Soit w un n-mot de tresse de longueur ℓ. On note $\mathrm{UL}(w)$ le nombre de mailles dans la région au-dessus à gauche de w écrit dans la grille $G(\ell, n)$.

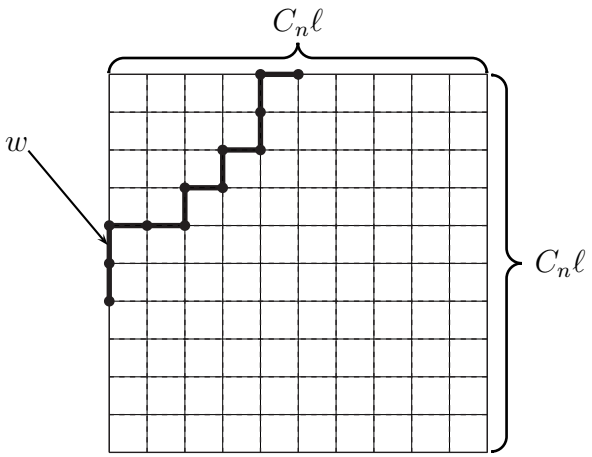


FIGURE 4 – Dans une grille $C_n\ell \times C_n\ell$, avec $C_n = 3^n/2$, on écrit un mot w en respectant les règles suivantes : le mot w touche le bord gauche (avec sa première lettre) et le bord supérieur (avec sa dernière lettre), chaque lettre positive (resp. négative) s'écrit horizontalement (resp. verticalement) et on écrit une seule lettre par segment. Sur ce diagramme, le chemin représente — par exemple — le mot $\sigma_1^{-2}\sigma_3\sigma_2\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_3\sigma_4^{-1}\sigma_3^{-1}\sigma_2$.

Si le n mot de tresse w de longueur ℓ est écrit dans $G(\ell, n)$, un mot w' obtenu depuis w par retournement ne borde pas nécessairement une région supérieure gauche plus grande que w (figure 6) :

Fait 4.5. *Il existe w, w' des n-mots de tresse vérifiant $w \curvearrowright^{(1)} w'$ et inscriptibles dans une grille $G(\ell, n)$ tels qu'on ait* $\mathrm{UL}(w') > \mathrm{UL}(w)$.

4.3 RETOURNEMENT PACIFIQUE

Afin de tenir compte des ε-retournements, on introduit un nouveau procédé de réécriture, très similaire au retournement de mot mais qui a la particularité de ne jamais supprimer de lettres.

Définition 4.6. Soient deux mots w et w' de $\{\sigma_1, \ldots, \sigma_{n-1}, \varepsilon_0\}^*$. On dit que w se *retourne pacifiquement en w' en une étape*, et on note $w \curvearrowright^P w'$, si on peut passer de w à w'
- soit en remplaçant un sous-mot $\sigma_j^{-1}\sigma_i$, avec $|j-i| = 1$, par $\sigma_i\sigma_j\sigma_i^{-1}\sigma_j^{-1}$,
- soit en remplaçant un sous-mot $\sigma_j^{-1}\sigma_i$, avec $|j-i| \geq 2$, par $\sigma_i\sigma_j^{-1}$,
- soit en remplaçant un sous-mot $\sigma_i^{-1}\sigma_i$ par $\varepsilon_0\varepsilon_0^{-1}$,
- soit en remplaçant un sous-mot $\varepsilon_0^{-1}\varepsilon_0$ par $\varepsilon_0\varepsilon_0^{-1}$.

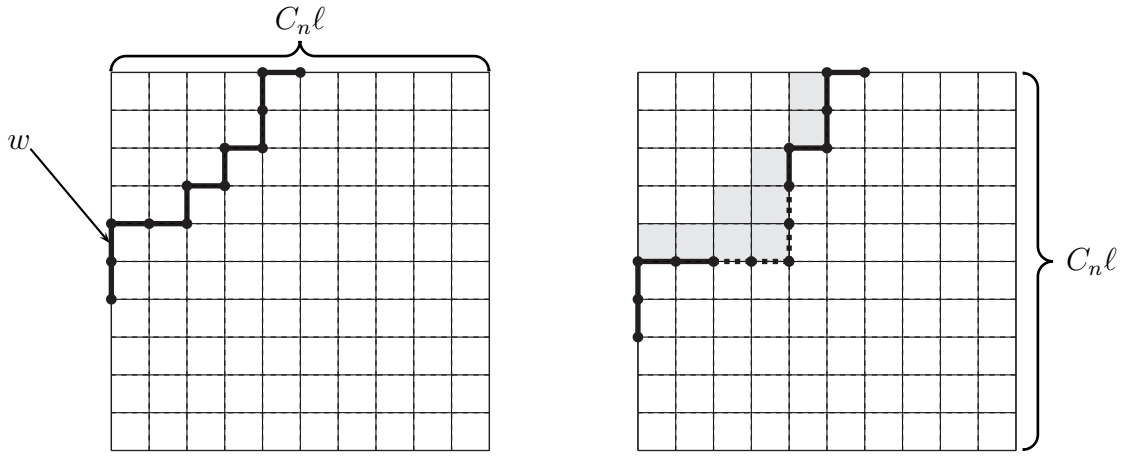


FIGURE 5 – En respectant les règles énoncées à la figure 4, on trace dans la grille de gauche le mot $\sigma_1^{-2}\sigma_3\sigma_2\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_3\sigma_4^{-1}\sigma_3^{-1}\sigma_2$, que l'on note w. Le retournement du motif $\sigma_2^{-1}\sigma_1$ de w en $\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$ et la réécriture adéquate du mot retourné dans la grille de droite permet d'accroître la zone supérieure gauche (cases grisées).

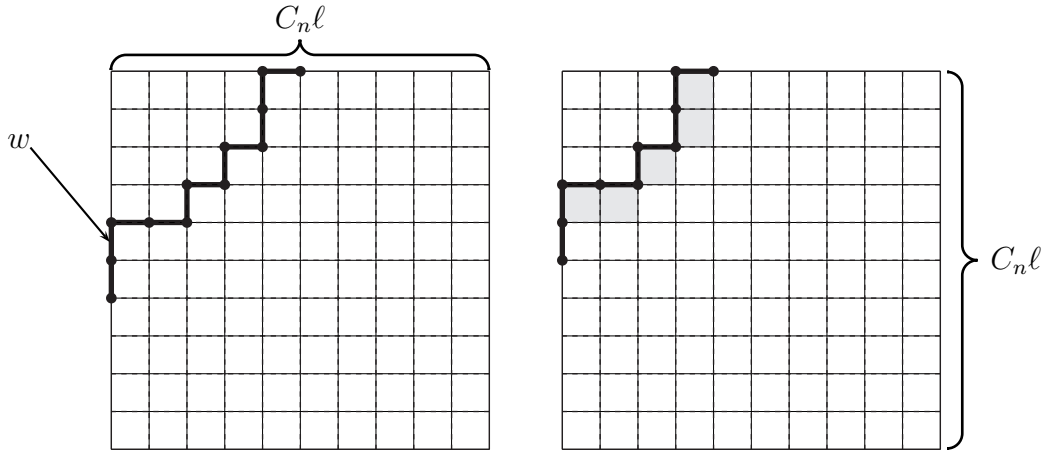


FIGURE 6 – En respectant les règles énoncées à la figure 4, on trace dans la grille de gauche le mot $\sigma_1^{-2}\sigma_3\sigma_2\sigma_2^{-1}\sigma_1\sigma_3^{-1}\sigma_3\sigma_4^{-1}\sigma_3^{-1}\sigma_2$, que l'on note w. Le retournement du motif $\sigma_3^{-1}\sigma_3$ de w en ε et la réécriture adéquate du mot retourné dans la grille de droite montre que la zone supérieure gauche décroît. Autrement le mot retourné recule dans la grille. Les cases grisées représentent les cases perdues.

De même que pour le retournement classique, on dit que w se *retourne pacifiquement en* w', et on note encore $w \curvearrowright^P w'$, s'il existe une suite de mots $w = w_0, w_1, \ldots, w_r = w'$ tels qu'on ait, pour tout i, $w_i \curvearrowright^P w_{i+1}$.

Remarque 4.7. On étend naturellement la définition de 2-complexité d'un mot w au retournement pacifique : la 2-complexité du retournement pacifique pour w est le nombre d'étapes de retournement pacifique requises pour obtenir un mot positif-négatif à partir de w.

Le premier résultat compare les 2-complexités du retournement pacifique et du retournement (classique).

Lemme 4.8. *La 2-complexité du retournement pacifique du mot w est supérieure à la 2-complexité du retournement de w.*

Démonstration. Il suffit de remarquer que toute étape de retournement nécessitée pour passer de w à un mot positif-négatif est également requise pour passer de w à un mot positif-négatif par retournement pacifique. □

On adapte maintenant la proposition 4.1 pour cette variante du retournement. On a :

Lemme 4.9. *Soit w un mot de tresse à n brins de longueur ℓ. Tout mot obtenu de w par retournement pacifique est de longueur au plus $C_n\ell$ avec $C_n = \frac{1}{2}3^n$.*

Démonstration. La preuve est en fait celle de la proposition 4.1 dans laquelle on prend soin de vérifier que la majoration donnée tient compte des retournements de sous-mots $\sigma_i^{-1}\sigma_i$ en $\varepsilon_0\varepsilon_0^{-1}$. □

Avec la proposition suivante, on établit une première borne supérieure pour la 2-complexité du retournement.

Lemme 4.10. *Pour tout ℓ et pour tout n, on a la majoration*

$$\mathrm{L}_2(\ell, n) \leq \frac{1}{4}3^{2n}\ell^2.$$

Démonstration. Soit w un n-mot de tresse de longueur ℓ écrit sur une grille de retournement $G(\ell, n)$. Comme le mot w se retourne pacifiquement en un mot positif-négatif uv^{-1}, il existe une suite de mots $w = w_0, \ldots w_r = uv^{-1}$ tels que le passage de w_i à w_{i+1} se fait en une étape de retournement pacifique. Il suffit de montrer que chaque étape de retournement pacifique produit un mot w_i à partir de w_{i-1} satisfaisant $\mathrm{UL}(w_i) > \mathrm{UL}(w_{i-1})$. En effet, la suite $(\mathrm{UL}(w_i))_{i\geq 0}$ étant majorée par le nombre de mailles dans la grille, cela suffit pour conclure que le nombre d'étapes ne peut excéder $3^{2n}\ell^2/4$.

Montrons donc que la suite $(\mathrm{UL}(w_i))_{i\geq 0}$ est strictement croissante. Il y a quatre transformations élémentaires à étudier. Les trois cas de retournement par commutativité sont évidents, une maille est ajoutée à la partie supérieure gauche. Il reste le cas $\sigma_{i+1}^{-1}\sigma_i$ dans un

mot $w_p\sigma_{i+1}^{-1}\sigma_i w_s$. Dans ce cas, on remarque qu'écrire le mot $w_p\sigma_i\sigma_{i+1}\sigma_i^{-1}\sigma_{i+1}^{-1}w_s$ dans la grille revient à translater le préfixe w_p du mot précédent d'une maille vers le bas et le suffixe w_s d'une maille vers la droite (voir la figure 5). On peut toujours réaliser ces opérations de translation car la grille est prévue pour accueillir n'importe quel mot issu du retournement pacifique de w (voir le lemme 4.9). □

D'après la section 3, on peut considérer qu'un mot de longueur ℓ est un mot de $\mathrm{BW}_{2\ell}$. Du lemme précédent on tire alors la première majoration du nombre d'étapes maximal que requiert le retournement d'un mot de longueur ℓ.

Proposition 4.11. *Pour $\ell \geq 1$, on a*

$$\mathrm{L}_2(\ell) \leq \frac{1}{4}3^{4\ell}\ell^2.$$

Remarque 4.12. Ce résultat améliore le résultat précédent [14, Corollary 3.3 (ii)] de plusieurs ordres de grandeur : la meilleure borne connue était supérieure à $4^{2^{2\ell^3-1}}$.

5 MAJORATION DE LA 2-COMPLEXITÉ : SÉPARATRICES

5.1 AMÉLIORATION DE LA BORNE

Dans ce paragraphe, on démontre une nouvelle borne supérieure pour la 2-complexité, meilleure que celle de la proposition 4.11. Ce résultat est fondé sur l'observation que tout pavé d'un diagramme de retournement est traversé au moins une fois par au moins une séparatrice. Il en découle que majorer le nombre de pavé que traverse chacune des séparatrices donne immédiatement une majoration du nombre de polygones dans le diagramme, et donc, de la 2-complexité.

Pour compter le nombre de pavés que traverse une séparatrice, on commence par y associer une notion de longueur.

Définition 5.1 (longueur d'une séparatrice)**.** On appelle *longueur* de la séparatrice Σ, et on la note $|\Sigma|$, le nombre de polygones qu'elle traverse.

Exemple 5.2. Dans la figure 7, les séparatrices du diagramme (a) sont de longueur 4, 5 et 6 et celles du diagramme (b) sont de longueur 3 et 5.

Les longueurs des séparatrices ne sont pas des données qu'on sait calculer ou du moins facilement borner. Toutefois, en associant chaque séparatrice à un mot tracé dans le diagramme, on parvient à une majoration.

Définition 5.3 (mot de séparatrice)**.** À toute séparatrice on associe le plus long mot intermédiaire possédant au moins une lettre sur le bord de chaque polygone traversé par la séparatrice.

On montre alors la borne supérieure annoncée.

Proposition 5.4. *Soient u et v deux simples tels qu'on ait $|u^{-1}v| = \ell$. On a alors*

$$\mathrm{L}_2(u^{-1}v) \in O(3^{2\ell}\ell^2).$$

Démonstration. Si w est le mot d'une séparatrice Σ, alors on a par définition $|\Sigma| \leq |w|$. Or, d'après la proposition 4.1, tout mot intermédiaire est de longueur inférieure à $3^{2\ell}/2$. On obtient donc $|\Sigma| \leq 3^{2\ell}/2$. On obtient le résultat en combinant cette borne avec le fait qu'il y a au plus $\ell(2\ell-1)$ séparatrices dans le diagramme de retournement de $u^{-1}v$ car u, v sont simples. □

Remarque 5.5. Ce résultat, énoncé dans le cas des simples, est généralisable au cas non simple. On multiplie alors la borne supérieure par un facteur quadratique ℓ^2. Bien que la borne qu'on donne ici en utilisant les séparatrices améliore d'un facteur exponentiel la borne calculée à l'aide du retournement pacifique (section 4), le résultat n'est pas pleinement satisfaisant : les calculs suggèrent que la longueur des mots intermédiaires est cubique au plus en la longueur des mots initiaux.

5.2 FORMALISME PRÉLIMINAIRE

Définition 5.6 (séparatrices horizontale, verticale et médiane)**.** On appelle séparatrice *horizontale* (resp. *verticale*) d'un hexagone la séparatrice y entrant et en sortant horizontalement (resp. verticalement). La troisième séparatrice est dite *médiane*. Dans un carré, on appelle séparatrice *horizontale* (resp. *verticale*) la séparatrice y entrant et en sortant horizontalement (resp. verticalement).

Notation. Pour un hexagone h, on note $\Sigma_m(h)$ (resp. $\Sigma_v(h)$, resp. $\Sigma_h(H)$) la séparatrice médiane (resp. verticale, resp. horizontale) de h. Pour un carré c, on note $\Sigma_h(c)$ (resp. $\Sigma_v(c)$) la séparatrice horizontale (resp. verticale) de c. Soit $\mathcal{D}$ un diagramme de retournement. Pour tous i, j, k, on note $\mathrm{H}_{ij,k}(\mathcal{D})$, ou simplement $\mathrm{H}_{ij,k}$, l'ensemble des hexagones de $\mathcal{D}$ dont la séparatrice médiane est $\Sigma_{i,j}$ et dont les deux autres séparatrices sont $\Sigma_{i,k}$ et $\Sigma_{j,k}$. On pose $\mathrm{H}^1_{ij,k} = \{H; H \in \mathrm{H}_{ij,k}, \Sigma_v(H) = \Sigma_{i,k}\}$ et $\mathrm{H}^2_{ij,k} = \{H; H \in \mathrm{H}_{ij,k}, \Sigma_v(H) = \Sigma_{j,k}\}$. On note H_{ijk} la réunion $\mathrm{H}_{ij,k} \cup \mathrm{H}_{ik,j} \cup \mathrm{H}_{jk,i}$. On note $\mathrm{Pol}(\mathcal{D})$ l'ensemble des polygones de $\mathcal{D}$.

Dans ce formalisme, on a le lemme suivant :

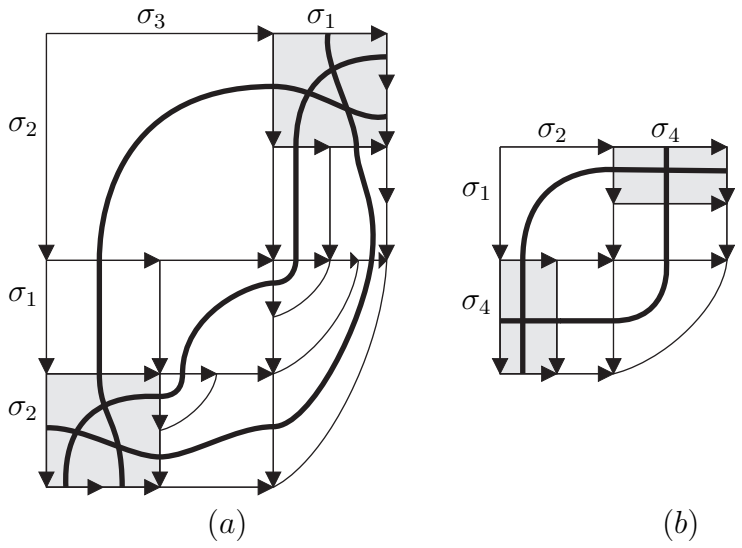


FIGURE 7 – Dans le schéma (a), le diagramme de retournement de $(\sigma_2\sigma_1\sigma_2)^{-1}\sigma_3\sigma_1$ montre qu'un diagramme de retournement peut comporter deux hexagones portant le même nom, c'est-à-dire deux hexagones dans lesquels les trois mêmes séparatrices se croisent. Les trois séparatrices (en trait gras) se rencontrent dans les deux hexagones grisés. Le schéma (b) illustre une répétition de carrés (en grisé).

Lemme 5.7. *Soit $\mathcal{D}$ un diagramme de retournement. Pour tous i, j, k distincts, on a*

$$\mathrm{H}_{ij,k} \neq \emptyset \implies \mathrm{H}_{ik,j} \cup \mathrm{H}_{jk,i} = \emptyset.$$

Démonstration. Supposons qu'il existe un hexagone h de $\mathcal{D}$ nommé $\{i, j, k\}$ tel qu'on ait $\Sigma_m(h) = \Sigma_{i,j}$, c'est-à-dire un hexagone de $\mathrm{H}_{ij,k}(\mathcal{D})$. Par l'argument de la proposition IV.4.5, si $\mathcal{D}$ contient un autre hexagone nommé $\{i, j, k\}$, alors ce dernier est dans $\mathrm{H}_{ij,k}$. □

Définition 5.8. On dit qu'un carré c (resp. un hexagone h) est *sur une séparatrice* $\Sigma_{i,j}$, si $\Sigma_{i,j}$ est la séparatrice verticale ou horizontale de c (resp. verticale, horizontale ou médiane de h). Réciproquement, on dit que $\Sigma_{i,j}$ *est une séparatrice* de c (resp. de h) si c (resp. h) est sur $\Sigma_{i,j}$.

Notation. On ordonne l'ensemble $\mathrm{Pol}_{i,j}$ des polygones sur une séparatrice $\Sigma_{i,j}$ par $<$ en posant $p_1 < p_2$, pour deux polygones de $\mathrm{Pol}_{i,j}$, si et seulement si p_1 apparaît sur la séparatrice $\Sigma_{i,j}$ avant p_2 lorsqu'on parcourt $\Sigma_{i,j}$ depuis le bord inférieur gauche du diagramme vers le bord supérieur droit. On étend classiquement cet ordre strict en un ordre large, qu'on notera $\leq$. Par exemple, dans la figure 9, on a $h_1 < h_2$.

Définition 5.9 (intervalle)**.** Soit $\mathcal{D}$ un diagramme de retournement. Soient p_1 et p_2 deux polygones de $\mathcal{D}$ vérifiant $p_1 < p_2$. On appelle *chaîne entre* p_1 *et* p_2 toute suite de polygones $q_0, \ldots, q_r$ vérifiant $q_0 = p_1$, $q_r = p_2$ et $q_j < q_{j+1}$, pour $0 \leq j \leq r-1$. On appelle *intervalle entre* p_1 *et* p_2 un des ensembles suivants :

- $[p_1, p_2] = \{p \in \mathrm{Pol}(\mathcal{D}); p \text{ est dans une chaîne entre } p_1 \text{ et } p_2\}$;
- $]p_1, p_2] = \{p \in \mathrm{Pol}(\mathcal{D})\backslash\{p_1\}; p \text{ est dans une chaîne entre } p_1 \text{ et } p_2\}$;
- $[p_1, p_2[= \{p \in \mathrm{Pol}(\mathcal{D})\backslash\{p_2\}; p \text{ est dans une chaîne entre } p_1 \text{ et } p_2\}$;
- $]p_1, p_2[= \{p \in \mathrm{Pol}(\mathcal{D})\backslash\{p_1, p_2\}; p \text{ est dans une chaîne entre } p_1 \text{ et } p_2\}$.

Définition 5.10 (hexagones consécutifs)**.** Deux hexagones h_1 et h_2 de $\mathrm{H}_{ij,k}$ sont *consécutifs* si l'ensemble $]h_1, h_2[\cap \mathrm{H}_{ij,k}$ est vide.

Définition 5.11 (courbe d'ordre)**.** On appelle *courbe d'ordre* d'un diagramme de retournement toute courbe passant par les coins supérieur gauche et inférieur droit du diagramme et qui ne traverse un segment que de gauche à droite ou de haut en bas.

Définition 5.12 (ordre, ordre local)**.** Soient p_1, p_2 deux polygones sur une séparatrice Σ'', avec $p_1 < p_2$. On ordonne les séparatrices Σ et Σ' sur l'intervalle $[p_1, p_2]$ en posant $\Sigma < \Sigma'$ (resp. $\Sigma <^* \Sigma'$) si toute (resp. au moins une) courbe d'ordre passant par le morceau de Σ'' entre p_1 et p_2 croise Σ avant Σ'. On dit alors que Σ est *inférieure* (resp. *localement inférieure*) à Σ'. Symétriquement, on dit que Σ' est *supérieure* (resp. *localement supérieure*) à Σ.

Notation. Si deux séparatrices Σ et Σ' se croisent (resp. ne se croisent pas) dans un polygone p, on dit qu'en p, on a $\Sigma = \Sigma'$ (resp. $\Sigma \neq \Sigma'$).

Définition 5.13 (voisinages inférieur, supérieur)**.** (Figure 8) Un *voisinage inférieur* (resp. *supérieur*) d'un polygone p est un ouvert V de $\mathbb{R}^2$, disjoint de p, dont la réunion avec p est convexe, qui ne contient aucun croisement des séparatrices de p, dont l'intersection avec chacune des séparatrices de p est non vide, et dont l'intersection avec les droites passant par les bords supérieur et droit (resp. inférieur et gauche) est vide.

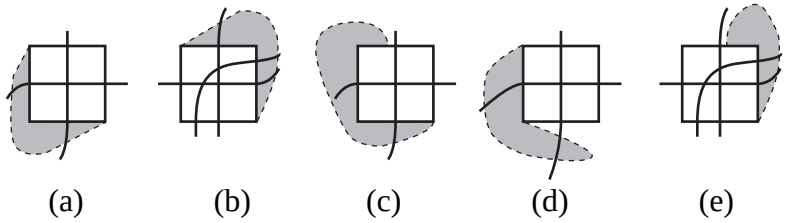


FIGURE 8 – Les parties grisées ne sont pas toutes des voisinages des polygones. Seuls les schémas (a) et (b) représentent un voisinage. Le premier est un voisinage inférieur et le second un voisinage supérieur. Le schéma (c) ne représente pas un voisinage car l'intersection avec la droite portée par le bord supérieur est non vide. Dans le schéma (d), il manque la convexité. Dans le schéma (e), toutes les séparatrices de l'hexagone ne sont pas dans la partie grisée.

Les hexagones jouent un rôle particulier vis-à-vis de leurs séparatrices médianes puisqu'ils en modifient l'orientation. On atteste de ce rôle par la définition suivante :

Définition 5.14 (hexagone réorienteur)**.** Soit la séparatrice Σ. L'hexagone h est un *hexagone réorienteur de* Σ si Σ est la séparatrice médiane de h.

5.3 CONSTRUCTION DES MOTIFS RÉPÉTITEURS

Pour toute cette section, on travaille dans un même diagramme de retournement $\mathcal{D}$ et on suppose qu'il existe deux hexagones de même nom $\{i, j, k\}$. Soient deux hexagones consécutifs h_1 et h_2 de $\mathrm{H}_{ij,k}$ vérifiant $h_1 < h_2$. Posons $\Sigma_v(h_1) = \Sigma_{j,k}$. Nous construisons dans la suite de cette section les différents diagrammes qu'induit la répétition du croisement des séparatrices $\Sigma_{i,j}$, $\Sigma_{i,k}$ et $\Sigma_{j,k}$.

De $\Sigma_v(h_1) = \Sigma_h(h_2)$ on tire qu'il existe m pour lequel $\mathrm{H}_{jk,m}$ est non vide. Posons $h_3 = \max(\mathrm{H}_{jk,m} \cap [h_1, h_2])$. Cette définition de h_3 a un sens puisque le retournement des mots de tresses étant convergent, le nombre d'étapes de retournement est fini. De plus, on suppose

$$\Sigma_h(h_3) = \Sigma_{j,m}. \tag{3}$$

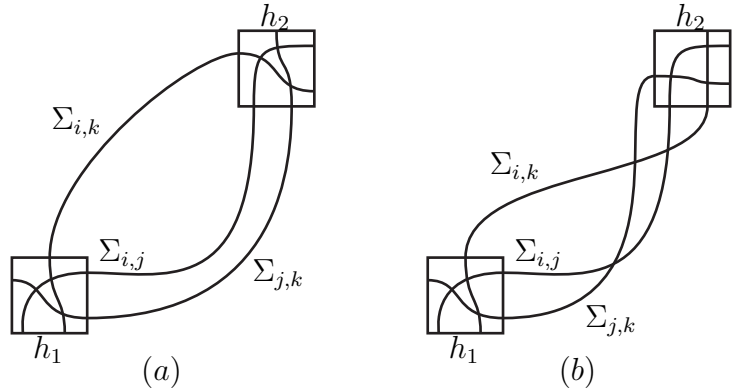


FIGURE 9 – Deux fragments extraits de diagrammes de retournement dans lesquels on ne fait figurer que certains éléments : deux hexagones consécutifs et les séparatrices les reliant. Les polygones représentent des hexagones. Les tracés courbes représentent des séparatrices. Les hexagones h_1 et h_2 sont deux hexagones consécutifs de $\mathrm{H}_{ij,k}$. D'après le lemme 5.7, seul le schéma (a) peut être issu d'un diagramme de retournement. En effet, dans le schéma (b), l'hypothèse que les deux hexagones sont consécutifs impose aux séparatrices de se croiser autour d'une autre séparatrice que $\Sigma_{i,j}$.

Lemme 5.15. *Soient deux séparatrices Σ, Σ' et deux polygones p_1, p_2. Si la séparatrice Σ est localement inférieure et localement supérieure à Σ' sur $[p_1, p_2]$ alors il existe un polygone p_3 duquel Σ et Σ' sont des séparatrices.*

Démonstration. La distance entre les deux séparatrices Σ et Σ' est une fonction continue prenant des valeurs négatives et positives sur $[p_1, p_2]$. Par suite du théorème des valeurs intermédiaires, il existe un polygone p_3 à l'intérieur duquel Σ et Σ' se croisent. □

Lemme 5.16 (lemme du passage)**.** *Soient trois séparatrices Σ, Σ' et Σ'' et deux polygones p_1 et p_2. On suppose que sur $[p_1, p_2[$ on a $\Sigma' < \Sigma$, $\Sigma <^* \Sigma''$ et $\Sigma' < \Sigma''$. On suppose de plus qu'en p_2 on a $\Sigma' = \Sigma''$ et $\Sigma \neq \Sigma''$. Alors il existe un polygone p_3 de $]p_1, p_2[$ tel que*

(i) en p_3 on a $\Sigma = \Sigma''$, et
(ii) sur $[p_1, p_3[$ on a $\Sigma < \Sigma''$.

Démonstration. Supposons que sur $[p_1, p_2[$ on a $\Sigma < \Sigma''$. Comme en p_2 on a $\Sigma' = \Sigma''$, on a également $\Sigma = \Sigma''$ ce qui n'est pas possible. La séparatrice Σ est localement supérieure à Σ''. Sur $[p_1, p_2[$, on a ainsi $\Sigma <^* \Sigma''$ et $\Sigma'' <^* \Sigma$. D'après le lemme 5.15, il existe un polygone p_3 dont les séparatrices sont Σ et Σ'', ce qui montre (i). Parmi les polygones p_3 qui conviennent, on choisit le premier (dans le sens du parcours de Σ) pour lequel, dans un voi-

sinage inférieur, on ait $\Sigma <^* \Sigma''$. Donc sur $[p_1, p_3[$, la séparatrice Σ est partout localement inférieure à Σ'', ce qui donne le point (ii). □

Lemme 5.17. *L'ensemble* $\mathrm{H}_{ij,m} \cap [h_3, h_2]$ *est non vide.*

Démonstration. La situation est celle de la figure 10. Comme h_3 est le dernier hexagone réorienteur de la séparatrice $\Sigma_{j,k}$ avant h_2, sur l'intervalle $[h_3, h_2]$, on a $\Sigma_{j,m} > \Sigma_{j,k}$. De plus, de $h_3 \in [h_1, h_2]$ et de $h_3 \in \mathrm{H}_{jk,m}$, on déduit que $\Sigma_h(h_3)$ est localement inférieure à $\Sigma_{i,j}$. D'après le lemme 5.16, on déduit que la séparatrice $\Sigma_h(h_3)$ croise la séparatrice $\Sigma_{i,j}$ avant h_2. Comme on a posé $\Sigma_h(h_3) = \Sigma_{j,m}$, on en déduit que la séparatrice $\Sigma_{j,m}$ croise la séparatrice $\Sigma_{i,j}$ dans un hexagone avant h_2. Posons $h_4 = \min(\mathrm{H}_{ijm} \cap [h_2, h_3])$. D'après le lemme 5.16, l'hexagone h_4 appartient à l'un des trois ensembles suivants : $\mathrm{H}^1_{im,j}$, $\mathrm{H}^1_{jm,i}$ ou $\mathrm{H}^1_{ij,m}$.

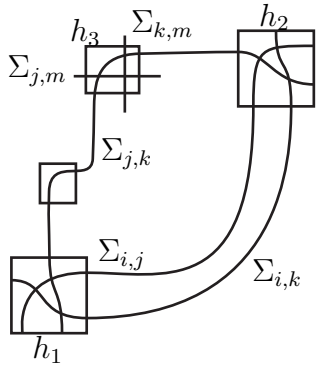


FIGURE 10 – (Lemme 5.17) Des hexagones consécutifs h_1 et h_2 on déduit l'existence de l'hexagone h_3.

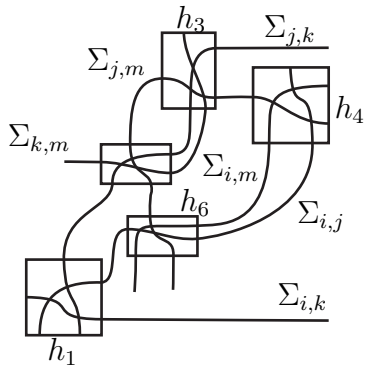


FIGURE 11 – (Lemme 5.17, cas $h_4 \in \mathrm{H}^1_{im,j}$). On montre en supposant le contraire que l'ensemble $\mathrm{H}_{ikm} \cap [h_1, h_4]$ est vide.

• Cas $h_4 \in \mathrm{H}^1_{im,j}$: (Fig. 11) Supposons que l'ensemble $\mathrm{H}_{ikm} \cap [h_1, h_4]$ n'est pas vide et notons h_5 son plus petit élément. La séparatrice $\Sigma_{i,m}$ est localement inférieure à $\Sigma_{i,j}$ au voisinage inférieur de h_4 et sur $[h_1, h_4]$ on a $\Sigma_{i,j} < \Sigma_{i,k}$. De plus, on a $\Sigma_{i,k} = \Sigma_{i,m}$ en h_5, donc sur $[h_1, h_4]$, la séparatrice $\Sigma_{i,m}$ est localement supérieure à la séparatrice $\Sigma_{i,j}$. Du lemme 5.15, on déduit que l'ensemble $\mathrm{H}_{im,j} \cap [h_1, h_4[$ n'est pas vide et on note h_6 son plus petit élément. D'après l'hypothèse $\mathrm{H}_{ikm} \cap [h_1, h_4] \neq \emptyset$, l'hexagone h_6 est dans $\mathrm{H}^2_{im,j}$. Sur $[h_6, h_5]$ on a donc $\Sigma_{i,j} < \Sigma_{i,m} < \Sigma_{j,m}$. Or on a également $\Sigma_{j,k} < \Sigma_{i,j}$. On en déduit $\Sigma_{j,k} < \Sigma_{j,m}$, puis $\Sigma_{k,m} < \Sigma_{j,k}$ donc $\Sigma_{k,m} < \Sigma_{i,j}$ et enfin $\Sigma_{k,m} < \Sigma_{i,k}$. Cette dernière inégalité contredit l'existence de h_5 puisqu'en h_5 on a $\Sigma_{k,m} = \Sigma_{i,k}$.

Du paragraphe précédent, on déduit que l'ensemble $\mathrm{H}_{jk,m} \cap [h_1, h_3[$ n'est pas vide et que son plus petit élément, disons l'hexagone h_7, est dans $\mathrm{H}^1_{jk,m}$. Par conséquent, l'ensemble $\mathrm{H}_{im,j} \cap [h_1, h_7]$ est non vide et son plus petit élément, l'hexagone h_8, est dans $\mathrm{H}^2_{im,j}$.

Mais ceci implique sur $[h_1, h_8]$ qu'on a $\Sigma_{j,m} > \Sigma_{i,m} > \Sigma_{i,j}$, et par suite que $\mathrm{H}_{ikm} \cap [h_1, h_8]$ est non vide. On a prouvé plus haut dans ce point que ce n'était pas possible.

• Cas $h_4 \in \mathrm{H}^1_{jm,i}$: (Fig. 12) Sur $[h_3, h_4[$, on a $\Sigma_{i,m} < \Sigma_{j,m}$ mais on a également $\Sigma_{j,k} < \Sigma_{i,m}$. Or, en h_3 on a $\Sigma_{j,m} = \Sigma_{j,k}$, donc du lemme du passage 5.16 on déduit que $\mathrm{H}_{jm,i} \cap [h_3, h_4[$ est non vide, ce qui contredit la minimalité de h_4.

• Cas $h_4 \in \mathrm{H}^1_{ij,m}$: (Fig. 13) On sait que $\mathrm{H}_{ijm} \cap [h_3, h_2]$ est non vide et on a montré que sur $[h_3, h_2]$ les ensembles $\mathrm{H}_{im,j}$ et $\mathrm{H}_{jm,i}$ étaient vides. On a donc sur $[h_3, h_2]$ l'égalité $\mathrm{H}_{ijm} = \mathrm{H}_{ij,m}$ et donc $\mathrm{H}_{ij,m} \cap [h_3, h_2]$ est non vide. □

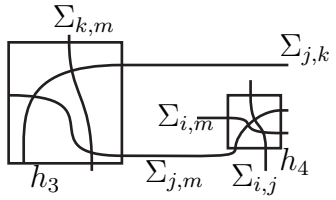


FIGURE 12 – (Lemme 5.17, cas $h_4 \in \mathrm{H}^1_{jm,i}$) La séparatrice $\Sigma_{i,m}$ est contrainte de croiser la séparatrice $\Sigma_{j,m}$ sur l'intervalle $[h_3, h_4[$, contredisant la définition de h_4.

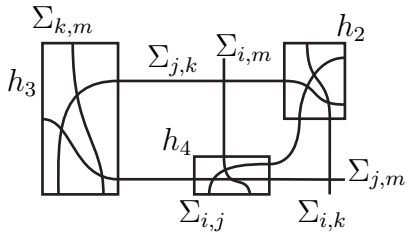


FIGURE 13 – (Lemme 5.17, cas $h_4 \in \mathrm{H}^1_{ij,m}$ et lemme 5.18) L'hexagone h_4 ne peut qu'appartenir à $\mathrm{H}^1_{ij,m}$. Dans les autres cas, on obtient des contradictions. Ici, on a illustré le cas $h_4 = h_9$.

Nous poursuivons la construction des motifs répétiteurs avec le lemme suivant, qui prouve a posteriori le choix de dessiner les séparatrices $\Sigma_{i,m}$ et $\Sigma_{j,m}$ dans cette configuration à la figure 13.

Notation. Pour tous entiers positifs p, q, p', q', on note $\mathrm{C}_{pq,p'q'}$ l'ensemble des carrés de $\mathcal{D}$ nommés $\{\{p, q\}, \{p', q'\}\}$. On note $\mathrm{C}^1_{pq,p'q'}$ (resp. $\mathrm{C}^2_{pq,p'q'}$) le sous-ensemble des carrés c de $\mathrm{C}_{pq,p'q'}$ vérifiant $\Sigma_v(c) = \Sigma_{p,q}$ (resp. $\Sigma_v(c) = \Sigma_{p',q'}$).

Lemme 5.18. *Les ensembles* $\mathrm{C}_{jk,im} \cap [h_4, h_2]$ *et* $\mathrm{C}_{ik,jm} \cap [h_4, h_2]$ *sont non vides.*

Démonstration. Posons $h_9 = \max(\mathrm{H}_{ij,m} \cap [h_4, h_2])$. Supposons que l'hexagone h_9 soit élément de $\mathrm{H}^2_{ij,m}$. L'hexagone h_2 est dans $\mathrm{H}^1_{ij,k}$ donc, sur $[h_1, h_2]$, on a $\Sigma_{i,j} < \Sigma_{j,k}$ et donc, dans le voisinage supérieur de h_9, on a $\Sigma_{j,k} < \Sigma_{j,m} < \Sigma_{i,j}$. Par le lemme du passage 5.16, l'ensemble $(\mathrm{H}_{jk,m} \cup \mathrm{H}_{ij,m}) \cap]h_9, h_2[$ est non vide. Or par définition de h_9, l'ensemble $\mathrm{H}_{ij,m} \cap]h_9, h_2[$. On en déduit que l'ensemble $\mathrm{H}_{jk,m} \cap]h_9, h_2[$, ce qui contredit la définition de l'hexagone h_3. Donc on obtient une contradiction. On conclut que h_9 est un élément de $\mathrm{H}^1_{ij,m}$ et on prouve l'énoncé après deux emplois du lemme du passage. □

Remarque 5.19. Dans la voisinage inférieur de l'hexagone h_4 on a $\Sigma_{j,k} < \Sigma_{i,m} < \Sigma_{i,k}$ et du lemme du passage on déduit que l'ensemble $(\mathrm{C}^1_{im,jk} \cup \mathrm{H}_{ikm}) \cap [h_1, h_4]$ est non vide. Notons p_{10} son élément le plus petit.

Lemme 5.20. *On a*

$$p_{10} \in \mathrm{C}^1_{im,jk} \implies \min\left(\mathrm{C}_{ik,jm} \cap [h_1, h_4]\right) \in \mathrm{C}^1_{ik,jm}.$$

Démonstration. Posons $c_{10} = p_{10}$. De $c_{10} \in \mathrm{C}^1_{im,jk}$, on tire que la séparatrice $\Sigma_{i,m}$ est localement inférieure et localement supérieure à $\Sigma_{i,j}$ sur $[h_1, h_4]$ donc, d'après le lemme 5.15, l'ensemble $\mathrm{H}_{ij,m} \cap [h_1, h_4[$ est non vide. De plus, en notant h_{11} son plus petit élément, on a $h_{11} \in \mathrm{H}^2_{ij,m}$. On en déduit que la séparatrice $\Sigma_{j,m}$ vérifie localement l'encadrement $\Sigma_{i,j} < \Sigma_{j,m} < \Sigma_{i,k}$. On conclut par minimalité de h_{11} et par application du lemme du passage. □

On étudie l'autre possibilité dans le lemme suivant.

Lemme 5.21. *On a*

$$p_{10} \in \mathrm{H}_{ikm} \implies p_{10} \in \mathrm{H}^2_{im,k}.$$

Démonstration. Posons $h_{10} = p_{10}$. L'hexagone h_{10} est sur la séparatrice $\Sigma_{k,m}$. Or, dans le voisinage inférieur de h_4, on a $\Sigma_{k,m} < \Sigma_{i,m} < \Sigma_{i,k}$. De cet encadrement, on déduit $h_{10} \in \mathrm{H}_{im,k}$. Supposons $h_{10} \in \mathrm{H}^1_{im,k}$. On a l'inégalité $\Sigma_{i,m} < \Sigma_{i,k}$ sur $[h_1, h_{10}]$. Donc localement sur $[h_1, h_{10}]$, la séparatrice $\Sigma_{i,m}$ est comprise entre $\Sigma_{i,k}$ et $\Sigma_{j,k}$. Puisqu'en h_1 on a $\Sigma_{i,k} = \Sigma_{j,k}$, par le lemme du passage, on obtient que $(\mathrm{C}_{jk,im} \cup \mathrm{H}_{ikm}) \cap [h_1, h_{10}[$ est non vide, ce qui contredit la minimalité de p_{10}. □

6 MAJORATION DE LA 2-COMPLEXITÉ : MOTIFS RÉPÉTITEURS

6.1 DÉFINITION DES MOTIFS RÉPÉTITEURS

En reprenant les notations de la section 5.3, on définit trois types de sous-diagrammes d'un diagramme de retournement, dont la présence signifie qu'il y a une répétition d'hexagones. Du lemme 5.20 on tire la définition suivante.

Définition 6.1 (motif répétiteur A)**.** Pour $l \in \{1, 2\}$, on appelle *motif répétiteur de type* $\mathrm{A}^l_{ij,k}(m)$ deux hexagones consécutifs h_1 et h_2 de $\mathrm{H}_{ij,k}$ satisfaisant

- $h_1 < h_2$,
- $h_1 \in \mathrm{H}^l_{ij,k}$,
- h_3 est un hexagone de $\mathrm{H}_{\Sigma_v(h_1),m}$,
- p_{10} est un carré.

Avec le résultat du lemme 5.21, on définit un autre type de motif répétiteur.

Définition 6.2 (motif répétiteur B)**.** Pour $l \in \{1, 2\}$, on appelle *motif répétiteur de type* $\mathrm{B}^l_{ij,k}(m)$ deux hexagones consécutifs h_1 et h_2 de $\mathrm{H}_{ij,k}$ satisfaisant

- $h_1 < h_2$,
- $h_1 \in \mathrm{H}^l_{ij,k}$,
- h_3 est un hexagone de $\mathrm{H}^1_{\Sigma_v(h_1),m}$,
- p_{10} est un hexagone.

Remarque 6.3. Dans la définition du motif répétiteur de type B, le fait que h_3 soit un hexagone de $\mathrm{H}^1_{\Sigma_v(h_1),m}$ provient de l'hypothèse (3). Remplacer cette hypothèse par l'hypothèse symétrique $h_3 \in \mathrm{H}^2_{\Sigma_v(h_1),m}$ mène à la définition d'un nouveau motif.

Définition 6.4 (motif répétiteur $\overline{\mathrm{B}}$)**.** Pour $l \in \{1, 2\}$, on appelle *motif répétiteur de type* $\overline{\mathrm{B}}^l_{ij,k}(m)$ deux hexagones consécutifs h_1 et h_2 de $\mathrm{H}_{ij,k}$ satisfaisant

- $h_1 < h_2$,
- $h_1 \in \mathrm{H}^l_{ij,k}$,
- h_3 est un hexagone de $\mathrm{H}^2_{\Sigma_v(h_1),m}$,
- p_{10} est un hexagone.

Définition 6.5. On dit d'un motif répétiteur $\mathfrak{m}$ qu'il *est sur* i, j, k, m s'il existe X parmi A, B et $\overline{\mathrm{B}}$ et l dans $\{1, 2\}$ tels que $\mathfrak{m}$ soit un motif de type $\mathrm{X}^l_{ij,k}(m)$.

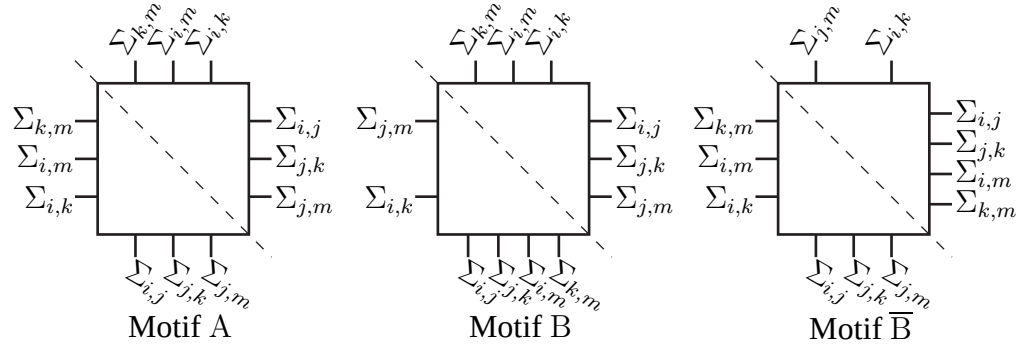


FIGURE 14 – Chacun des trois motifs répétiteurs est schématisé en ne tenant compte que des positions relatives des séparatrices et de leurs orientations. Un motif de type A est symétrique par rapport à l'axe diagonal NO/SE. Les motifs de type B et $\overline{\mathrm{B}}$ sont images les uns des autres par cette symétrie.

On conclut en énonçant la proposition résumant les lemmes 5.17, 5.18, 5.20 et 5.21 et exprimant le fait qu'une répétition d'hexagones donne nécessairement lieu à un motif répétiteur.

Proposition 6.6. *Soit $\mathcal{D}$ un diagramme de retournement. Supposons que deux hexagones de $\mathcal{D}$ portent le même nom $\{i, j, k\}$. Alors il existe un entier m distinct de i, j, k tel que $\mathcal{D}$ admette un motif répétiteur sur i, j, k, m.*

6.2 BORNES SUPÉRIEURES

Le but de cette section est de montrer que, moyennant une conjecture sur les diagrammes de retournement, la borne supérieure naturelle pour la 2-complexité des mots $u^{-1}v$, avec u, v des mots simples, est quartique en la longueur de $u^{-1}v$.

Notation. Soient u, v des mots positifs. On note $h(u^{-1}v)$ (resp. $c(u^{-1}v)$, resp. $d(u^{-1}v)$) le nombre d'hexagones (resp. de carrés, resp. de digones) dans le diagramme de retournement de $u^{-1}v$.

Lemme 6.7. *Soient u, v deux mots simples vérifiant $|u^{-1}v| = \ell$. On a alors*

$$h(u^{-1}v) \in O(\ell^2 + d(u^{-1}v)).$$

Démonstration. Soit $w_0, \ldots, w_p$ une suite de retournement maximale issue de $u^{-1}v$. Le retournement d'un sous-mot $\sigma_i^{-1}\sigma_j$, pour $|j - i| = 1$, dans le mot w_m implique $|w_{m+1}| - |w_m| = 2$. De façon analogue, le retournement d'un sous-mot $\sigma_i^{-1}\sigma_i$ dans un mot w_m implique $|w_{m+1}| - |w_m| = -2$. Finalement, le retournement d'un sous-mot $\sigma_i^{-1}\sigma_j$, avec $|i - j| > 1$, dans un mot w_m implique $|w_{m+1}| - |w_m| = 0$. Autrement dit, un hexagone du diagramme contribue $+2$ à la longueur de w_p, un digone contribue -2 et un carré contribue 0. On a donc $2|h(w_0) - d(w_0)| = ||w_0| - |w_p||$. Le mot terminal w_p s'écrit comme le produit $v'u'^{-1}$, avec u' et v' deux mots simples puisque u et v sont simples. On en déduit, d'après le lemme 3.10, que les longueurs $|u'|$ et $|v'|$ sont inférieures à $\ell(2\ell - 1)$ donc dans $O(\ell^2)$. □

Le lemme précédent établit que dans un diagramme de retournement d'un mot négatif-positif les nombres de digones et d'hexagones ne diffèrent que d'une quantité quadratique en la longueur du bord supérieur gauche. On relie maintenant le nombre de carrés au nombre de digones.

Lemme 6.8. *Soient u, v deux mots simples vérifiant $|u^{-1}v| = \ell$. On a alors*

$$c(u^{-1}v) \in O(\ell^4 + h(u^{-1}v)).$$

Remarque 6.9. Contrairement à la preuve du lemme 6.7, on ne peut pas compter le nombre de carrés dans un diagrammes en mesurant la différence de longueur entre le mot initial et le mot final puisque le carré ne modifie pas la longueur des mots qui le bordent ; autrement dit, appliquer une relation de commutation à un mot ne modifie pas sa longueur.

Démonstration. D'après la section 3, on peut considérer sans perte de généralité, que la largeur de $u^{-1}v$ est inférieure à 2ℓ. Donc le nombre de noms de carrés est dans $O(\ell^4)$. Enfin, chaque répétition de carrés nécessite un hexagone — et un digone (figure 7 (b)). □

Lemme 6.10. *Soient u et v deux mots simples vérifiant $|u^{-1}v| = \ell$. On a*

$$\mathrm{L}_2(u^{-1}v) = O(\ell^4 + h(u^{-1}v)).$$

Démonstration. D'après les lemmes 6.7 et 6.8, on a

$$\begin{aligned}\mathrm{L}_2(u^{-1}v) &= c(u^{-1}v) + d(u^{-1}v) + h(u^{-1}v)\\ &= O(\ell^4 + h(u^{-1}v)) + O(h(u^{-1}v) + \ell^2) + h(u^{-1}v)\\ &= O(\ell^4 + h(u^{-1}v)).\end{aligned}$$

□

On établit maintenant des bornes supérieures pour la 2-complexité.

Proposition 6.11. *Soient u, v deux mots simples vérifiant $|u^{-1}v| = \ell$ et soit $\mathcal{D}$ le diagramme de retournement de $u^{-1}v$. Supposons que $\mathcal{D}$ contienne $O(\ell^4)$ motifs répétiteurs, alors on a*

$$\mathrm{L}_2(u^{-1}v) \in O(\ell^4).$$

La preuve est immédiate.

Démonstration. Le nombre de noms d'hexagones est dans $O(\ell^3)$, donc, en tenant compte des motifs répétiteurs, il y a au plus $O(\ell^4)$ hexagones. On applique ensuite le lemme 6.10. □

En réalité, on ne connaît pas de diagramme de retournement contenant plus de $O(\ell^4)$ motifs répétiteurs. On conjecture :

Conjecture 6.12. *Un diagramme de retournement ne contient au plus qu'un seul motif répétiteur pour chaque type et chaque valeur des paramètres.*

En supposant cette conjecture vraie, de la proposition 6.11 on obtient immédiatement :

Proposition 6.13. *Supposons la conjecture 6.12 vraie. Soient u, v deux mots de tresse simples (resp. quelconques) vérifiant $|u^{-1}v| = \ell$ et soit $\mathcal{D}$ le diagramme de retournement de $u^{-1}v$. Alors on a*

$$\mathrm{L}_2(u^{-1}v) \in O(\ell^4) \quad (\textit{resp.}\ \mathrm{L}_2(u^{-1}v) \in O(\ell^6)).$$

Démonstration. En supposant la conjecture 6.12 vraie, le nombre de motifs répétiteurs dans $\mathcal{D}$ est dans $O(\ell^4)$. On conclut grâce à la proposition 6.11. □

La motifs répétiteurs sont des agencements complexes de séparatrices, d'hexagones de carrés et de digones. Leur riche structure donne l'espoir qu'on puisse prouver la conjecture 6.12 simplement en montrant que la coexistence de trop de motifs est impossible.

BIBLIOGRAPHIE

[1] E. Artin. Theory of braids. *Ann. Math.*, 48 :101–126, 1947.

[2] M. Autord. Comparing Gröbner bases and word reversing. *European-Asian Journal of Mathematics*, to appear.

[3] M. Autord and P. Dehornoy. On the combinatorial distance between the expressions of a permutation. *http ://arxiv.org/abs/0902.3074v1*. Submitted for publication.

[4] J. Birman, K.H. Ko, and S.J. Lee. A new approach to the word problem in the braid groups. *Adv. Math.*, 139(2) :322–353, 1998.

[5] L.A. Bokut, Y. Fong, W.-F. Ke, and L.-S. Shiao. Gröbner-Shirshov bases for the braid semigroup. In *Advances in algebra*, pages 60–72. World Sci. Publ., 2003.

[6] L.A. Bokut and P.S. Kolesnikov. Gröbner-Shirshov bases : from their incipiency to the present. *J. Math. Sc.*, 116(1) :2894–2916, 2003. (Translated from Russian).

[7] N. Brady, T. Riley, and H. Short. *The geometry of the word problem for finitely generated groups.* Advanced Courses in Mathematics - Birkhäuser. , 2007.

[8] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Innsbruck, 1965.

[9] A.H. Clifford and G.B. Preston. *The algebraic theory of semigroups. Vol. I.* Mathematical Surveys. 7. Providence, R.I. : American Mathematical Society (AMS). XV, 224 p. , 1961.

[10] R. Corran. A normal form for a class of monoids including the singular braid monoids. *J. Algebra*, 223 :256–282, 2000.

[11] P. Dehornoy. Deux propriétés des groupes de tresses. *C.R. Acad. Sci. Paris*, 315 :633–638, 1992.

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

[13] P. Dehornoy. *Braids and Self-Distributivity*, volume 192 of *Progr. Math.* Birkhäuser, 2000.

[14] P. Dehornoy. On completeness of word reversing. *Discrete Math.*, 225 :93–119, 2000.

[15] P. Dehornoy. Groupes de Garside. *Ann. Sci. École Norm. Sup. Paris*, 35 :267–306, 2002.

[16] P. Dehornoy. Complete positive group presentations. *J. Algebra*, 268 :156–197, 2003.

[17] P. Dehornoy and B. Wiest. On word reversing in braid groups. *Int. J. Algebra Comput.*, 16(5) :941–957, 2006.

[18] Ed. Green, T. Mora, and V. Ufnarovski. The non-commutative Gröbner freaks. In M. et al. Bronstein, editor, *Symbolic rewriting techniques*, volume 15 of *Prog. Comput. Sci. Appl. Log.*, pages 93–104. Birkäuser Verlag, 1998.

[19] H. Hermiller and J. Meier. Artin groups, rewriting systems and three-manifolds. *J. Pure Appl. Algebra*, 136 :141–156, 1999.

[20] A. Heyworth. Rewriting as a special case of Gröbner basis theory. In M. Atkinson, N. Gilbert, J. Howie, S. Linton, and E. Robertson, editors, *Computational and Geometric Aspects of Modern Algebra*, volume 275 of *Lecture Note Series*, pages 101–105. London Math. Soc., 2000.

[21] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II. *Ann. Math.*, 79 :109–203, 205–326, 1964.

[22] F. Mora. Gröbner bases for non-commutative polynomial rings. In Springer, editor, *Proc. AAECC 3*, volume 229 of *Lect. Notes Comput. Sci.*, pages 353–362, 1986. Zbl 0659.16003.

[23] M. Picantin. *Petits groupes gaussiens*. PhD thesis, Université de Caen, 2000.

[24] B. Reinert. Tutorial on Gröbner bases in monoid and group rings. In *Federated Logic Conference '99 Workshop on Gröbner Bases and Rewriting Techniques*, 1999.

[25] A.I. Shirshov. Some algorithmics problems for Lie algebras. *Sib. Math. Zh.*, 3 :292–296, 1962. (In Russian).

[26] K. Tatsuoka. An isoperimetric inequality for Artin groups of finite type. *Trans. Amer. Math. Soc*, 339(2) :537–551, 1993.

[27] V.A. Ufnarovskij. *Combinatorial and Asymptotic Methods in Algebra*, volume 57 of *Encyclopaedia of Mathematical Sciences*, chapter I, pages 1–196. Springer, 1995. Zbl 0826.16001.