



HAL
open science

Un hybride du groupe de Thompson F et du groupe de tresses $B^{\circ\circ}$

Emilie Tesson

► **To cite this version:**

Emilie Tesson. Un hybride du groupe de Thompson F et du groupe de tresses $B^{\circ\circ}$. Théorie des groupes [math.GR]. Normandie Université, 2018. Français. NNT : 2018NORMC212 . tel-01871101

HAL Id: tel-01871101

<https://theses.hal.science/tel-01871101>

Submitted on 10 Sep 2018

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

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



Normandie Université

THESE

Pour obtenir le diplôme de doctorat

Spécialité Mathématiques

Préparée au sein de l'Université de Caen Normandie

Un hybride du groupe de Thompson F et du groupe de tresses B_∞

Présentée et soutenue par
Emilie TESSON

Thèse soutenue publiquement le 02/03/2018
devant le jury composé de

Monsieur Patrick DEHORNOY	Professeur des universités émérite, Université de Caen Normandie	Directeur de thèse
Monsieur François DIGNE	Professeur des universités émérite, Université de Picardie Jules Verne	Rapporteur
Madame Emmanuelle FEAUX DE LACROIX	Maître de conférences, Université de Caen Normandie	Examinateur
Monsieur Matthieu PICANTIN	Maître de conférences, Université Denis- Diderot, Paris 7	Examinateur
Madame Sarah REES	Professeur, Université de Newcastle, Royaume-Uni	Rapporteur

Thèse dirigée par Patrick DEHORNOY, Laboratoire de Mathématiques Nicolas Oresme



Introduction

Principalement, l'objet de cette thèse est l'étude d'un certain monoïde, ici noté H^+ , qui, apparemment, ne figure pas dans la littérature, mais qui apparaît assez naturellement comme hybride du monoïde B_∞^+ des tresses positives et du monoïde de Thompson F^+ . On verra que le monoïde H^+ hérite des propriétés de chacun de ses deux « parents », typiquement des propriétés de tresses pour ce qui concerne la multiplication à gauche, et des propriétés à la Thompson pour ce qui concerne la multiplication à droite. Cette étude se révèle assez délicate, en particulier parce que le monoïde H^+ n'est pas de type fini et ne possède pas toujours des multiples communs, et, indépendamment des résultats spécifiques sur H^+ , on sera amené à établir quelques propriétés générales pour traiter une telle situation.

Le monoïde H^+

Le monoïde H^+ est le monoïde spécifié par la présentation explicite suivante :

$$(\mathcal{P}) \quad H^+ := \left\langle \theta_1, \theta_2, \dots \mid \begin{array}{ll} \theta_j \theta_i = \theta_i \theta_{j+1} & \text{pour } j \geq i + 2 \\ \theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{i+3} & \text{pour } j = i + 1 \end{array} \right\rangle^+.$$

Cette présentation est directement réminiscente de celle du monoïde de tresses infinies

$$B_\infty^+ := \left\langle \sigma_1, \sigma_2, \dots \mid \begin{array}{ll} \sigma_j \sigma_i = \sigma_i \sigma_j & \text{pour } j \geq i + 2 \\ \sigma_j \sigma_i \sigma_j = \sigma_i \sigma_j \sigma_i & \text{pour } j = i + 1 \end{array} \right\rangle^+,$$

et de celle du monoïde de Thompson

$$F^+ := \langle a_1, a_2, \dots \mid a_j a_i = a_i a_{j+1} \text{ pour } j \geq i + 1 \rangle^+.$$

Dans les trois cas, on a des relations de commutation, ou de quasi-commutation, à savoir des relations du type $xy = yx$ ou $xy = yx'$: dans le cas de B_∞^+ , il s'agit de vraie commutation dans le cas des générateurs σ_i d'indices non adjacents, dans le cas de F^+ et de H^+ , c'est une quasi-commutation qui prend la forme « $21 = 13$ » ou « $31 = 14$ ». Noter que les relations de longueur 3 peuvent aussi être vues comme des relations de quasi-commutation : dans le cas de B_∞^+ , on peut lire la relation de longueur 3 comme « $2(12) = (12)1$ », soit une quasi-commutation de 2 et de 12 avec décalage de l'indice de -1 . De même, pour H^+ , on peut lire la relation de longueur 3 comme « $2(12) = (12)4$ » (quasi-commutation de 2 et de 12 avec décalage de l'indice de $+2$).

On peut voir le monoïde de Thompson F^+ comme une version tordue du monoïde abélien libre $\mathbb{N}^{(\infty)}$, qui admet la présentation

$$\langle a_1, a_2, \dots \mid a_j a_i = a_i a_j \text{ pour } i < j \rangle^+,$$

dans laquelle les relations de commutation sont remplacées par des quasi-commutation par décalage +1. De ce point de vue, le monoïde H^+ se trouve exactement dans la même position par rapport au monoïde B_∞^+ , dont il est une version tordue de la même façon. On peut donc résumer la situation sous la forme d'une relation de proportionnalité

$$(E) \quad \boxed{\frac{H^+}{B_\infty^+} = \frac{F^+}{\mathbb{N}^{(\infty)}}.}$$

La comparaison des propriétés des monoïdes $\mathbb{N}^{(\infty)}$, F^+ , et B_∞^+ montre que des variations syntaxiques apparemment mineures dans les relations d'une présentation suffisent à modifier radicalement les propriétés. Il ne faut donc pas trop attendre de l'« égalité (E) » pour déduire les propriétés du monoïde H^+ : on va voir cependant que, pour ce qui est de celles qui ont pu être démontrées ici, elles sont directement réminiscentes de celles des deux monoïdes « cousins » F^+ et B_∞^+ . Plus précisément, on montrera que, pour ce qui concerne la multiplication à gauche, H^+ est réminiscent de B_∞^+ , tandis que, pour ce qui concerne la multiplication à droite, H^+ est davantage réminiscent de F^+ .

Principaux résultats

Les principaux résultats établis dans la suite sont les suivants.

D'abord, on montre l'existence d'un système de réécriture convergent pour la présentation (\mathcal{P}) .

Proposition A. (propositions II.3.11 et II.3.20) *Tout élément a de H^+ possède une unique représentation $\text{NF}(a)$ par un mot sans facteur $\theta_i \theta_j$ avec $j \geq i + 3$ et sans facteur $\theta_i \theta_{i+1} \theta_{i+3}$ (« forme normale de a »); il existe un système de réécriture convergent vers cette forme normale.*

D'autre part, on montre que le monoïde H^+ a de bonnes propriétés de régularité, principalement en ce qui concerne la relation de divisibilité à gauche :

Proposition B. (propositions IV.2.4, IV.2.5, IV.2.6, IV.2.9, et IV.3.11) *Le monoïde H^+ admet la simplification à gauche et à droite. Il admet des pgcd à gauche, et des ppcm à droite conditionnels. L'existence de multiples communs à droite est un problème décidable.*

Par ailleurs, on montre que, pour tout n , les générateurs $\theta_1, \dots, \theta_n$ possèdent un ppcm à droite Δ_n . Appelant *simples* les éléments de H^+ qui divisent à gauche au moins un élément Δ_n , on établit les résultats de type « Garside » suivants :

Proposition C. (propositions V.2.17, V.3.24, et V.4.13) *Il existe $2 \cdot 3^{n-2}$ éléments simples divisant Δ_n . Les formes normales des éléments simples sont celles qui n'ont pas de facteur θ_i^2 , $\theta_i\theta_{i+2}$, $\theta_i\theta_{i+1}\theta_{i+2}$, ni $\theta_i\theta_{i+1}\theta_i$. Tout élément de H^+ admet une unique décomposition gloutonne (« left greedy decomposition ») en produit d'éléments simples.*

Enfin, de diverses observations, négatives et positives, sur les représentations de H^+ dans d'autres monoïdes, on peut extraire le résultat suivant :

Proposition D. (proposition VI.1.40) *Envoyer θ_i sur la matrice (infinie)*

$$\left(\begin{array}{c|cc|c} I_i & 0 & & 0 \\ \hline & t & (1+t)s^{-1} & \\ \hline & (1-t)s & -t & \\ \hline 0 & & 0 & I_\infty \end{array} \right), \text{ où } I_n \text{ est la matrice unité de taille } n, \text{ dé-}$$

fini une représentation linéaire de H^+ . Aucun contre-exemple n'a été trouvé à la fidélité, même en spécialisant à $s = 1$.

Par ailleurs, pour établir les résultats concernant la divisibilité à gauche dans H^+ , en particulier la décidabilité de l'existence de multiples à droite communs, on a dû étendre les résultats connus sur le retournement de facteur. Une version des résultats s'énonce comme suit.

Proposition E. (propositions III.2.8 et III.3.18) *Si (S, R) est une présentation complétée à droite et si S' est un ensemble de S -mots incluant S et clos par R -complément à droite, alors le retournement à droite est complet pour (S, R) si, et seulement si, la condition du cube à droite est satisfaite pour tout triplet de mots de S' , et le R -retournement d'un S -mot signé w termine si, et seulement si, le R' -retournement de w vu comme S' -mot réussit, où R' est l'ensemble des relations $uC(u, v) = vC(v, u)$ pour u, v dans S' .*

Organisation du texte

La thèse est divisée en six chapitres, plus une courte annexe informatique.

Le chapitre I est introductif. On commence par rappeler la notion générale de monoïde présenté, ainsi que la terminologie relative aux relations de divisibilité d'un monoïde, avec les notions dérivées de pgcd, de ppcm, et de noethérianité. Ensuite, on présente les deux monoïdes qui forment le contexte de cette étude, à savoir le monoïde des tresses positives B_∞^+ , tresses à un nombre de brins illimité, et le monoïde de Thompson F^+ , sous-monoïde

positif du groupe de Thompson F . On présente aussi le monoïde \widehat{BV}^+ des tresses parenthésées positives, qui est une extension à la fois de B_∞^+ et de F^+ , dont il est un produit de Zappa–Szep. Ensuite, on introduit le monoïde H^+ , objet de notre étude, et on établit quelques propriétés simples résultant directement de la présentation, notamment la noethérianité, la décidabilité du problème de mots, et on observe que le monoïde de Thompson F^+ est un quotient de H^+ .

Dans le chapitre II, on montre l’existence d’une forme normale sur H^+ obtenue par un système de réécriture simple. Pour cela, après avoir rappelé dans la section II.1 le contexte général des systèmes de réécriture et le critère de convergence basé sur la confluence locale (« diamond lemma »), on commence par traiter dans la section II.2 le cas facile du monoïde de Thompson F^+ , puis on étudie dans la section II.3 le cas de H^+ . On y montre que l’approche utilisée pour F^+ fonctionne pour H^+ , de façon un peu moins directe. Comme applications, on établit la **proposition A** mentionnée plus haut, puis, par un argument original et peut-être intéressant, on déduit un résultat de simplification conditionnel, à savoir que, si H^+ est simplifiable à gauche, alors il est aussi simplifiable à droite.

Le chapitre III est un chapitre général consacré à la méthode du retournement de facteur pour étudier un monoïde présenté, et on y met en place les outils qui permettront d’étudier spécifiquement le monoïde H^+ dans le chapitre suivant. Dans la littérature, la méthode du retournement a été appliquée principalement au cas de monoïdes admettant des ppcm (monoïdes de tresses, et plus généralement d’Artin–Tits sphériques, etc.), ce qui n’est pas le cas du monoïde H^+ : il existe des mots de Θ^* dont le retournement ne termine pas. Nos résultats montrent comment contourner le problème quand on connaît une famille de mots S' incluant S et close par complément au sens où, si u et v sont dans S' et si le retournement de $\bar{u}v$ termine, alors il termine sur un mot de la forme $v'u'$ avec u' et v' encore dans S' . La méthode consiste à passer de l’alphabet initial S à l’alphabet étendu S' , le point-clé étant que le retournement pour S se factorise (en un sens convenable) par le retournement pour S' . Le chapitre est organisée en trois sections. On y rappelle d’abord dans la section III.1 la définition du retournement dans le contexte d’une présentation complétée, ainsi que (sans répéter les démonstrations) les résultats standard sur la reconnaissance de la complétude par la condition dite du cube. Ensuite, on établit des résultats nouveaux, à savoir, dans la section III.2 un nouveau critère de complétude et, dans la section III.3, un nouveau critère de terminaison, valables dans le cas de monoïdes n’admettant pas toujours de multiples communs, et dont la réunion est la **proposition E** ci-dessus.

Dans le chapitre IV, on applique au cas du monoïde H^+ les résultats généraux du chapitre III. On commence par rappeler dans la section IV.1 comment utiliser le retournement, lorsqu’il est complet, pour résoudre le problème de mots et étudier les multiples communs et la divisibilité dans un monoïde présenté, puis on aborde le cas de H^+ . Dans la section IV.2, on

établit la complétude du retournement par condition du cube (à droite) et on en déduit la simplifiabilité et l'existence des ppcm à droite conditionnels. Ensuite, on étudie, dans la section IV.3, les questions liées à la non-terminaison possible du retournement. Le résultat principal est l'identification d'une famille explicite (et infinie) de mots S' close par complément à droite au sens évoqué ci-dessus. Deviner une famille S' convenable et ensuite faire toutes les vérifications nécessaires demande du travail. Comme application, on en déduit la décidabilité de l'existence de multiples à droite communs, complétant ainsi la démonstration de la **proposition B** ci-dessus.

Le chapitre V est celui qui contient les résultats les plus délicats. Sur le modèle de la très riche combinatoire des éléments simples des monoïdes de tresses B_n^+ , définis comme diviseurs des éléments de Garside Δ_n , ppcm des atomes $\sigma_1, \dots, \sigma_{n-1}$, on étudie ici les éléments, aussi notés Δ_n , qui sont les ppcm (à droite) des atomes $\theta_1, \dots, \theta_{n-1}$, et la combinatoire de leurs diviseurs à gauche, qui se révèle très intéressante. On a donc une suite d'éléments Δ_n , chacun diviseur à gauche du suivant (avec un élément intermédiaire $\Delta_{n+0,5}$ naturel), et on étudie les éléments dits *simples* qui sont les diviseurs à gauche des éléments Δ_n . Le chapitre est organisé en quatre sections. Dans la section V.1, on introduit les éléments Δ_n , puis les éléments simples, et on établit une majoration explicite de leur hauteur. Dans la section V.2, le point-clé est que les diviseurs de Δ_n de longueur ℓ qui ne sont pas diviseurs de Δ_{n-1} se partitionnent en trois familles en correspondance bijective avec les diviseurs de Δ_{n-1} de longueur respectivement $\ell - 1$, $\ell - 2$, et $\ell - 3$ (proposition V.2.3). On en déduit que le nombre $N_{n,\ell}$ de tels diviseurs de Δ_n apparaît dans un triangle de Pascal généralisé où on fait la somme des 3 termes au-dessus, et que le nombre total de diviseurs de Δ_n dans H^+ est $2 \cdot 3^{n-3}$ (à mettre en regard de $n!$ pour le monoïde B_n^+). Dans la section V.3, on montre, par un argument inductif délicat basé sur la partition ci-dessus, que les formes normales des éléments simples (au sens du chapitre II) sont celles qui évitent les facteurs interdits mentionnés dans la proposition C. Enfin, poursuivant le parallèle avec les monoïdes de tresses, on montre dans la section V.4 l'existence d'une structure « presque-Garside » sur le monoïde H^+ en construisant des décompositions gloutonnes (« greedy normal decomposition ») pour les éléments de H^+ , ce qui complète la démonstration des résultats de la **proposition C** ci-dessus.

Enfin, le chapitre final VI regroupe deux sections presque indépendantes. Dans la section VI.1, on étudie les représentations du monoïde H^+ dans d'autres monoïdes. On observe que, mises à part les représentations, certainement non fidèles, induites par le passage à la projection sur le monoïde F^+ , les tentatives de représentations via les tresses ou les permutations parenthésées (groupes \widehat{BV} et \widehat{V}) se heurtent à une obstruction topologique. On étudie donc des représentations fonctionnelles, linéaires ou non, en faisant agir H^+ sur un ensemble de suites. Cette approche mène à la construction de plusieurs représentations exotiques. Une famille naturelle est paramétrée

par les matrices 2×2 vérifiant $A^2 = I$. La représentation associée à la matrice unité est la projection sur le monoïde de Thompson F^+ , et on voit facilement que la représentation correspondant à la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est non fidèle (mais reste assez mystérieuse). L'exemple le plus prometteur est celui mentionné dans la **proposition D** ci-dessus. Enfin, dans la section VI.2, on liste quelques-unes des nombreuses questions ouvertes possibles, axées ici sur les propriétés de relation de la divisibilité à droite du monoïde H^+ , puis sur l'existence d'un plongement de H^+ dans un groupe, et finalement sur les représentations de H^+ .

L'annexe informatique fournit quelques précisions sur l'utilisation d'expérimentations informatiques pour étudier le monoïde H^+ , plus spécifiquement sur la représentation des données et sur les divers algorithmes utilisés, en particulier pour dénombrer les éléments simples et pour étudier les représentations linéaires de H^+ .

Table des matières

Introduction	i
Le monoïde H^+	i
Principaux résultats	ii
Organisation du texte	iii
Chapitre I. Le monoïde H^+	1
1. Généralités sur les monoïdes	1
1.1. Monoïdes présentés	1
1.2. Diviseurs et multiples	4
1.3. Noethérianité	7
2. Le contexte	9
2.1. Le monoïde de tresses positives B_∞^+	9
2.2. Le monoïde de Thompson F^+	11
2.3. Tresses et permutations parenthésées	13
3. Le monoïde H^+	15
3.1. Présentation par générateurs et relations	16
3.2. Paramètres numériques	17
3.3. Lien avec le monoïde de Thompson	20
Chapitre II. Utilisation de la réécriture	23
1. Systèmes de réécriture	23
1.1. Réécriture associée à une présentation	23
1.2. Convergence	25
1.3. Noethérianité et confluence	26
2. Le cas du monoïde de Thompson	28
2.1. Le système \mathcal{E}_F	28
2.2. Les mots \mathcal{E}_F -réduits	29
3. Le cas du monoïde H^+	31
3.1. Le système \mathcal{E}_H	31
3.2. Les mots \mathcal{E}_H -réduits	35
3.3. Applications	38
Chapitre III. La méthode du retournement de facteur	43
1. Le retournement de facteur	44
1.1. Suites et diagrammes de retournement	44
1.2. Complétude du retournement	50
1.3. Terminaison du retournement	53

2. Un nouveau critère de complétude	56
2.1. Ensembles clos par complément	56
2.2. Énoncé principal et exemple	59
2.3. Démonstration de la proposition III.2.8	60
3. Un nouveau critère de terminaison	66
3.1. Les présentations (S', R')	67
3.2. Comparaison des retournements	69
3.3. Application à la terminaison	74
Chapitre IV. Utilisation du retournement	77
1. Principes généraux	77
1.1. Simplifiabilité	77
1.2. Multiples communs	78
1.3. Le problème de mots	80
2. Le retournement pour H^+ : complétude	83
2.1. La condition du cube à droite	83
2.2. Applications I : simplifiabilité et ppcm	88
2.3. Le retournement à gauche	90
3. Le retournement pour H^+ : terminaison	91
3.1. Un ensemble clos par complément	92
3.2. Application II : résultats de décidabilité	97
3.3. Terminaison du retournement à gauche	100
Appendice : variantes de la présentation	101
Chapitre V. Les éléments simples de H^+	103
1. Les éléments Δ_n	104
1.1. Le ppcm de $\theta_1, \dots, \theta_{n-1}$	104
1.2. Les diviseurs à gauche de Δ_n	107
2. Dénombrement des éléments simples	109
2.1. Résultats préparatoires	110
2.2. Le résultat de partition	120
2.3. Dénombrement des diviseurs de Δ_n	122
3. Forme normale et décomposition	124
3.1. Décidabilité de la simplicité	125
3.2. Le lemme-clé	127
3.3. Forme normale des éléments simples	131
4. La structure « presque-Garside » de H^+	135
4.1. Décompositions gloutonnes	135
4.2. Le cas du monoïde H^+	138
Chapitre VI. Suite et fin...	143
1. Les représentations du monoïde H^+	143
1.1. Représentations géométriques et fonctionnelles	144
1.2. La représentation Φ_S	147
1.3. Les représentations $\Phi_{s,t}$	152
2. Des questions ouvertes	156

2.1. Propriétés des relations de divisibilité	156
2.2. Le groupe H	157
2.3. Représentations du monoïde H^+ (et du groupe H)	159
Annexe informatique	163
1. Représentation des données	163
2. Principaux algorithmes	164
2.1. Mise sous forme normale	164
2.2. Retournement à droite et procédures dérivées	165
2.3. Comptage des éléments simples	168
2.4. Représentations linéaires	169
Bibliographie	171
Index	175

Chapitre I

Le monoïde H^+

Dans ce chapitre introductif, on rappelle le contexte général des monoïdes présentés, et, en particulier, le cas des monoïdes de tresses et de Thompson, et on introduit le monoïde H^+ qui est notre principal sujet d'étude. Après la définition, on établit quelques premières propriétés.

Ce chapitre comporte trois sections. Dans la section 1, on rappelle le contexte général des monoïdes présentés, et on introduit les notions classiques liées aux relations de divisibilité, en particulier les notions de pgcd et de ppcm, et celle de monoïde noethérien.

Dans la section 2, on introduit les deux principaux monoïdes qui forment le contexte de cette étude, à savoir le monoïde des tresses B_∞^+ et le monoïde de Thompson F^+ . On présente également le monoïde des tresses parenthésées \widehat{BV}^+ , qui est un hybride des deux précédents, en l'occurrence un produit de Zappa-Szep.

Enfin, dans la section 3, on introduit le monoïde H^+ objet de la thèse, par une présentation qui en fait un (autre) hybride des monoïdes B_∞^+ et F^+ , et on établit quelques propriétés qui dérivent directement de la présentation, en particulier la noethérianité et la décidabilité du problème de mots. On observe également que le monoïde de Thompson F^+ est un quotient propre de H^+ .

1. Généralités sur les monoïdes

1.1. Monoïdes présentés. On rappelle ici les notions et notations standards concernant les monoïdes libres et les présentations de monoïde.

Le point de départ est la notion de mot sur un alphabet.

DÉFINITION 1.1 (mot, concaténation). (i) Si S est un ensemble non vide (« *alphabet* »), un S -mot est une suite finie w d'éléments de S , c'est-à-dire une application d'un intervalle $\{1, \dots, \ell\}$ dans S . L'entier ℓ est appelé la *longueur* de w , notée $|w|$. Pour $1 \leq i \leq \ell$, on note $w[i]$ l'image de i , appelé la *i -ème lettre* de w . On note ε le *mot vide*, à savoir l'unique fonction de \emptyset dans S , donc est l'ensemble vide; sa longueur est 0. On note S^* l'ensemble de tous les mots sur S .

(ii) Si u, v sont deux S -mots de longueurs respectives p et q , on note $u \cdot v$, ou uv , la *concaténation* de u et v , définie comme le S -mot w de longueur $p+q$ défini par $w[i] := u[i]$ pour $1 \leq i \leq p$ et $w[i] := v[i-p]$ pour $p+1 \leq i \leq p+q$.

Le résultat suivant est alors classique :

PROPOSITION 1.2 (**monoïde libre**). *La structure $(S^*, \cdot, \varepsilon)$ est un monoïde libre de base S .*

La démonstration de la proposition 1.2 est facile (voir par exemple [28, section I.4], et on ne la redonne pas ici. On rappelle qu'un monoïde M est dit *libre* de base S si M est engendré par S et si, pour tout monoïde M' et toute application $\phi : S \rightarrow M'$, il existe un morphisme de monoïde $\phi^* : M \rightarrow M'$ prolongeant ϕ (et qui, de surcroît, est unique).

Dans la suite, on note généralement S^* pour le monoïde $(S^*, \cdot, \varepsilon)$.

La proposition 1.2 implique que tout monoïde M engendré par un ensemble S est un quotient du monoïde S^* : il existe une congruence \equiv sur S^* , c'est-à-dire une relation d'équivalence compatible avec la concaténation des mots, telle que M est (isomorphe au) quotient S^*/\equiv .

LEMME 1.3. *Pour tout ensemble R de paires d'éléments de S^* , il existe une plus petite congruence \equiv_R incluant R .*

DÉMONSTRATION. Soit \equiv_R la relation binaire sur S^* telle que $w \equiv_R w'$ est vraie s'il existe une suite finie w_0, \dots, w_ℓ vérifiant $w = w_0, w' = w_\ell$ et, pour tout $i < \ell$, il existe des S -mots u_i, u'_i et $\{v_i, v'_i\}$ dans R vérifiant $w_i = u_i v_i u'_i$ et $w_{i+1} = u_i v'_i u'_i$.

Alors \equiv_R est une congruence sur le monoïde S^* incluant R . D'abord \equiv_R est réflexive car, pour tout w , la suite (w) témoigne pour $w \equiv_R w$. Ensuite, si (w_0, \dots, w_ℓ) témoigne pour $w \equiv_R w'$, alors (w_ℓ, \dots, w_0) témoigne pour $w' \equiv_R w$. Puis, si (w_0, \dots, w_ℓ) témoigne pour $w \equiv_R w'$ et (w'_0, \dots, w'_ℓ) témoigne pour $w' \equiv_R w''$, alors la suite $(w_0, \dots, w_\ell, w'_1, \dots, w'_\ell)$ témoigne pour $w \equiv_R w''$. Donc \equiv_R est une relation d'équivalence sur S^* . Par ailleurs, \equiv_R est une congruence sur le monoïde S^* : si (w_0, \dots, w_ℓ) témoigne pour $w \equiv_R w'$, alors $(uw_0v, \dots, uw_\ell v)$ témoigne pour $uwv \equiv_R uw'v$. Enfin, si $\{v, v'\}$ appartient à R , la suite (v, v') témoigne pour $v \equiv_R v'$, et donc \equiv_R inclut R — plus exactement : \equiv_R contient tous les couples (w, w') tels que la paire $\{w, w'\}$ est dans R .

Supposons que \cong est une congruence sur S^* incluant R (au sens ci-dessus), et qu'on a $w \equiv_R w'$. Il existe alors une suite (w_0, \dots, w_ℓ) témoignant pour $w \equiv_R w'$. Par définition, pour chaque i , il existe u_i, u'_i et $\{v_i, v'_i\}$ dans R vérifiant $w_i = u_i v_i u'_i$ et $w_{i+1} = u_i v'_i u'_i$. Puisque R est inclus dans \cong et que \cong est symétrique, on a $v_i \cong v'_i$, puis $u_i v_i u'_i \cong u_i v'_i u'_i$, c'est-à-dire $w_i \cong w_{i+1}$, puisque \cong est une congruence, et enfin $w = w_0 \cong w_\ell = w'$ car \cong est transitive (pour le cas $\ell \geq 2$) et réflexive (pour le cas $\ell = 1$). Donc \cong inclut \equiv_R , qui est la plus petite congruence incluant R . \square

Dans le contexte du lemme 1.3, la plus petite congruence incluant R est appelée la congruence *engendrée* par R . Pour spécifier un monoïde M engendré par un ensemble S , il suffit de spécifier la congruence \equiv_R telle que M est S^*/\equiv_R , et donc de spécifier un sous-ensemble R de $S^* \times S^*$ engendrant \equiv_R .

DÉFINITION 1.4 (présentation). On appelle *présentation de monoïde* un couple (S, R) , où S est un ensemble non vide et R est un ensemble de paires de mots de S^* . On note alors $\langle S \mid R \rangle^+$ le monoïde S^*/\equiv_R , où \equiv_R est la congruence sur S^* engendrée par R . Si u est un S -mot, on note $[u]$ la classe de u par rapport à \equiv_R .

Quand il n'y a pas de confusion possible, on notera \equiv au lieu de \equiv_R . On sait que, dans le contexte de la définition 1.4, on note généralement « $u = v$ » au lieu de « $\{u, v\}$ » les relations de R .

EXEMPLE 1.5 (monoïdes libres). Pour tout ensemble S , la congruence sur S^* engendrée par l'ensemble vide est l'égalité : les seules suites (w_0, \dots, w_ℓ) témoignant pour une équivalence $w \equiv_R w'$ sont les suites triviales (w) . Donc le monoïde $\langle S \mid \emptyset \rangle^+$ est $S^*/=$, c'est-à-dire S^* .

EXEMPLE 1.6 (monoïdes commutatifs libres). Soit S un ensemble fini à n éléments, disons $S = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$. On pose

$$(1.7) \quad M = \langle S \mid \{\mathbf{a}_i \mathbf{a}_j = \mathbf{a}_j \mathbf{a}_i \mid i \neq j\} \rangle^+.$$

Notons \equiv la congruence engendrée par les relations de (1.7). Pour décrire M , il suffit d'identifier un élément distingué dans chaque classe d'équivalence pour \equiv . Soit F l'application de S^* dans \mathbb{N}^n définie par

$$F(w) = (|w|_{\mathbf{a}_1}, \dots, |w|_{\mathbf{a}_n}),$$

où $|w|_{\mathbf{a}_i}$ est le nombre d'occurrences de \mathbf{a}_i dans w . Par définition, on a $F(\mathbf{a}_i \mathbf{a}_j) = F(\mathbf{a}_j \mathbf{a}_i)$ pour tous i, j . Par ailleurs, pour tous mots u, v de S^* , on a $F(uv) = F(u) + F(v)$, où $+$ est la somme terme à terme sur \mathbb{N}^n . Il en résulte que la relation $F(w) = F(w')$ est un congruence sur S^* , qui inclut les relations de (1.7). Par conséquent, $w \equiv w'$ implique $F(w) = F(w')$. Dans l'autre sens, appelons *normaux* les S -mots du type $\mathbf{a}_1^{e_1} \dots \mathbf{a}_n^{e_n}$ avec $e_1, \dots, e_n \geq 0$. Alors tout S -mot est \equiv -équivalent à un mot normal. Si deux S -mots w, w' vérifient $F(w) = F(w')$, alors ils sont tous deux \equiv -équivalents au même S -mot normal, et donc vérifient $w \equiv w'$. Par conséquent, les relations $w \equiv w'$ et $F(w) = F(w')$ sont équivalentes. De plus, si w et w' sont des S -mots normaux distincts, alors, par définition, on a $F(w) \neq F(w')$. Par conséquent, tout S -mot est \equiv -équivalent à un *unique* S -mot normal, et l'application F induit une bijection entre l'ensemble S_{norm} des S -mots normaux et l'ensemble \mathbb{N}^n .

De plus, on a noté que $F(uv) = F(u) + F(v)$ est vérifié pour tous S -mots u, v , donc la bijection ci-dessus est un isomorphisme entre le monoïde M et le monoïde $(\mathbb{N}^n, +)$. En d'autres termes, le monoïde M est (isomorphe à) $(\mathbb{N}^n, +)$.

Par construction, M est un monoïde commutatif et il est engendré par $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$. On peut noter que M est un monoïde commutatif *libre* de base $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$. En effet, soit M_1 un monoïde commutatif quelconque, et soit ϕ une application de $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ dans M_1 . Par définition, M est le quotient du monoïde libre S^* par la congruence \equiv . Soit ϕ^* l'unique extension de ϕ en un homomorphisme du monoïde libre S^* dans M_1 (lemme 1.2).

Si deux S -mots w, w' sont \equiv -équivalents, ils vérifient $F(w) = F(w')$ et, comme M_1 est commutatif par hypothèse, on doit avoir $\phi^*(w) = \phi^*(w')$. Par conséquent, ϕ^* induit un morphisme bien défini de S^*/\equiv , c'est-à-dire de M , dans M_1 . Donc M est libre de base S dans la variété des monoïdes commutatifs (mais pas dans la variété des monoïdes quelconques).

EXEMPLE 1.8 (monoïdes de Baumslag-Solitar). Considérons

$$(1.9) \quad M = \langle \mathbf{a}, \mathbf{b} \mid \mathbf{ba} = \mathbf{ab}^2 \rangle^+.$$

On note \equiv la congruence sur $\{\mathbf{a}, \mathbf{b}\}^*$ associée à la présentation (1.9). Comme dans l'exemple 1.6, on peut identifier un élément distingué dans chaque classe d'équivalence. Appelons *normaux* les mots de la forme $\mathbf{a}^p \mathbf{b}^q$ avec $p, q \geq 0$. À partir de deux invariants par rapport à \equiv , à savoir le nombre d'occurrences de la lettre \mathbf{a} et l'application $I_{\mathbf{b}}(w) := \sum_{i=1}^{|w|} \delta_{w(i), \mathbf{b}} 2^{\#\{i < j \leq |w| \mid w(j) = \mathbf{a}\}}$, où $\delta_{x,y}$ vaut 1 pour $x = y$ et 0 sinon, on peut montrer que chaque classe contient un, et un seul mot normal. Par conséquent, l'application $\phi : [\mathbf{a}^p \mathbf{b}^q] \mapsto (p, q)$ définit une bijection de M sur l'ensemble \mathbb{N}^2 . De plus, on trouve

$$\mathbf{a}^p \mathbf{b}^q \cdot \mathbf{a}^r \mathbf{b}^s = \mathbf{a}^{p+1} \mathbf{b}^{2q} \mathbf{a}^{r-1} \mathbf{b}^s = \mathbf{a}^{p+2} \mathbf{b}^{2^2 q} \mathbf{a}^{r-2} \mathbf{b}^s = \dots = \mathbf{a}^{p+r} \mathbf{b}^{2^r q + s}.$$

De là, ϕ établit un isomorphisme entre M et $(\mathbb{N} \times \mathbb{N}, *)$ avec $*$ définie par

$$(p, q) * (r, s) = (p + r, 2^r q + s),$$

ce qui signifie que M est isomorphe au produit semi-direct $\mathbb{N} \rtimes_{\varphi} \mathbb{N}$ avec $\varphi : \mathbb{N} \rightarrow \text{Aut}(\mathbb{N}, +)$ défini par $\varphi_r(q) = 2^r q$.

1.2. Diviseurs et multiples. On rappelle ici la terminologie relative aux relations de divisibilité dans un monoïde.

DÉFINITION 1.10 (**diviseur à gauche**). Si M est un monoïde et x, y deux éléments de M , on dit que x est un *diviseur à gauche* de y ou que y est un *multiple à droite* de x , noté $x \preceq y$, s'il existe x' dans M satisfaisant $xx' = y$. Pour y dans M , on pose $\text{Div}(y) = \{x \in M \mid x \preceq y\}$.

Par exemple, la relation de divisibilité à gauche dans le monoïde $(\mathbb{N}, +)$ coïncide avec l'ordre standard des entiers. Plus généralement, pour deux éléments x, y de \mathbb{N}^n , on a $x \preceq y$ si, et seulement si, on a $x(k) \leq y(k)$ est vrai pour tout k . En effet, l'égalité $xx' = y$ implique $\forall k (x(k) \leq x(k) + x'(k) = y(k))$ et $\forall k (x(k) \leq y(k))$ implique $xx' = y$ pour x' déterminé par $x'(k) = y(k) - x(k)$.

On rappelle qu'un monoïde M est dit *simplifiable à gauche* (resp., à droite) si toute relation $xy = xz$ (resp., $yx = zx$) avec x, y, z dans M implique $y = z$. On dit que M est *simplifiable* s'il est à la fois simplifiable à gauche et à droite.

LEMME 1.11. (i) *Si M est un monoïde, la relation de divisibilité à gauche dans M est un préordre partiel qui est invariant par multiplication à gauche.*

(ii) *Si M est un monoïde simplifiable à gauche et sans élément inversible non trivial, la relation de divisibilité à gauche dans M est un ordre partiel.*

DÉMONSTRATION. (i) Soit M un monoïde. Si on note 1 l'élément neutre de M , on a $x1 = x$ pour tout x dans M . Donc la relation \preccurlyeq est réflexive. Ensuite, si nous avons $xx' = y$ et $yy' = z$, nous en déduisons $x(x'y') = yy' = z$, donc \preccurlyeq est transitive. Supposons maintenant $x \preccurlyeq y$. Par définition, nous avons $xx' = y$ pour un certain x' dans M . On en déduit que, pour tout $z \in M$, on a $(zx)x' = z(xx') = zy$, d'où $zx \preccurlyeq zy$.

(ii) Il reste à montrer que \preccurlyeq est antisymétrique. Supposons que $x \preccurlyeq y$ et $y \preccurlyeq x$. Alors, il existe x' et y' dans M tels que $xx' = y$ et $yy' = x$. On en déduit que $yy'x' = y$, donc, par simplifiabilité à gauche, $y'x' = 1$. Or, M ne possède aucun élément inversible non trivial, donc on obtient $y' = x' = 1$, d'où $x = y$. \square

Au lieu de considérer la divisibilité à gauche qui correspond à multiplier à droite, nous pouvons, symétriquement, utiliser la multiplication à gauche.

DÉFINITION 1.12 (**diviseur à droite**). Si M est un monoïde et x, y deux éléments de M , on dit que x est *diviseur à droite* de y ou que y est *multiple à gauche* de x , noté $y \succcurlyeq x$, s'il existe x' dans M satisfaisant $x'x = y$. Pour y dans M , on pose $\widetilde{\text{Div}}(y) = \{x \in M \mid y \succcurlyeq x\}$.

Les relations de divisibilité à droite et à gauche ont des propriétés entièrement symétriques.

Lorsque les relations de divisibilité sont des relations d'ordre, il est naturel de considérer les éventuelles bornes inférieures et bornes supérieures associées.

DÉFINITION 1.13 (**ppcm, pgcd**). Soit M un monoïde. Pour x dans M et S inclus dans M , on dit que x est un *plus petit multiple à droite commun*, ou *ppcm à droite*, de S , si x est un multiple à droite de tous les éléments de S et que tout élément de M qui est multiple à droite de tous les éléments de S est multiple à droite de x . Si S possède deux éléments, on dit "ppcm à droite de x et y " pour "ppcm de $\{x, y\}$ " et on le note $x \vee y$ s'il est unique.

De même, on dit que x est un *plus grand diviseur à gauche commun*, ou *pgcd à gauche*, de S , si x est un diviseur à gauche de tous les éléments de S et que tout élément de M qui est un diviseur à gauche de tous les éléments de S est un diviseur à gauche de x . Si S possède deux éléments, on dit "pgcd à gauche de x et y " pour "pgcd de $\{x, y\}$ " et on le note $x \wedge y$ s'il est unique.

Les notions de ppcm à gauche et pgcd à droite sont définies symétriquement en utilisant la divisibilité à droite.

Reprenant l'exemple du monoïde commutatif libre \mathbb{N}^n , on vérifie facilement que deux éléments x, y admettent comme ppcm (bilatère) l'élément z défini par $z(k) := \max(x(k), y(k))$, et comme pgcd l'élément z' défini par $z'(k) := \min(x(k), y(k))$.

DÉFINITION 1.14 (**multiples communs**). On dit qu'un monoïde M *admet des multiples à droite communs* (*resp.*, des ppcm à droite) si deux éléments quelconques de M possèdent un multiple à droite commun (*resp.*, un

ppcm à droite). On dit que M admet des ppcm à droite conditionnels si deux éléments de M qui admettent un multiple à droite commun, possèdent un ppcm à droite.

LEMME 1.15. *Si M est un monoïde simplifiable à gauche, sans élément inversible non trivial et si x, y sont deux éléments de M , alors, un ppcm (resp., un pgcd) à droite (resp., à gauche) de x et y est unique s'il existe.*

DÉMONSTRATION. Supposons que z et z' sont des ppcm à droite de x et y . L'hypothèse z est un ppcm à droite de x et y implique $z \preceq z'$, tandis que z' est un ppcm à droite de x et y implique $z' \preceq z$. Or, par le lemme 1.11, la relation \preceq est un ordre partiel, d'où $z = z'$. L'argument est similaire pour les pgcd à gauche. \square

Quand on a l'unicité des ppcm à droite, il est naturel d'introduire :

DÉFINITION 1.16 (**complément**). Sous les hypothèses du lemme 1.15, pour x, y dans M tels que le ppcm à droite de x et y existe, on appelle *complément à droite*, et on note $x \setminus y$, l'unique élément z vérifiant $xz = x \vee y$.

Le complément à gauche x / y est défini symétriquement. L'opération complément est relié au produit par une formule simple, qui revient à l'associativité du ppcm.

LEMME 1.17. *Si M est un monoïde simplifiable à gauche, sans élément inversible non trivial et admettant des ppcm à droite conditionnels, alors, pour tous x, y, z dans M , on a*

$$(1.18) \quad (xy) \setminus z = y \setminus (x \setminus z).$$

DÉMONSTRATION. Supposons que $(xy) \setminus z$ existe. Par définition, $(xy) \vee z$ est un multiple à droite de xy . De plus, par transitivité de \preceq , la relation $x \preceq xy$ implique $x \preceq (xy) \vee z$. Donc $(xy) \vee z$ est un multiple commun à droite de x et z . Comme M admet des ppcm à droite conditionnels, cela implique que $x \vee z$ existe et, par définition, $(xy) \vee z$ est un multiple à droite de $x \vee z$. Par conséquent, $(xy) \vee z$ est un multiple à droite commun de $x \vee z$ et de xy . Ceci implique que $x \vee z$ et de xy ont un ppcm à droite et on a $(xy) \vee (x \vee z) \preceq (xy) \vee z$. Réciproquement, par la transitivité de \preceq , la relation $z \preceq x \vee z$ implique $z \preceq (xy) \vee (x \vee z)$. Donc $(xy) \vee (x \vee z)$ est un multiple commun à droite de z et de xy . Ceci implique $(xy) \vee z \preceq (xy) \vee (x \vee z)$. Par le lemme 1.11, la relation \preceq est un ordre partiel, donc $(xy) \vee z = (xy) \vee (x \vee z)$. On obtient donc

$$\begin{aligned} xy((xy) \setminus z) &= (xy) \vee z = (xy) \vee (x \vee z) = (xy) \vee (x(x \setminus z)) \\ &= x(y \vee (x \setminus z)) = xy(y \setminus (x \setminus z)), \end{aligned}$$

et on simplifie à gauche par xy . \square

Pour terminer ces rappels, notons qu'il existe des liens entre existence des pgcd et des ppcm.

PROPOSITION 1.19 (existence ppcm). *Si M est un monoïde tel que toute famille non vide d'éléments de M admet un pgcd à gauche, alors M admet des ppcm à droite conditionnels.*

DÉMONSTRATION. Soient x et y deux éléments de M qui admettent un multiple à droite commun. Soit S la famille de tous les multiples à droite communs de x et y . Par hypothèse, S est non vide donc il admet un pgcd à gauche, noté z . Par définition, x divise à gauche tout élément de S , donc il divise à gauche z . De même, y divise à gauche z . Donc z est un multiple à droite commun de x et y . De plus, tout élément de S est un multiple à droite de z puisque z divise à gauche tous les éléments de S . Ainsi, z est un ppcm à droite de x et y . \square

1.3. Noéthérianité. On étudie des conditions de finitude impliquant les relations de divisibilité. Appelées conditions de noéthérianité, ces hypothèses assurent automatiquement l'existence de certains éléments maximaux ou minimaux. Avec ces conditions supplémentaires, nous donnerons une réciproque au lemme 1.19.

DÉFINITION 1.20 (diviseur propre). Si M est un monoïde et si x, y sont dans M , on dit que x est un *diviseur propre à gauche* (resp., à droite) de y , noté $x \prec y$ (resp., $y \succ x$), si on a $xx' = y$ (resp., $y = x'x$) avec x' non inversible.

Si M est un monoïde simplifiable à gauche et sans élément inversible non trivial, la relation \prec est un ordre partiel strict sur M .

Si R est une relation binaire sur un ensemble S , une suite décroissante par rapport à R est une suite (finie ou infinie) (x_0, x_1, \dots) telle que $x_{i+1}Rx_i$ pour tout i . La relation R est dite *bien fondée* si toute sous-famille non vide S' de S a un élément R -minimal, c'est-à-dire, un élément x dans S' satisfaisant que yRx n'est vérifié pour aucun y dans S' . On sait que ceci équivaut à la non-existence d'une suite infinie décroissante par rapport à R .

DÉFINITION 1.21 (noéthérianité). Un monoïde est dit *noéthérien à gauche* (resp., à droite) si la relation associée \prec (resp., \succ) est bien fondée.

Par le critère rappelé ci-dessus, un monoïde est noéthérien à gauche (resp., à droite) si, et seulement si, il n'existe aucune suite décroissante infinie dans M par rapport à la relation \prec (resp., \succ).

Par exemple, le monoïde commutatif libre \mathbb{N}^n est noéthérien (des deux côtés) : en effet, les relations $x \prec y$ et $x \succ y$ sont équivalentes à la conjonction de $\forall k (x(k) \leq y(k))$ et de $\exists k (x(k) < y(k))$. Il est clair qu'il n'existe pas de suite infinie décroissante.

Il est souvent difficile d'établir qu'un monoïde spécifié par une présentation est noéthérien. Cependant, il existe un cas où c'est facile :

PROPOSITION 1.22 (noéthérianité). *Supposons que (S, R) est une présentation de monoïde et que toutes les relations de R sont du type $u = v$ avec*

$|u| = |v|$. Alors le monoïde $\langle S \mid R \rangle^+$ est noethérien et n'admet aucun élément inversible non trivial.

DÉMONSTRATION. Une induction sur la longueur d'une dérivation de w à w' montre que, si w et w' sont deux S -mots R -équivalents, on a $|w| = |w'|$. Pour g dans $\langle S \mid R \rangle^+$, définissons $|g|$ comme la valeur commune de $|w|$ pour tous les S -mots w représentant g . Alors $fg = h$ entraîne $|f| + |g| = |h|$, et, par conséquent, $g \prec h$ entraîne $|g| < |h|$, ce qui interdit l'existence d'une suite infinie décroissante pour \prec . L'argument est le même pour $\tilde{\succ}$.

Enfin, comme le mot vide est le seul mot de longueur nulle, il ne peut exister d'élément inversible autre que 1 : en effet, $gh = 1$ entraîne $|g| + |h| = 0$, d'où $|g| = |h| = 0$, et $g = h = 1$. \square

Par définition, les hypothèses de noethérianité garantissent l'existence d'éléments qui sont minimaux ou maximaux pour la divisibilité.

LEMME 1.23. *Si M est un monoïde simplifiable à gauche, sans élément inversible non trivial, noethérien à droite, et si X est un sous-ensemble non vide de M inclus dans $\text{Div}(m)$ pour un certain m de M . Alors X admet un élément \prec -maximal.*

DÉMONSTRATION. Pour tout a dans X , par définition, il existe un élément $f(a)$ vérifiant $af(a) = m$, unique puisque M est simplifiable à gauche. Posons $Y := \{f(a) \mid a \in X\}$. Puisque X est non vide, Y est non vide. Alors, par hypothèse, il existe un élément b dans Y qui est $\tilde{\succ}$ -minimal. Soit a un élément de X vérifiant $ab = m$, c'est-à-dire $f(a) = b$. On va montrer que a est \prec -maximal dans X .

En effet, supposons qu'on a $a \preccurlyeq a'$, soit $a' = ac$, et $a' \in X$. Par construction, on a $m = a'f(a') = acf(a') = af(a)$, donc $f(a) = cf(a')$ par simplification, et, de là, $f(a) \succcurlyeq f(a')$ dans Y . Le choix de a exclut $f(a) \tilde{\succ} f(a')$. Par conséquent, c doit être inversible, ce qui signifie qu'on n'a pas $a \prec a'$. \square

L'intérêt pour nous ici du résultat précédent est de fournir une (sorte de) réciproque à la proposition 1.19 :

PROPOSITION 1.24 (**pgcd**). *Si M est un monoïde simplifiable à gauche sans élément inversible non trivial, noethérien à droite et admettant des ppcm à droite conditionnels, alors toute sous-famille non vide de M admet un pgcd à gauche.*

DÉMONSTRATION. Soit S une famille non vide de M . Soit m un élément de S et soit X la famille des éléments de M qui divisent à gauche tout élément de S . Par définition, X est inclus dans $\text{Div}(m)$ et il est non vide car contient 1 . Par le lemme 1.23, l'ensemble X contient un élément \prec -maximal, disons a . On va montrer que a est pgcd à gauche de S , ce qui, par définition, signifie montrer qu'on a forcément $x \preccurlyeq a$ pour tout x dans X .

Soit donc x un élément de X . Par hypothèse, on a $a \preccurlyeq m$ et $x \preccurlyeq m$, et m est un multiple à droite commun de a et x . Comme M admet des ppcm à droite conditionnels, a et x ont un ppcm à droite $a \vee x$. Soit s quelconque

dans S . Comme a et x appartiennent à X , on doit avoir $a \preccurlyeq s$ et $x \preccurlyeq s$, d'où $a \vee x \preccurlyeq s$ par définition du ppcm. Ceci montre que $a \vee x$ appartient à X . Comme par définition, on a $a \preccurlyeq a \vee x$ et que a est \prec -maximal dans X , on déduit $a = a \vee x$, d'où $x \preccurlyeq a$. \square

Pour terminer, on rappelle la notion d'atome dans un monoïde.

DÉFINITION 1.25 (atome). Un élément a d'un monoïde M est un *atome* si a n'est pas inversible et toute décomposition de a contient au plus un élément non inversible.

En d'autres termes, a est un atome si a n'est pas inversible et s'il n'existe aucune égalité $a = a_1 a_2$ avec a_1, a_2 tous deux non inversibles. Sous de bonnes conditions, on est assurés que les atomes forment une famille génératrice minimale :

PROPOSITION 1.26 (atomes générateurs). *Si M est un monoïde simplifiable à gauche, noethérien à droite et à gauche et sans élément inversible non trivial, une partie S de M engendre M si, et seulement si, elle contient 1 et tous les atomes de M .*

On omet la démonstration de ce résultat, qui ne sera pas utilisé directement dans la suite.

2. Le contexte

Comme on l'a observé dans l'introduction, le monoïde qu'on se propose d'étudier est lié à la fois aux monoïdes de tresses et au monoïde de Richard Thompson F^+ . On rappelle ici la définition et les propriétés de base de ces monoïdes, ainsi que celles du monoïde \widehat{BV}^+ qui est un composite des précédents, et qui, de ce fait, apparaît comme un cousin direct de H^+ .

2.1. Le monoïde de tresses positives B_∞^+ . Le point de départ est la notion de *groupe des tresses à n brins* [6]. Pour tout entier $n \geq 1$, on considère des *diagrammes de tresses à n brins*, obtenus en empilant des diagrammes élémentaires d'un des types suivants

$$\begin{array}{ccccccc} & 1 & 2 & & i & i+1 & & n-1 & n \\ \sigma_i : & | & | & \cdots & \diagdown & \diagup & \cdots & | & | \\ & | & | & & \diagup & \diagdown & & | & | \\ \sigma_i^{-1} : & | & | & \cdots & \diagup & \diagdown & \cdots & | & | \end{array}$$

On peut voir ces diagrammes (bidimensionnels) comme la projection sur le plan de familles de courbes de \mathbb{R}^3 reliant (par exemple) les n points $(i, 0, 1)$, $1 \leq i \leq n$, aux n points $(i, 0, 0)$, $1 \leq i \leq n$, sans se croiser et avec la règle que la 3ème coordonnée évolue de façon monotone (pas de rebroussement). On a alors une notion naturelle d'*isotopie* de telles familles de courbes, c'est-à-dire de déformation continue laissant les extrémités fixes, qui induit une

relation \sim sur les diagrammes projetés. Le principe est d'appeler *tresse à n brins* la classe d'isotopie d'une famille de n courbes ou, ce qui revient au même, la classe pour \sim des diagrammes projections. On note B_n l'ensemble des tresses à n brins.

La concaténation des diagrammes — ou des courbes dont ils sont la projection — définit sur B_n un produit. Celui-ci est associatif, admet comme élément neutre la classe du diagramme sans croisement, et toute tresse admet un inverse, à savoir l'image par réflexion dans un miroir horizontal. Donc B_n est muni d'une structure de groupe.

Par construction, toute tresse de B_n admet une expression comme produit d'un nombre fini de tresses σ_i et σ_i^{-1} . Donc, la famille $\{\sigma_1, \dots, \sigma_{n-1}\}$ engendre le groupe B_n . D'un point de vue algébrique, le résultat de base est le suivant, établi par Emil Artin vers 1925 [2, 3], voir Figure 1 :

PROPOSITION 2.1 (**présentation**). *Pour tout entier $n \geq 1$, le groupe B_n admet la présentation*

$$(2.2) \quad B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_j \sigma_i = \sigma_i \sigma_j & \text{pour } j \geq i + 2 \\ \sigma_j \sigma_i \sigma_j = \sigma_i \sigma_j \sigma_i & \text{pour } j = i + 1 \end{array} \right\rangle.$$

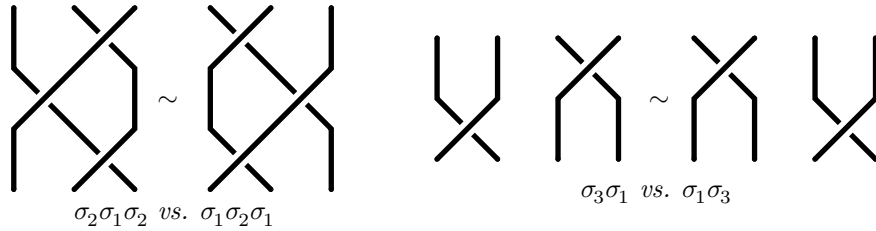


FIGURE 1. Les relations de tresses

Pour tout n , l'application identité de $\{\sigma_1, \dots, \sigma_{n-1}\}$ dans $\{\sigma_1, \dots, \sigma_n\}$ induit un homomorphisme injectif $i_{n,n+1}$ de B_n dans B_{n+1} , et on peut identifier B_n avec le sous-groupe de B_{n+1} engendré par $\sigma_1, \dots, \sigma_{n-1}$. On note alors B_∞ la réunion de tous les groupes B_n — formellement : la limite inductive du système des $(B_n, i_{n,n+1})$ — qui admet donc la présentation (infinie)

$$(2.3) \quad B_\infty = \left\langle \sigma_1, \sigma_2, \dots \mid \begin{array}{ll} \sigma_j \sigma_i = \sigma_i \sigma_j & \text{pour } j \geq i + 2 \\ \sigma_j \sigma_i \sigma_j = \sigma_i \sigma_j \sigma_i & \text{pour } j = i + 1 \end{array} \right\rangle.$$

Comme les relations des présentations (2.2) et (2.3) ne font intervenir aucun inverse des générateurs, on peut également considérer les monoïdes que celles-ci définissent, à savoir

$$(2.4) \quad B_n^+ := \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_j \sigma_i = \sigma_i \sigma_j & \text{pour } j \geq i + 2 \\ \sigma_j \sigma_i \sigma_j = \sigma_i \sigma_j \sigma_i & \text{pour } j = i + 1 \end{array} \right\rangle^+,$$

$$(2.5) \quad B_\infty^+ := \left\langle \sigma_1, \sigma_2, \dots \mid \begin{array}{ll} \sigma_j \sigma_i = \sigma_i \sigma_j & \text{pour } j \geq i + 2 \\ \sigma_j \sigma_i \sigma_j = \sigma_i \sigma_j \sigma_i & \text{pour } j = i + 1 \end{array} \right\rangle^+.$$

Suivant un résultat non trivial, dû à F.A. Garside [37, 38], le monoïde B_n^+ est isomorphe au sous-monoïde du groupe B_n engendré par $\sigma_1, \dots, \sigma_{n-1}$ et, de même, B_∞^+ est isomorphe au sous-monoïde du groupe B_∞ engendré par les éléments σ_i , $i \geq 1$. Le point de la démonstration est d'établir que les monoïdes B_n^+ et B_∞^+ sont simplifiables et admettent des multiples communs, ce qui permet d'appliquer le théorème de Ore [48] et de montrer que B_n (*resp.*, B_∞) est un groupe de fractions (à droite et à gauche) pour le monoïde B_n^+ (*resp.*, B_∞^+). Pour cela, la propriété cruciale est l'existence dans le monoïde B_n^+ d'un ppcm (à droite et à gauche) Δ_n pour les générateurs $\sigma_1, \dots, \sigma_{n-1}$, à savoir

$$(2.6) \quad \Delta_n := (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1 \sigma_2)(\sigma_1).$$

Les diviseurs de l'élément Δ_n , appelés éléments *simples* de B_n^+ , sont au nombre de $n!$, en correspondance bijective avec les permutations de $\{1, \dots, n\}$. Tout élément du groupe B_n , donc en particulier tout élément du monoïde B_n^+ , admet une décomposition canonique en produit d'éléments simples : c'est la forme normale dite « greedy », objet de la théorie de Garside [36, 28].

2.2. Le monoïde de Thompson F^+ . Le groupe de Thompson F a été introduit à la fin des années 1960 par Richard Thompson [45, 53] dans son étude de l'associativité, et il admet plusieurs caractérisations équivalentes. La plus usuelle [15] définit F comme le groupe des difféomorphismes croissants de l'intervalle réel $[0, 1]$ affines par morceau et dyadiques, au sens où les pentes des segments et leurs extrémités sont des rationnels dyadiques (rationnels dont le dénominateur est une puissance de 2). On montre qu'un élément de F est spécifié par un couple de divisions dyadiques de $[0, 1]$ (partition en intervalles à extrémités dyadiques) et, de là, de façon équivalente, par un couple d'arbres binaires finis, voir la figure 2.

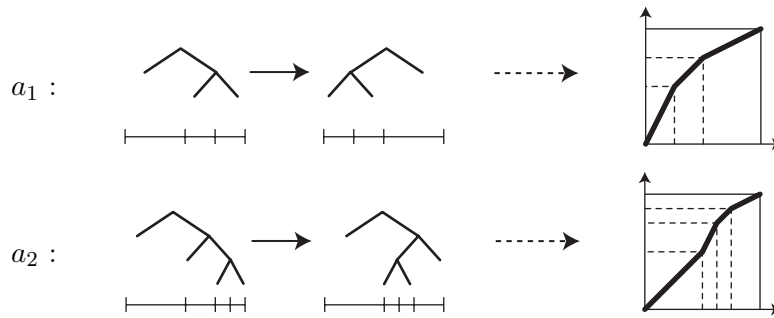


FIGURE 2. Correspondance entre couples d'arbres binaires, couples de décompositions dyadiques de $[0, 1]$, et difféomorphismes dyadiques croissants de $[0, 1]$

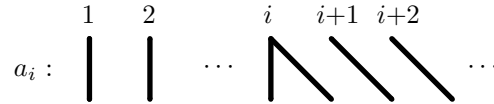
On montre que F est engendré par l'élément a_1 de la figure 2, qui est la dilatation de rapport 2 sur $[0, 1/4]$ suivie d'une translation sur $[1/4, 1/2]$ et

d'une contraction de rapport $1/2$ sur $[1/2, 1]$, et de ses images translatées a_i , où a_i est l'identité sur $[0, 1 - 2^{-(n-1)}]$ suivie d'une copie homothétique de a_1 de rapport $1/2^{n-1}$ sur $[1 - 2^{-(n-1)}, 1]$. Il est alors facile de donner une présentation en termes des générateurs a_i [15] :

PROPOSITION 2.7 (**présentation**). *Le groupe F admet la présentation*

$$(2.8) \quad F := \langle a_1, a_2, \dots \mid a_j a_i = a_i a_{j+1} \text{ pour } j \geq i + 1 \rangle.$$

Pour se rapprocher du formalisme des diagrammes de tresses, il est commode de passer des arbres binaires aux forêts (familles finies d'arbres) en considérant les sous-arbres attachés sous les nœuds de la branche droite. Il est alors naturel d'associer au générateur a_i le diagramme de bifurcation suivant



Alors les relations de (2.8) correspondent aux diagrammes de la figure 3.

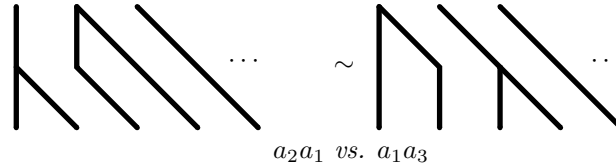


FIGURE 3. Les relations de Thompson

Comme les relations de la présentation (2.3) du groupe B_∞ , les relations de (2.8) ne font pas apparaître d'inverse des générateurs, et on peut donc considérer le monoïde défini par ces relations, à savoir

$$(2.9) \quad F^+ := \langle a_1, a_2, \dots \mid a_j a_i = a_i a_{j+1} \text{ pour } j \geq i + 1 \rangle^+.$$

Il est alors assez facile (plus facile que pour B_∞^+) de montrer que le monoïde F^+ est isomorphe au sous-monoïde du groupe F engendré par les éléments a_i , $i \geq 1$. À nouveau, le point de la démonstration est d'établir que le monoïde F^+ est simplifiable et admet des multiples communs à droite (et même des ppcm à droite), d'où il résulte par le théorème de Ore que F est un groupe de fractions à droite pour F^+ . Les éléments du monoïde F^+ sont donc représentés de façon fidèle par classes d'isotopie de diagrammes de bifurcation (ou par les arbres correspondants, qui ne dépendent pas de l'ordre d'énumération) comme sur la figure 3.

REMARQUE 2.10. La présentation (2.8) du groupe F est redondante : on vérifie que F est engendré par a_1 et a_2 , à partir desquels les autres éléments a_i se définissent par conjugaison. En termes des générateurs a_1 et a_2 , le groupe F possède une présentation finie, avec seulement deux relations.

Mais des inverses figurent dans les relations, qui donc ne définissent pas naturellement de monoïde. Par contre, il existe une autre présentation naturelle de F en termes d'une famille de générateurs A_α indexés par les suites finies de 0 et de 1, et tels que a_i correspond à $A_{11\dots 1}$, $i - 1$ fois 1 [22]. L'intérêt de cette présentation, encore plus redondante que celle de (2.8), est de mener à un monoïde F^{+*} qui possède des ppcm à droite et à gauche, et qui, par rapport à F^+ , peut être vu comme une version duale, au sens où les monoïdes de Birman–Ko–Lee [7] sont duaux des monoïdes de tresses B_n^+ .

2.3. Tresses et permutations parenthésées. Quand le groupe de tresses B_∞ et le groupe de Thompson F sont vus comme groupes de classes d'isotopie de diagrammes, respectivement de croisements et de bifurcations, il est naturel de chercher à les marier en un groupe qui les admettrait tous deux comme sous-groupes. Cela a été fait par M. Brin dans [11, 12] et P. Dehornoy dans [24], le groupe obtenu étant appelé \widehat{BV} (en tant que version tressée du groupe F) ou B_\bullet , groupe des tresses parenthésées (en tant que version « thompsonifiée », ou parenthésée, du groupe de tresses). Le groupe est engendré par une double famille de générateurs, σ_i , $i \geq 1$, et a_j , $j \geq 1$, en termes desquels il possède une présentation dont les relations sont

- les relations de tresses de (2.2),
- les relations de Thompson de (2.8),
- plus des relations mixtes entre les deux familles de générateurs [11, 24], voir figure 4 :

PROPOSITION 2.11 (**présentation**). *Le groupe \widehat{BV} admet la présentation*

$$(2.12) \quad \widehat{BV} = \left\langle \begin{array}{l} \sigma_1, \sigma_2, \dots \\ a_1, a_2, \dots \end{array} \left| \begin{array}{l} (2.2) + a_j \sigma_i = \sigma_i a_j, \quad \sigma_{j-1} a_i = a_i \sigma_j \quad \text{pour } j \geq i + 2 \\ (2.8) + a_j \sigma_i \sigma_j = \sigma_i a_i, \quad a_i \sigma_j \sigma_i = \sigma_i a_j \quad \text{pour } j = i + 1 \end{array} \right. \right\rangle.$$

Comme dans le cas de B_∞ et F , la présentation (2.12) est positive (pas d'inverse des générateurs dans les relations), et elle définit donc un monoïde, à savoir

$$(2.13) \quad \widehat{BV}^+ := \left\langle \begin{array}{l} \sigma_1, \sigma_2, \dots \\ a_1, a_2, \dots \end{array} \left| \begin{array}{l} (2.2)^+ a_j \sigma_i = \sigma_i a_j, \quad \sigma_{j-1} a_i = a_i \sigma_j \quad \text{pour } j \geq i + 2 \\ (2.8)^+ a_j \sigma_i \sigma_j = \sigma_i a_i, \quad a_i \sigma_j \sigma_i = \sigma_i a_j \quad \text{pour } j = i + 1 \end{array} \right. \right\rangle^+.$$

À nouveau, on montre que le monoïde \widehat{BV}^+ se plonge dans le groupe \widehat{BV} comme sous-monoïde engendré par les éléments σ_i et a_j , et que \widehat{BV} est un groupe de fractions à droite pour \widehat{BV}^+ . Les monoïdes B_∞^+ et F^+ apparaissent comme sous-monoïdes de \widehat{BV}^+ , engendrés respectivement par les éléments σ_i et par les éléments a_j . Le point est que le monoïde \widehat{BV}^+ est un produit de Zappa-Szep [51, 55] de F^+ et de B_∞^+ , c'est-à-dire un analogue à un produit semi-direct, mais où chacun des deux monoïdes agit sur l'autre : ici le monoïde F^+ agit sur B_∞^+ par dédoublement de brins, tandis que B_∞^+ agit sur F^+ par permutation des positions [13, 24].

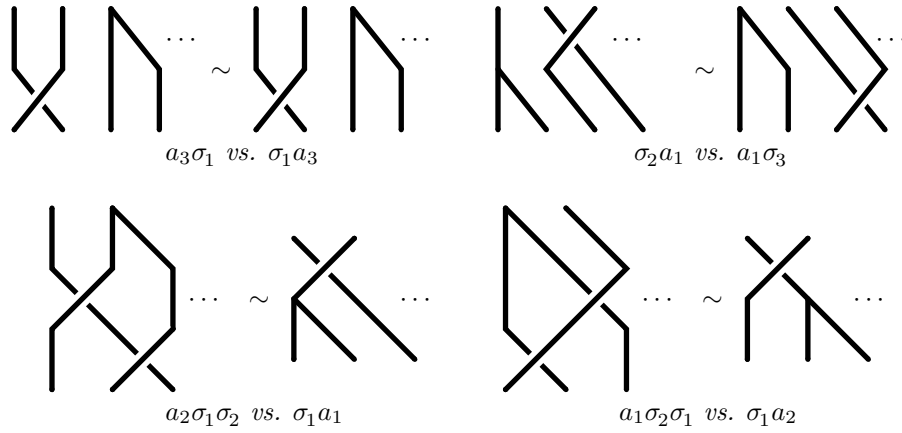


FIGURE 4. Les relations mixtes de tresses parenthésées : quatre familles de relations où les générateurs σ_i et a_j interfèrent. L'interprétation diagrammatique de σ_i et a_j est la même que plus haut, et les relations se lisent naturellement.

REMARQUE 2.14. Les relations des présentations (2.8) et (2.12) ne sont pas invariantes par symétrie, et on trouve dans la littérature les deux versions, typiquement « $21 = 13$ » (comme ici), ou « $12 = 31$ » (comme par exemple dans [24]) : cela dépend, pour F^+ , de l'ordre de composition des difféomorphismes. De là, si on veut que les diagrammes se lisent de haut en bas, cela revient à associer aux éléments a_i des diagrammes de bifurcations (comme ici ou dans [11]), ou des diagramme de confluence (comme dans [24]) : *mutatis mutandis*, les propriétés sont évidemment similaires.

Tout diagramme de tresses à n brins définit une permutation de l'ensemble $\{1, \dots, n\}$, à savoir la fonction qui, à chaque entier i associe la position initiale du brin qui finit en position i . Cette permutation est invariante par isotopie des diagrammes, et on obtient donc une application bien définie $\pi_n : B_n \rightarrow \mathfrak{S}_n$. On vérifie que π_n est un homomorphisme de groupe, surjectif mais non injectif puisque, par construction, $\pi_n(\sigma_i)$ est la transposition, notée s_i , qui échange i et $i + 1$, et est d'ordre 2. On vérifie que le groupe \mathfrak{S}_n admet, en termes des transpositions s_i , la présentation

$$(2.15) \quad \mathfrak{S}_n = \left\langle s_1, \dots, s_{n-1} \mid s_i^2 = 1 \text{ et } \begin{array}{l} s_j s_i = s_i s_j \quad \text{pour } j \geq i + 2 \\ s_j s_i s_j = s_i s_j s_i \quad \text{pour } j = i + 1 \end{array} \right\rangle.$$

Les résultats sont les mêmes pour B_∞ et le groupe \mathfrak{S}_∞ formé des permutations de $\mathbb{N}_{>0}$ finalement égales à l'identité, qui admet la présentation

$$(2.16) \quad \mathfrak{S}_\infty = \left\langle s_1, s_2, \dots \mid s_i^2 = 1 \text{ et } \begin{array}{l} s_j s_i = s_i s_j \quad \text{pour } j \geq i + 2 \\ s_j s_i s_j = s_i s_j s_i \quad \text{pour } j = i + 1 \end{array} \right\rangle.$$

Quand, partant du groupe de tresses parenthésées, on projette de même les générateurs σ_i sur des éléments s_i d'ordre 2, c'est-à-dire quand on remplace σ_i par s_i et qu'on ajoute les relations $s_i^2 = 1$ dans la présentation (2.13),

on obtient un nouveau groupe, noté \widehat{V} dans [11], qu'on peut voir soit comme une version « permutée » du groupe de Thompson F , soit comme une version « thompsonifiée », ou parenthésée, du groupe de permutations \mathfrak{S}_∞ . La présentation de \widehat{V} correspondante est donc

$$(2.17) \quad \widehat{V} = \left\langle \begin{array}{l} s_1, s_2, \dots \\ a_1, a_2, \dots \end{array} \middle| \begin{array}{l} (2.16) \\ (2.8) \end{array} + \begin{array}{l} a_j s_i = s_i a_j, \quad s_{j-1} a_i = a_i s_j \quad \text{pour } j \geq i + 2 \\ a_j s_i s_j = s_i a_i, \quad a_i s_j s_i = s_i a_j \quad \text{pour } j = i + 1 \end{array} \right\rangle.$$

Comme (2.17) est une présentation positive, elle définit aussi un monoïde :

$$(2.18) \quad \widehat{V}^+ = \left\langle \begin{array}{l} s_1, s_2, \dots \\ a_1, a_2, \dots \end{array} \middle| \begin{array}{l} (2.16) \\ (2.8) \end{array} + \begin{array}{l} a_j s_i = s_i a_j, \quad s_{j-1} a_i = a_i s_j \quad \text{pour } j \geq i + 2 \\ a_j s_i s_j = s_i a_i, \quad a_i s_j s_i = s_i a_j \quad \text{pour } j = i + 1 \end{array} \right\rangle^+.$$

À nouveau, on montre que le monoïde \widehat{V}^+ se plonge dans le groupe \widehat{V} , qui en est un groupe de fractions à droite, et que \widehat{V} est produit de Zappa-Szép des monoïdes F^+ et \mathfrak{S}_∞ (ce dernier étant un groupe) [11].

On associe aux éléments du monoïde \widehat{V}^+ des diagrammes semblables à ceux de la figure 4, à la différence près que les croisements ne sont plus orientés, c'est à dire qu'on ne distingue plus entre σ_i et σ_i^{-1} : les brins se croisent sans qu'il y ait un dessus et un dessous. La figure 5 illustre les relations mixtes entre permutations parenthésées.

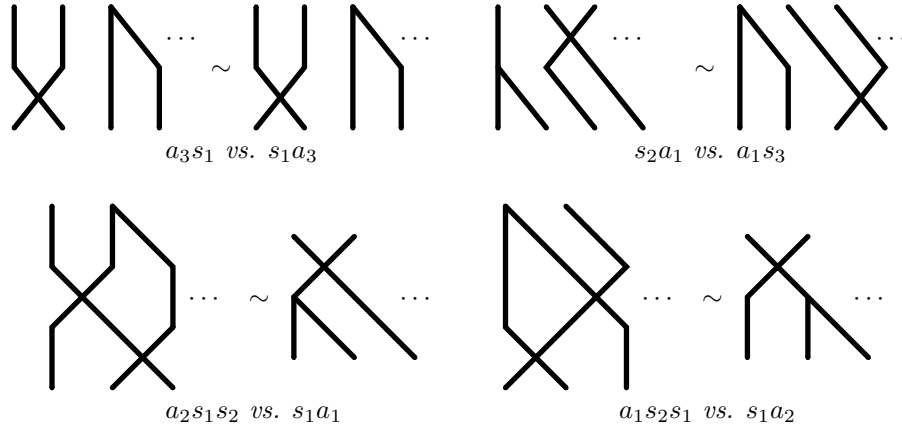


FIGURE 5. Les relations mixtes de permutations parenthésées : les diagrammes sont les mêmes que dans la figure 4, mais les croisements n'ont pas d'orientation.

3. Le monoïde H^+

On introduit ici à l'aide d'une présentation explicite le monoïde H^+ qui est l'objet principal de ce travail. Ensuite, l'examen des relations de la présentation permet d'établir directement plusieurs propriétés.

La section est divisée en trois sous-sections. Dans la section 3.1, on introduit H^+ à partir d'une présentation syntaxiquement proche de celles de B_∞^+

et de F^+ . Dans la section 3.2, on associe à chaque mot de l'alphabet Θ considéré divers paramètres numériques sur lesquels des récurrences pourront être fondées, et qui donnent quelques premiers résultats faciles : noethérianité du monoïde, finitude du nombre de représentants d'un élément, décidabilité du problème de mots. Dans la section 3.3 enfin, on établit un lien simple de projection entre le monoïde H^+ et le monoïde de Thompson, et on conclut avec quelques-unes des questions pour la suite.

3.1. Présentation par générateurs et relations.

DÉFINITION 3.1 (**monoïde H^+**). On pose

$$(3.2) \quad H^+ := \left\langle \theta_1, \theta_2, \dots \left| \begin{array}{ll} \theta_j \theta_i = \theta_i \theta_{j+1} & \text{pour } j \geq i + 2 \\ \theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{i+3} & \text{pour } j = i + 1 \end{array} \right. \right\rangle^+.$$

On note Θ l'ensemble $\{\theta_i \mid i \geq 1\}$, et $R_{\mathcal{P}}$ l'ensemble des relations de (3.2) ; les relations $\theta_j \theta_i = \theta_i \theta_{j+1}$ sont dites *de type 2*, et les relations $\theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{i+3}$ sont dites *de type 3*. On note (\mathcal{P}) la présentation (3.2), c'est-à-dire le couple $(\Theta, R_{\mathcal{P}})$, et $\equiv_{\mathcal{P}}$, ou simplement \equiv , la congruence sur Θ^* engendrée par $R_{\mathcal{P}}$.

Plusieurs propriétés résultent directement de la forme des relations de (\mathcal{P}) . On rappelle que, pour tout mot w , la longueur de w , c'est-à-dire le nombre de lettres de w , est notée $|w|$ (définition 1.1).

LEMME 3.3. *L'application « longueur » de Θ^* dans \mathbb{N} induit un homomorphisme de H^+ vers $(\mathbb{N}, +)$.*

DÉMONSTRATION. Chacune des relations de (\mathcal{P}) consiste en deux mots de même longueur. À partir de là, une induction sur le nombre d'étapes de dérivation montre que $u \equiv v$ entraîne $|u| = |v|$. Par conséquent, pour tout a dans H^+ , tous les Θ -mots représentant a ont la même longueur, donc la longueur induit une application bien définie de H^+ dans \mathbb{N} . Par construction, l'application ainsi définie est un homomorphisme de H^+ dans $(\mathbb{N}, +)$ puisque, si u représente a et v représente b , alors uv représente ab . \square

Il est donc loisible de parler de la longueur d'un élément de H^+ :

DÉFINITION 3.4 (**longueur**). Pour a dans H^+ , on note $|a|$ la valeur commune des longueurs $|w|$ pour w mot de Θ^* représentant a .

Le proposition 1.22 implique directement :

PROPOSITION 3.5 (**noethérianité**). *Le monoïde H^+ est noethérien : il n'existe pas de suite infinie strictement décroissante pour la division à gauche, ni pour la division à droite. L'élément 1 est le seul élément inversible de H^+ , et les atomes de H^+ sont les éléments θ_i avec $i \geq 1$.*

On rappelle que la non-existence d'élément inversible non trivial entraîne que les relations de divisibilité à gauche et à droite de H^+ sont des ordres partiels.

Une autre propriété lisible sur la liste de $R_{\mathcal{P}}$ est l'invariance par translation des indices.

PROPOSITION 3.6 (décalage). *L'application « décalage » de Θ dans lui-même qui envoie θ_i sur θ_{i+1} , pour tout i , induit un endomorphisme de H^+ .*

DÉMONSTRATION. Notons dec l'application « décalage » sur Θ . Puisque Θ^* est un monoïde libre de base Θ , l'application dec se prolonge en un homomorphisme

$$\text{dec}^* : \Theta^* \longrightarrow H^+.$$

Maintenant, on trouve

$$\text{dec}^*(\theta_j\theta_i) = \theta_{j+1}\theta_{i+1} = \theta_{i+1}\theta_{j+2} = \text{dec}^*(\theta_i\theta_{j+1}) \text{ pour } j > i + 1,$$

$$\text{dec}^*(\theta_j\theta_i\theta_j) = \theta_{j+1}\theta_{i+1}\theta_{j+1} = \theta_{i+1}\theta_{j+1}\theta_{j+3} = \text{dec}^*(\theta_i\theta_j\theta_{j+2}) \text{ pour } j = i + 1.$$

Ainsi, pour toute relation $u = v$ de $R_{\mathcal{P}}$, on a $\text{dec}^*(u) = \text{dec}^*(v)$. De là, il résulte que $u \equiv v$ entraîne $\text{dec}^*(u) \equiv \text{dec}^*(v)$. Donc dec^* induit une application bien définie de H^+ dans lui-même, qui, par construction, est un endomorphisme du monoïde H^+ . \square

NOTATION 3.7 (décalage). Pour a dans H^+ , on note $\text{dec}(a)$ l'image de a par l'endomorphisme de décalage de la proposition 3.6.

3.2. Paramètres numériques. Pour étudier les générateurs pouvant apparaître dans les expressions d'un élément du monoïde H^+ , on va définir plusieurs paramètres numériques, les principaux étant appelés la *hauteur*, le *plafond*, et l'*aire*. Bien que les relations ne laissent pas les valeurs de ceux-ci invariantes, on peut souvent donner des bornes explicites. Comme première application, on montre que chaque élément de H^+ n'admet qu'un nombre fini d'expressions, et, de là, que le problème de mots est décidable.

Le premier paramètre numérique naturel attaché à un mot est sa longueur, et on a vu ci-dessus qu'il induit un paramètre bien défini sur le monoïde H^+ . Il sera utile d'introduire d'autres paramètres. Le suivant contrôle les indices des lettres :

DÉFINITION 3.8 (hauteur). On appelle *support* d'un mot w de Θ^* l'ensemble $\text{Supp}(w)$ des entiers i tels que θ_i apparaît dans w . La *hauteur* de w est alors le maximum du support, soit

$$(3.9) \quad \text{ht}(w) := \max(\text{Supp}(w)) = \max\{i \mid \theta_i \text{ apparaît dans } w\}.$$

Par exemple, le support du mot $\theta_6\theta_1\theta_2$ est l'ensemble $\{1, 2, 6\}$, et sa hauteur est 6.

Dans toute la suite, pour $p \leq q$ entiers, on note $\{p, \dots, q\}$ l'intervalle $\{i \in \mathbb{Z} \mid p \leq i \leq q\}$ — parfois aussi noté $\llbracket p, q \rrbracket$. Alors, pour tout mot w , la définition implique immédiatement la relation parfois utile

$$(3.10) \quad \text{Supp}(w) \subseteq \{1, \dots, \text{ht}(w)\}.$$

Comme les relations de Thompson de (2.8), mais contrairement aux relations de tresses de (2.2), les relations de (\mathcal{P}) ne préservent pas les indices

des générateurs apparaissant dans des mots, et, comme on l'a vu, ni le support, ni la hauteur ne sont invariants pour \equiv . Par exemple, on peut vérifier qu'il existe deux autres mots équivalents au mot $\theta_6\theta_1\theta_2$ considéré ci-dessus, à savoir $\theta_1\theta_7\theta_2$, de hauteur 7, et $\theta_1\theta_2\theta_8$, de hauteur 8 : la hauteur est un paramètre lié à un Θ -mot, pas à un élément de H^+ , qui est une classe d'équivalence de Θ -mots.

Le paramètre suivant est du même type, mais on verra que lui est laissé invariant par les relations de (\mathcal{P}) .

DÉFINITION 3.11 (plafond). Pour w mot dans Θ^* , on définit le *plafond* $\lceil w \rceil$ de w par $\lceil \varepsilon \rceil = 0$ et, pour $w = \theta_{i_1}\theta_{i_2}\cdots\theta_{i_\ell}$,

$$(3.12) \quad \lceil w \rceil := \max\{i_p + \ell - p \mid p = 1, \dots, \ell\}.$$

Par exemple, le plafond de $\theta_6\theta_1\theta_3\theta_7\theta_2$ (qui est de hauteur 7) est

$$10 = \max\{6 + 4, 1 + 3, 3 + 2, 7 + 1, 2 + 0\}.$$

LEMME 3.13. (i) *Pour tout mot w de Θ^* , on a*

$$(3.14) \quad \text{ht}(w) \leq \lceil w \rceil \leq \text{ht}(w) + |w| - 1.$$

(ii) *Si les indices des lettres de w forment une suite strictement croissante, alors $\lceil w \rceil$ est l'indice de la dernière lettre, et on a $\lceil w \rceil = \text{ht}(w)$.*

DÉMONSTRATION. Le point (i) résulte immédiat des définitions. Pour (ii), on écrit $w = \theta_{i_1}\cdots\theta_{i_\ell}$ avec $i_1 < \cdots < i_\ell$. Alors les nombres $i_p + \ell - p$ forment une suite croissante au sens large, et sa borne supérieure est la dernière valeur, soit $i_\ell + \ell - \ell = i_\ell$. \square

L'intérêt d'introduire ici le plafond vient du résultat suivant :

LEMME 3.15. *Si w et w' sont des mots de Θ^* représentant le même élément de H^+ , on a $\lceil w \rceil = \lceil w' \rceil$.*

DÉMONSTRATION. Il suffit de montrer le résultat dans le cas où w' est obtenu à partir de w en appliquant une relation de $R\mathcal{P}$.

Supposons d'abord $w = u\theta_i\theta_{i+1}\theta_{i+3}v$ et $w' = u\theta_{i+1}\theta_i\theta_{i+1}v$ avec $|v| = \ell$. Pour $\lceil w \rceil$, la contribution de u est $\lceil u \rceil + \ell + 3$, celle de v est $\lceil v \rceil$, et celle de $\theta_i\theta_{i+1}\theta_{i+3}$ est

$$\max(i + 2 + \ell, (i + 1) + 1 + \ell, (i + 3) + \ell),$$

soit $i + 3 + \ell$, d'où, finalement,

$$\lceil w \rceil = \max(\lceil u \rceil + \ell + 3, i + 3 + \ell, \lceil v \rceil).$$

Un calcul analogue pour $\lceil w' \rceil$ donne pour $\theta_{i+1}\theta_i\theta_{i+1}$ la contribution

$$\max((i + 1) + 2 + \ell, i + 1 + \ell, (i + 2) + \ell),$$

soit à nouveau $i + 3 + \ell$, et on déduit

$$\lceil w' \rceil = \max(\lceil u \rceil + \ell + 3, i + 3 + \ell, \lceil v \rceil) = \lceil w \rceil.$$

Supposons maintenant $w = u\theta_j\theta_i v$ et $w' = u\theta_i\theta_{j+1}v$, avec $j \geq i + 2$ et, à nouveau, $|v| = \ell$. Pour $\lceil w \rceil$, la contribution de u est $\lceil u \rceil + \ell + 2$, celle de v est $\lceil v \rceil$, et celle de $\theta_j\theta_i$ est $\max(j+1+\ell, i+\ell)$, soit $j+1+\ell$, d'où, finalement,

$$\lceil w \rceil = \max(\lceil u \rceil + \ell + 2, j + 1 + \ell, \lceil v \rceil).$$

Un calcul analogue pour $\lceil w' \rceil$ donne pour $\theta_i\theta_{j+1}$ la contribution

$$\max(i + 1 + \ell, (j + 1) + \ell),$$

soit à nouveau $j + 1 + \ell$, et on déduit

$$\lceil w' \rceil = \max(\lceil u \rceil + \ell + 2, j + 1 + \ell, \lceil v \rceil) = \lceil w \rceil. \quad \square$$

Du coup, il est naturel de poser :

DÉFINITION 3.16 (plafond). Pour a dans H^+ , on note $\lceil a \rceil$ la valeur commune de $\lceil w \rceil$ pour w mot de Θ^* représentant a .

Alors, (3.14) implique immédiatement

PROPOSITION 3.17 (bornes hauteur). Pour tout mot w de Θ^* représentant un élément a de H^+ , on a

$$(3.18) \quad \lceil a \rceil - |a| + 1 \leq \text{ht}(w) \leq \lceil a \rceil.$$

Une application importante des résultats précédents est qu'ils permettent de résoudre le problème de mots du monoïde H^+ :

PROPOSITION 3.19 (problème de mots I). Le problème de mots pour la présentation (\mathcal{P}) du monoïde H^+ est décidable.

DÉMONSTRATION. Pour chaque mot w de Θ^* , la classe d'équivalence de w vis-à-vis de \equiv est finie : en effet, $w' \equiv w$ implique d'une part $|w'| = |w|$ et, d'autre part, $\text{Supp}(w') \subseteq \{1, \dots, \lceil w \rceil\}$, et le nombre de mots vérifiant ces deux conditions est borné supérieurement par $\lceil w \rceil^{|w|}$.

Par conséquent, partant de deux mots w, w' de Θ^* , on peut décider s'ils sont \equiv -équivalents en partant de w et en appliquant autant que faire se peut les relations de (\mathcal{P}) jusqu'à ce qu'aucun mot nouveau n'apparaisse plus : à ce moment-là, on a énuméré complètement la classe de w , et il suffit de regarder si le mot w' apparaît dans la liste ainsi construite. \square

Pour terminer, on note que l'application « plafond » n'est pas un homomorphisme, mais on obtient facilement une formule la reliant au produit :

PROPOSITION 3.20 (produit). Pour tous a, b dans H^+ , on a

$$(3.21) \quad \lceil ab \rceil = \max(\lceil a \rceil + |b|, \lceil b \rceil).$$

DÉMONSTRATION. Soit $\theta_{i_1} \dots \theta_{i_\ell}$ représentant a et $\theta_{j_1} \dots \theta_{j_m}$ représentant b . On trouve

$$\begin{aligned} \lceil ab \rceil &= \max(\max\{i_p + \ell + m - p \mid p = 1, \dots, \ell\}, \max\{j_q + m - q \mid q = 1, \dots, m\}) \\ &= \max(\max\{i_p + \ell - p \mid p = 1, \dots, \ell\} + m, \max\{j_q + m - q \mid q = 1, \dots, m\}) \\ &= \max(\lceil a \rceil + |b|, \lceil b \rceil). \quad \square \end{aligned}$$

En termes de diviseurs, la proposition 3.20 implique immédiatement :

COROLLAIRE 3.22 (diviseur). *Chacune des relations $a \preceq b$ (« a divise b à gauche ») et $b \succcurlyeq a$ (« a divise b à droite ») implique $[a] \leq [b]$.*

Sur le modèle du plafond, on peut aussi introduire la notion symétrique de *plancher* en posant, pour tout Θ -mot w ,

$$[w] := \inf\{i \mid \theta_i \text{ apparaît dans } w\},$$

et montrer que $[w]$ est invariant par les relations de (\mathcal{P}) . Les propriétés du plancher sont en général triviales, et, n'étant pratiquement pas utilisées dans la suite, on peut les omettre ici. La seule application où la notion de plancher apparaît commode est la démonstration de l'injectivité de l'application « décalage » :

PROPOSITION 3.23 (décalage II). *L'endomorphisme de décalage sur H^+ est injectif.*

DÉMONSTRATION. Soit Θ_2 l'ensemble des éléments θ_i avec $i \geq 2$, et soit H_2^+ le sous-monoïde de H^+ engendré par Θ_2 . L'invariance du plancher par \equiv implique qu'aucune expression d'un élément de H_2^+ ne peut contenir le générateur θ_1 . Par conséquent, deux mots de Θ_2^* sont $\equiv_{\mathcal{P}}$ -équivalents si, et seulement si, ils sont équivalents modulo les relations de (\mathcal{P}) n'impliquant pas θ_1 , et donc H_2^+ admet comme présentation Θ_2 muni de ces relations. Alors le même argument que pour la proposition 3.6 montre que l'application $\overline{\text{dec}}$ de Θ_2 dans Θ qui envoie θ_i sur θ_{i-1} pour $i \geq 2$ induit un homomorphisme de H_2^+ dans H^+ . Celui-ci est, par construction, une rétraction pour $\overline{\text{dec}}$, qui est donc injective. \square

On introduit pour terminer un dernier paramètre numérique mesurant les mots de Θ^* :

DÉFINITION 3.24 (aire). Pour w mot dans Θ^* , l'*aire* de w est la somme des indices des lettres de w , soit $\mathbf{a}(\varepsilon) := 0$ et, pour $w = \theta_{i_1}\theta_{i_2}\cdots\theta_{i_\ell}$,

$$(3.25) \quad \mathbf{a}(w) := i_1 + i_2 + \cdots + i_\ell.$$

Noter que, par construction, on a toujours

$$\mathbf{a}(w) \leq |w| \cdot \text{ht}(w).$$

La figure 6 récapitule les différents paramètres numériques attachés aux mots en les lettres θ_i .

3.3. Lien avec le monoïde de Thompson. Une autre propriété découlant directement de la forme des relations de la présentation (\mathcal{P}) est l'existence d'un lien direct avec le monoïde F^+ . En effet, les relations de (\mathcal{P}) de type 2 *sont* des relations de la présentation (2.8), et on va voir que les relations de type 3 en sont des conséquences :

PROPOSITION 3.26 (projection). *L'application $\pi : \theta_i \mapsto a_i$ induit un homomorphisme surjectif du monoïde H^+ sur le monoïde de Thompson F^+ .*

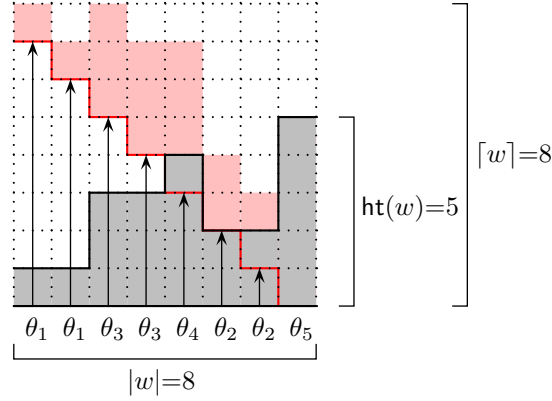


FIGURE 6. Les différents paramètres attachés à un mot de Θ^* , ici $w := \theta_1^2 \theta_3^2 \theta_4 \theta_2^2 \theta_5$: un rectangle gris de hauteur i est attaché à chaque lettre θ_i . La largeur du diagramme est $|w|$, sa hauteur est $\lceil w \rceil$, le plafond $\lceil w \rceil$ est la hauteur quand les rectangles sont translétés (en rose), et l'aire est le nombre de carrés gris sous la courbe, ici 21.

DÉMONSTRATION. Soit π^* l'extension de π en un homomorphisme du monoïde libre Θ^* dans le monoïde F^+ . Comme d'habitude, il s'agit de montrer que $w \equiv w'$ implique $\pi^*(w) = \pi^*(w')$, et il suffit de le vérifier quand (w, w') est une des relations de (\mathcal{P}) . Le cas des relations de type 2 est trivial puisque celles-ci sont des relations de la présentation (2.8). Considérons une relation de type 3, par exemple, $\theta_2 \theta_1 \theta_2 = \theta_1 \theta_2 \theta_4$. On trouve dans F^+

$$\pi^*(\theta_2 \theta_1 \theta_2) = a_2 a_1 a_2 = a_1 a_3 a_2 = a_1 a_2 a_4 = \pi^*(\theta_1 \theta_2 \theta_4).$$

Donc π^* induit un homomorphisme de H^+ dans F^+ . Celui-ci est surjectif puisque, par construction, chacun des générateurs a_i est dans l'image. \square

Dans toute la suite, on notera π la projection de H^+ sur F^+ ainsi obtenue. Il est facile de montrer que π n'est pas injective : par exemple, chacun des deux éléments $\theta_2 \theta_1$ et $\theta_1 \theta_3$ n'admet qu'une seule expression, car aucune relation de $R_{\mathcal{P}}$ ne peut être appliquée et, dans H^+ , on a donc $\theta_2 \theta_1 \neq \theta_1 \theta_3$. Par contre, dans F^+ , on trouve

$$\pi(\theta_2 \theta_1) = a_2 a_1 = a_1 a_3 = \pi(\theta_1 \theta_3).$$

On a expliqué dans la section 2.2 comment associer à tout élément du monoïde F^+ un arbre binaire fini — ou plutôt, dans le formalisme adapté ici, une forêt (ensemble d'arbres) — qui le spécifie. Par composition, on peut donc associer à tout élément de H^+ une telle forêt. Mais, comme l'application π n'est pas bijective, on ne peut espérer que la forêt ainsi associée spécifie l'élément de H^+ dont il vient. On étudiera au chapitre VI la question naturelle de savoir si la représentation de H^+ par forêt peut être amendée pour devenir bijective.

Des questions pour la suite. Au terme des observations précédentes, toutes plus ou moins évidentes au vu des relations de (\mathcal{P}) , de nombreuses questions concernant le monoïde H^+ restent ouvertes :

- Le monoïde H^+ est-il simplifiable à droite et à gauche ?
- Le monoïde H^+ admet-il des ppcm et des pgcd ?
- Le monoïde H^+ admet-il, comme le monoïde de tresses B_∞^+ , une structure de Garside ; existe-t-il une plus petite famille de Garside, que dire de la forme normale associée, etc. ?
- Les éléments du monoïde H^+ admettent-ils, comme ceux du monoïde de Thompson F^+ , une représentation fidèle par forêt ?
- Le monoïde H^+ se plonge-t-il dans le groupe H défini par la présentation (\mathcal{P}) ?

Ces questions sont l'objet des chapitres qui suivent.

Chapitre II

Utilisation de la réécriture

Faire l'analyse d'un monoïde (ou un groupe, ou toute autre structure algébrique), dont une famille de générateurs est identifiée, repose souvent sur la définition, si cela est possible, d'un représentant distingué, ou forme normale, parmi les divers mots en les générateurs représentant un élément. Il existe plusieurs méthodes pour construire des formes normales, parmi lesquelles les systèmes de réécriture et les formes normales liées à une famille de Garside. Dans le cas du monoïde H^+ , on verra que chacune de ces deux approches peut être utilisée pour définir une forme normale. On commence dans ce chapitre avec l'approche « système de réécriture », l'approche « Garside » sera développée dans le chapitre V.

Ce chapitre assez bref est organisé en trois sections. Dans la section 1, on rappelle le contexte général des règles de réécriture pour l'étude d'un monoïde présenté, et le critère de convergence basé sur la confluence locale et la noethérianité. Dans la section 2, on étudie comme illustration et premier exemple facile, le cas de la présentation I.2.8 du monoïde F^+ et on montre qu'elle est associée à un système convergent. Enfin, dans la section 3, on traite de même le cas du monoïde H^+ à partir de la présentation donnée en (\mathcal{P}) . On montre à nouveau la convergence du système de réécriture associé, et on utilise la forme normale ainsi obtenue pour démontrer un résultat de simplifiabilité conditionnelle, à savoir que, *si* le monoïde H^+ est simplifiable à gauche, alors il est aussi simplifiable à droite.

1. Systèmes de réécriture

On rappelle d'abord la procédure générale pour associer un système de réécriture à une présentation de monoïde et le critère de convergence classique par vérification de la noethérianité et de la confluence locale (section 1.1). Ensuite, on traite soigneusement le cas du monoïde F^+ (section 2.1).

1.1. Réécriture associée à une présentation. Un *système de réécriture* sur un ensemble X est simplement une relation binaire sur X , c'est-à-dire un ensemble de couples de $X \times X$. Nous allons considérer ici des systèmes de réécriture sur des ensembles de mots S^* . Si \mathcal{E} est un système de réécriture sur S^* , on écrira en général $w \rightarrow_{\mathcal{E}} w'$, ou simplement $w \rightarrow w'$, lu « w se réécrit en w' en une étape » pour $(w, w') \in \mathcal{E}$. On notera alors $\Rightarrow_{\mathcal{E}}$ (ou \Rightarrow) la clôture réflexive-transitive de $\rightarrow_{\mathcal{E}}$: on a donc $w \Rightarrow_{\mathcal{E}} w'$ s'il existe une suite

finie (w_0, \dots, w_m) vérifiant $w_0 = w$, $w_m = w'$ et $w_i \rightarrow_{\mathcal{E}} w_{i+1}$ pour $0 \leq i < m$. Dans ce cas, on dit que w est \mathcal{E} -réductible à w' .

On associe à chaque présentation de monoïde (S, R) une famille de systèmes de réécriture comme suit. On rappelle que, dans une présentation de monoïde, une relation est une paire (non ordonnée) de mots $\{u, v\}$ — notée en général $u = v$.

DÉFINITION 1.1 (réécriture associée). Supposons que (S, R) est une présentation de monoïde. Une *orientation* de R est une liste \vec{R} de couples de mots telle que, pour toute paire $\{u, v\}$ dans R , exactement un des deux couples (u, v) , (v, u) est dans \vec{R} , et \vec{R} ne contient que ces couples. Le système de réécriture *associé* à (S, \vec{R}) est alors l'ensemble $\mathcal{E}(S, \vec{R})$ de tous les couples $(w_1 u w_2, w_1 v w_2)$ pour w_1, w_2 dans S^* et (u, v) dans \vec{R} .

On dira qu'un système de réécriture \mathcal{E} est *associé* à une présentation (non orientée) (S, R) s'il existe une orientation \vec{R} de R telle que \mathcal{E} est le système associé à (S, \vec{R}) . Choisir une orientation pour une présentation (S, R) , c'est choisir, pour chaque relation, une direction de gauche à droite ou de droite à gauche. Une présentation à n relations a donc 2^n orientations, et il existe donc 2^n systèmes de réécriture associés.

EXEMPLE 1.2. Considérons la présentation (I.2.8) du monoïde de Thompson F^+ . La présentation a une infinité de relations, et il existe donc une infinité d'orientations possibles. Dans la suite, on considèrera l'orientation définie par le choix

$$(1.3) \quad a_i a_{j+1} \rightarrow a_j a_i \quad \text{pour } j \geq i + 1,$$

et on notera \mathcal{E}_F le système de réécriture associé. Une suite typique de réécritures pour \mathcal{E}_F est la suite de mots

$$a_1^2 a_3 a_4 a_2 \rightarrow a_1 a_2 a_1 a_4 a_2 \rightarrow a_1 a_2 a_3 a_1 a_2.$$

On note que le dernier mot est \mathcal{E}_F -réduit : aucune réécriture ultérieure ne peut lui être appliqué.

Comme on l'a rappelé dans la section I.1.1, si (S, R) est une présentation de monoïde, alors \equiv_R est la congruence sur S^* engendrée par les relations de R , qui est aussi la relation d'équivalence engendrée par les couples de mots de la forme $(w_1 u w_2, w_1 v w_2)$ avec $u = v$ dans R , de sorte qu'on a

$$\langle S \mid R \rangle^+ = S^* / \equiv_R.$$

Il existe une relation simple entre la relation \equiv_R et la réécriture associée à une orientation de (S, R) :

LEMME 1.4. *Si (S, R) est une présentation de monoïde et si \mathcal{E} est associé à \vec{R} , la relation \equiv_R est la clôture symétrique de la relation $\Rightarrow_{\mathcal{E}}$: pour tous w, w' dans S^* , la relation $w \equiv_R w'$ est satisfaite si, et seulement si, il existe une suite finie de mots (w_0, \dots, w_{2m}) vérifiant $w = w_0$, $w' = w_{2m}$, et $w_{2i} \Rightarrow_{\mathcal{E}} w_{2i-1}$ et $w_{2i} \Rightarrow_{\mathcal{E}} w_{2i+1}$ pour tout i .*

Autrement dit, deux mots w, w' sont \equiv_R -équivalents s'il existe un zigzag de réécritures et de réécritures inversées reliant w à w' :

$$\begin{array}{ccccccc}
 w = w_0 & & w_2 & & w_4 & & \dots & & w_{2m} = w' \\
 & \searrow & & \swarrow & & \searrow & & \swarrow & \\
 & & w_1 & & w_3 & & \dots & & w_{2m-1}
 \end{array}$$

DÉMONSTRATION. Supposons que \mathcal{E} est associé à l'orientation \vec{R} de R . Notons $w \bowtie w'$ pour « il existe un zigzag du type ci-dessus reliant w et w' ». D'abord $w \bowtie w'$ entraîne $w \equiv_R w'$ car, si (w_0, \dots, w_{2m}) relie w à w' , on a $w_i \equiv_R w_{i+1}$ pour tout i , d'où $w_0 \equiv_R w_{2m}$ par transitivité de \equiv_R . Dans l'autre sens, il résulte de la définition que la relation \bowtie est une relation d'équivalence, et qu'elle est compatible avec la multiplication à gauche et à droite, puisque c'est le cas de la relation $\Rightarrow_{\mathcal{E}}$. Donc \bowtie est une congruence sur S^* . D'autre part, $u \Rightarrow_{\mathcal{E}} v$, donc aussi $u \bowtie v$ est vérifié pour tout couple (u, v) de \vec{R} . Puisque, par définition, \equiv_R est la plus petite congruence sur S^* qui inclue R , donc aussi \vec{R} , on déduit que \equiv_R est incluse dans \bowtie , c'est-à-dire que $w \equiv_R w'$ entraîne $w \bowtie w'$. Donc, finalement, $w \equiv_R w'$ équivaut à $w \bowtie w'$. \square

REMARQUE 1.5. On a associé ci-dessus des systèmes de réécriture (en général multiples) à toute présentation (S, R) . Mais, inversement, il existe bien de nombreux systèmes de réécriture qui ne proviennent pas de présentations orientées. En effet, si \mathcal{E} provient d'une présentation, alors, par définition, $w \Rightarrow_{\mathcal{E}} w'$ entraîne $w_1 w w_2 \Rightarrow_{\mathcal{E}} w_1 w' w_2$ pour tous w_1, w_2 . Donc, si un système de réécriture \mathcal{E} ne satisfait pas cette compatibilité avec le produit, il ne peut provenir d'une présentation. Par exemple, supposons $S = \{\mathbf{a}, \mathbf{b}\}$ et soit \mathcal{E} l'ensemble des couples $(\mathbf{a}w, \mathbf{b}w)$ pour w dans S^* : on peut réécrire \mathbf{a} en \mathbf{b} , mais seulement pour une lettre \mathbf{a} en position initiale. On a alors $\mathbf{a} \Rightarrow_{\mathcal{E}} \mathbf{b}$, mais pas $\mathbf{b}\mathbf{a} \Rightarrow_{\mathcal{E}} \mathbf{b}\mathbf{b}$, et \mathcal{E} ne peut provenir d'une présentation.

1.2. Convergence. Si \mathcal{E} est un système de réécriture sur S^* , un mot w de S^* est dit \mathcal{E} -réduit (ou \mathcal{E} -irréductible) s'il n'est \mathcal{E} -réductible à aucun mot w' distinct de w . Le cas qui va nous intéresser ici est celui où \mathcal{E} est convergent :

DÉFINITION 1.6 (**convergent**). Un système de réécriture \mathcal{E} sur S^* est *convergent* si, pour tout mot w , il existe un unique mot \mathcal{E} -réduit w' tel que w est \mathcal{E} -réductible à w' ; dans ce cas, le mot w' est noté $\text{red}_{\mathcal{E}}(w)$, ou simplement $\text{red}(w)$.

LEMME 1.7. *Supposons que \mathcal{E} est un système de réécriture associé à une présentation de monoïde (S, R) , et que \mathcal{E} est convergent. Alors, pour tous w, w' dans S^* , la relation $w \equiv_R w'$ équivaut à $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$.*

DÉMONSTRATION. Supposons que \mathcal{E} est associé à l'orientation \vec{R} de R . D'abord $w \Rightarrow_{\mathcal{E}} w'$ entraîne $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$. En effet, par hypothèse, on a $w' \Rightarrow_{\mathcal{E}} \text{red}(w')$. Si on a $w \Rightarrow_{\mathcal{E}} w'$, on déduit par transitivité $w \Rightarrow_{\mathcal{E}} \text{red}_{\mathcal{E}}(w')$. D'un autre côté, on a $w \Rightarrow_{\mathcal{E}} \text{red}_{\mathcal{E}}(w)$. Comme, par hypothèse, $\text{red}_{\mathcal{E}}(w)$ et

$\text{red}_{\mathcal{E}}(w')$ sont \mathcal{E} -réduits, l'hypothèse d'unicité entraîne $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$. De là, par le lemme 1.4, on déduit que $w \equiv_R w'$ entraîne $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$.

Inversement, notons $w \bowtie w'$ la relation $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$. Puisque $\text{red}_{\mathcal{E}}$ est une fonction, \bowtie est une relation d'équivalence. Ensuite, \bowtie est compatible avec la multiplication à gauche et à droite. En effet, supposons $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$. Alors, pour tous w_1, w_2 , on a à la fois $w_1 w w_2 \Rightarrow_{\mathcal{E}} \text{red}_{\mathcal{E}}(w_1 w w_2)$ et

$$w_1 w w_2 \Rightarrow_{\mathcal{E}} w_1 \text{red}(w) w_2 \Rightarrow_{\mathcal{E}} \text{red}_{\mathcal{E}}(w_1 \text{red}_{\mathcal{E}}(w) w_2),$$

d'où, par unicité,

$$(1.8) \quad \text{red}_{\mathcal{E}}(w_1 w w_2) = \text{red}_{\mathcal{E}}(w_1 \text{red}_{\mathcal{E}}(w) w_2)$$

et, de même,

$$(1.9) \quad \text{red}_{\mathcal{E}}(w_1 w' w_2) = \text{red}_{\mathcal{E}}(w_1 \text{red}_{\mathcal{E}}(w') w_2).$$

De là, $\text{red}_{\mathcal{E}}(w) = \text{red}_{\mathcal{E}}(w')$ entraîne $\text{red}_{\mathcal{E}}(w_1 w w_2) = \text{red}_{\mathcal{E}}(w_1 w' w_2)$, et \bowtie est une congruence sur S^* . Enfin, si (u, v) est dans \vec{R} , on a $u \Rightarrow_{\mathcal{E}} v$ par définition, d'où $\text{red}_{\mathcal{E}}(u) = \text{red}_{\mathcal{E}}(v)$, c'est-à-dire $u \bowtie v$. Donc \bowtie inclut \vec{R} , donc R . Par conséquent, \bowtie inclut la congruence \equiv_R engendrée par R , c'est-à-dire que $w \bowtie w'$ entraîne $w \equiv_R w'$. \square

On déduit directement :

PROPOSITION 1.10 (forme normale). *Si un des systèmes de réécriture, soit \mathcal{E} , associés à une présentation (S, R) d'un monoïde M est convergent, alors les mots \mathcal{E} -réduits fournissent une forme normale unique pour les éléments de M .*

DÉMONSTRATION. Par le lemme 1.7, la classe d'équivalence d'un mot w par rapport à \equiv_R contient un et un seul mot \mathcal{E} -réduit, à savoir le mot $\text{red}_{\mathcal{E}}(w)$. \square

1.3. Noethérianité et confluence. Afin de pouvoir appliquer la proposition 1.10, on est confronté au problème de reconnaître quand un système de réécriture est ou non convergent. Le critère traditionnel est d'établir la possible confluence du système.

DÉFINITION 1.11 (confluence). Un système de réécriture \mathcal{E} sur X est dit *confluent* si, pour tous x, x', x'' dans X ,

$$(1.12) \quad (x \Rightarrow_{\mathcal{E}} x' \text{ et } x \Rightarrow_{\mathcal{E}} x'') \text{ entraîne } \exists x''' (x' \Rightarrow_{\mathcal{E}} x''' \text{ et } x'' \Rightarrow_{\mathcal{E}} x''').$$

De même, \mathcal{E} est dit *localement confluent* si, pour tous x, x', x'' dans X ,

$$(1.13) \quad (x \rightarrow_{\mathcal{E}} x' \text{ et } x \rightarrow_{\mathcal{E}} x'') \text{ entraîne } \exists x''' (x' \Rightarrow_{\mathcal{E}} x''' \text{ et } x'' \Rightarrow_{\mathcal{E}} x''').$$

En d'autres termes, \mathcal{E} est confluente (*resp.*, localement confluente) si tout demi-diagramme du type ci-dessous à gauche (*resp.*, à droite) peut être complété en un losange :



La différence est que, pour la confluence locale, on suppose que x se réécrit en x' et x'' en une étape, tandis que, pour la confluence générale, le nombre d'étapes est non limité. Il est évidemment plus facile d'établir la confluence locale que la confluence générale. Le point important est que, sous des conditions propices, les deux propriétés sont équivalentes.

DÉFINITION 1.14 (noéthérianité). Un système de réécriture \mathcal{E} est dit *noéthérien* s'il n'existe pas de suite infinie de réécritures non-triviales, c'est-à-dire pas de suite infinie a_0, a_1, \dots vérifiant $a_i \rightarrow_{\mathcal{E}} a_{i+1}$ pour tout i .

LEMME 1.15 (« diamond lemma »). [47] *Si \mathcal{E} est un système de réécriture noéthérien, les propriétés suivantes sont équivalentes :*

- (i) \mathcal{E} est convergent ;
- (ii) \mathcal{E} est confluente ;
- (iii) \mathcal{E} est localement confluente.

DÉMONSTRATION. On note X l'ensemble sur lequel \mathcal{E} agit. Supposons \mathcal{E} convergent, et supposons qu'on a $x \Rightarrow_{\mathcal{E}} x'$ et $x \Rightarrow_{\mathcal{E}} x''$. Alors on déduit $\text{red}_{\mathcal{E}}(x) = \text{red}_{\mathcal{E}}(x') = \text{red}_{\mathcal{E}}(x'')$, d'où $x' \Rightarrow_{\mathcal{E}} \text{red}_{\mathcal{E}}(x)$ et $x'' \Rightarrow_{\mathcal{E}} \text{red}_{\mathcal{E}}(x)$. Par conséquent, \mathcal{E} est confluente, il suffit de choisir $x''' := \text{red}_{\mathcal{E}}(x)$. Donc (i) entraîne (ii).

Il est clair que (ii) entraîne (iii), qui en est un cas particulier.

Supposons enfin \mathcal{E} noéthérien et localement confluente. Puisque la relation $\rightarrow_{\mathcal{E}}$ n'a pas de suite infinie, il est standard qu'il existe une application « rang » $\rho : X \rightarrow \mathbf{Ord}$ (les ordinaux) telle que $x \rightarrow_{\mathcal{E}} x'$ entraîne $\rho(x) > \rho(x')$, à savoir l'application définie par

$$\rho(x) := \begin{cases} 0 & \text{si } x \text{ est } \mathcal{E}\text{-réduit,} \\ \sup\{\rho(x') + 1 \mid x \rightarrow_{\mathcal{E}} x'\} & \text{sinon.} \end{cases}$$

On montre par induction sur l'ordinal α que, pour x vérifiant $\rho(x) = \alpha$, il existe un unique élément \mathcal{E} -réduit x' vérifiant $x \Rightarrow_{\mathcal{E}} x'$. Pour $\alpha = 0$, la seule possibilité est que x soit \mathcal{E} -réduit, et le résultat est vrai. Supposons $\alpha \geq 1$, et $\rho(x) = \alpha$. Comme α est non nul, il existe au moins un élément x' vérifiant $x \rightarrow_{\mathcal{E}} x'$. On a alors $\rho(x') < \alpha$, et l'hypothèse d'induction implique qu'il existe y' unique \mathcal{E} -réduit et vérifiant $x' \Rightarrow_{\mathcal{E}} y'$. On a donc aussi $x \Rightarrow_{\mathcal{E}} y'$. Si x' est le seul élément vérifiant $x \rightarrow_{\mathcal{E}} x'$, on a terminé. Sinon, soit x'' un autre élément vérifiant $x \rightarrow_{\mathcal{E}} x''$. Par confluence locale, il existe x''' vérifiant à la fois $x' \Rightarrow_{\mathcal{E}} x'''$ et $x'' \Rightarrow_{\mathcal{E}} x'''$, et on a $\rho(x''') < \alpha$ et $\rho(x''') < \alpha$.

Par hypothèse d'induction, il existe y'' et y''' uniques \mathcal{E} -réduits et vérifiant $x'' \Rightarrow_{\mathcal{E}} y''$ et $x''' \Rightarrow_{\mathcal{E}} y'''$. Alors x' se réduit à la fois à y' et à y''' , donc, par hypothèse d'induction, on a $y' = y'''$. De même, x'' se réduit à la fois à y'' et à y''' , donc, par hypothèse d'induction, on a $y'' = y'''$. Ceci montre que *tout* élément x'' obtenu en une étape à partir de x se réduit à y' , et donc que y' est l'unique élément \mathcal{E} -réduit auquel x se réduit. Donc \mathcal{E} est convergent, et (iii) implique (i). \square

Par conséquent, pour autant qu'on ait un système noethérien, il suffit d'établir la confluence locale pour déduire la convergence.

2. Le cas du monoïde de Thompson

Dans le cas des monoïdes de tresses, on sait que, même s'il existe des solutions au problème de mots basés sur des systèmes de réécriture, notamment liés à des bases de Gröbner-Shirshov [9], une approche directement basée sur l'orientation des relations d'une présentation ne peut pas fournir un système convergent [41].

Par contre, on va voir maintenant que la présentation (I.2.8) du monoïde de Thompson F^+ relève d'une approche par système de réécriture.

2.1. Le système \mathcal{E}_F .

NOTATION 2.1 (**système \mathcal{E}_F**). On pose $A := \{a_i \mid i \geq 1\}$, et on définit \mathcal{E}_F comme le système de réécriture sur A^* associé à la présentation (I.2.8) du monoïde F^+ via l'orientation

$$(2.2) \quad a_i a_j \rightarrow a_{j-1} a_i \quad \text{pour } i \geq 1 \text{ et } j \geq i + 2,$$

Le système \mathcal{E}_F est donc celui considéré dans l'exemple 1.2 (écrit ici avec $j - 1$ au lieu de j pour faciliter la lecture). On notera \rightarrow_F et \Rightarrow_F pour les relations associées à \mathcal{E}_F , voire \rightarrow et \Rightarrow si aucune ambiguïté n'est possible.

On va démontrer :

PROPOSITION 2.3 (**convergence**). *Le système \mathcal{E}_F est convergent.*

Au vu du lemme 1.15, il suffit, pour établir le résultat, de montrer que \mathcal{E}_F est à la fois noethérien et localement confluent. Les deux points sont faciles.

LEMME 2.4. *Le système \mathcal{E}_F est noethérien.*

DÉMONSTRATION. Pour w dans A^* , définissons inductivement un entier $\rho(w)$ par

$$(2.5) \quad \rho(\varepsilon) := 0 \quad \text{et} \quad \rho(w a_i) := \rho(w) + i :$$

autrement dit, $\rho(w)$ est la somme des indices des générateurs a_i figurant dans w (et donc l'équivalent de ce qu'on a appelé l'aire dans le cas des Θ -mots). Alors $w \rightarrow_F w'$ entraîne $\rho(w) > \rho(w')$. En effet, pour tous w_1, w_2 dans A^* , on trouve

$$\rho(w_1 a_i a_j w_2) = \rho(w_1) + \rho(w_2) + i + j$$

$$> \rho(w_1) + \rho(w_2) + i + j - 1 = \rho(w_1 a_{j-1} a_i w_2).$$

Comme l'ordre usuel de \mathbb{N} est bien fondé, il ne peut donc exister de suite infinie pour \rightarrow_F . \square

LEMME 2.6. *Le système \mathcal{E}_F est localement confluent.*

DÉMONSTRATION. Supposons $w \rightarrow_F w'$ et $w \rightarrow_F w''$. Par définition, w' et w'' sont obtenus à partir de w en remplaçant un facteur de longueur 2 de type $a_{j+1} a_i$ par le mot $a_i a_j$ correspondant.

Si les facteurs de longueur 2 impliqués dans les deux réductions coïcident, on obtient un témoin de confluence w''' en posant $w''' := w' = w''$. Si les facteurs de longueur 2 sont disjoints, les deux réductions commutent, et on obtient un témoin de confluence w''' en enchaînant (dans n'importe quel ordre) les deux réductions. Il reste le cas où les facteurs de longueur 2 se chevauchent, ce qui correspond à

$$w = w_1 a_i a_j a_k w_2, \quad w' = w_1 a_{j-1} a_i a_k w_2, \quad w'' = w_1 a_i a_{k-1} a_j w_2$$

avec $i \geq 1$, $j \geq i + 2$, et $k \geq j + 2$, donc $k \geq i + 4$. On trouve alors

$$\begin{array}{ccccc}
 & & w_1 a_{j-1} \underline{a_i a_k} w_2 & \longrightarrow & w_1 \underline{a_{j-1} a_{k-1}} a_i w_2 & & \\
 & \nearrow & & & & \searrow & \\
 w_1 \underline{a_i a_j} a_k w_2 & & & & & & w_1 a_{k-2} a_{j-1} a_i w_2 \\
 & \searrow & & & & \nearrow & \\
 & & w_1 a_i \underline{a_{k-1} a_j} w_2 & \longrightarrow & w_1 a_{k-2} \underline{a_i a_j} w_2 & &
 \end{array}$$

d'où le résultat pour $w''' := w_1 a_{k-2} a_{j-1} a_i w_2$. \square

La proposition 2.3 résulte alors directement du lemme 1.15.

Appliquant la proposition 1.10, on obtient un résultat de forme normale dans le monoïde de Thompson F^+ :

PROPOSITION 2.7 (**forme normale**). *Les mots \mathcal{E}_F -réduits fournissent une forme normale unique pour les éléments du monoïde F^+ .*

2.2. Les mots \mathcal{E}_F -réduits. Il est facile de caractériser les mots \mathcal{E}_F -réduits en termes de facteurs interdits.

DÉFINITION 2.8 (**éviter**). Si \mathcal{L} est un ensemble de mots de A^* , on dit qu'un mot w de A^* *évite* \mathcal{L} si aucun facteur de w n'appartient à \mathcal{L} .

On rappelle que, si v et w sont des mots, v est un *facteur* de w s'il existe w_1, w_2 vérifiant $w = w_1 v w_2$ (un facteur est un sous-mot formé de lettres consécutives).

Alors la définition du système de réécriture \mathcal{E}_F implique directement :

PROPOSITION 2.9 (**mots réduits**). *Soit*

$$\mathcal{I}_F := \{a_i a_j \mid i \geq 1 \text{ et } j \geq i + 2\}.$$

Alors un mot de A^ est \mathcal{E}_F -réduit si, et seulement si, il évite l'ensemble \mathcal{I}_F .*

On en déduit que le langage formé par les mots \mathcal{E}_F -réduits est « *quasi-régulier* » : à ceci près que l'alphabet A est infini, le langage est reconnu par le « *quasi-automate* » excluant les facteurs de longueur deux $a_i a_j$ avec $j \geq i+2$. Pour obtenir un énoncé précis, on peut se restreindre à un sous-alphabet fini, et énoncer :

COROLLAIRE 2.10 (régulier). *Pour tout n , l'intersection de l'ensemble des mots \mathcal{E}_F -réduits avec $\{a_1, \dots, a_n\}^*$ est un langage régulier.*

On termine par quelques remarques faciles sur le système \mathcal{E}_F . La première remarque est l'existence d'une stratégie simple permettant de construire de façon inductive la forme \mathcal{E}_F -réduite d'un mot : si w est un mot \mathcal{E}_F -réduit, on obtient la forme \mathcal{E}_F -réduite de wa_i en poussant a_i le plus possible vers la gauche. On commence par un résultat préparatoire.

LEMME 2.11. *Toute relation du type $wa_k = a_j w$ dans A^* implique $j = k$.*

DÉMONSTRATION. On montre l'implication par récurrence sur $|w|$. Pour $|w| = 0$, soit $w = \varepsilon$, l'hypothèse est $a_k = a_j$, et le résultat est vrai. Supposons $|w| \geq 1$. Comme les mots wa_k et $a_j w$ sont égaux, on a nécessairement que a_j est la première lettre de w , et que a_k est la dernière lettre de w . Donc il existe w' vérifiant $w = a_j w' a_k$. L'hypothèse $wa_k = a_j w$ s'écrit alors $a_j w' a_k a_k = a_j a_j w' a_k$, qui implique $w' a_k = a_j w'$ en retirant a_j à gauche et a_k à droite. Or on a $|w'| < |w|$, donc l'hypothèse de récurrence implique $j = k$. \square

PROPOSITION 2.12 (réduction). *Si w est un mot \mathcal{E}_F -réduit, alors, pour tout i , il existe une unique décomposition (w_1, w_2) de w telle que la forme réduite de wa_i est $w_1 a_j w_2$ avec $j = i - |w_2|$.*

DÉMONSTRATION. On montre l'existence par récurrence sur la longueur de w . Pour $|w| = 0$, on a $w = \varepsilon$ et le résultat est vrai pour $(w_1, w_2) = (\varepsilon, \varepsilon)$.

On suppose $|w| \geq 1$. Alors il existe un mot positif w' et un générateur a_k vérifiant $w = w' a_k$. Comme $w' a_k$ est \mathcal{E}_F -réduit, les seules relations de \mathcal{E}_F pouvant s'appliquer à $w' a_k a_i$ font nécessairement intervenir la lettre finale a_i .

Si on a $i \leq k + 1$, on ne peut appliquer aucune relation à $w' a_k a_i$. Donc le mot wa_i est \mathcal{E}_F -réduit et le résultat est vrai pour $(w_1, w_2) = (w, \varepsilon)$.

Supposons maintenant $i \geq k + 2$. On a $w' a_k a_i \rightarrow_F w' a_{i-1} a_k$. Or w' est \mathcal{E}_F -réduit, car c'est un facteur du mot \mathcal{E}_F -réduit w , et vérifie $|w'| < |w|$, donc on peut appliquer l'hypothèse de récurrence à w' . Ceci implique qu'il existe une décomposition $w' = w'_1 w'_2$ telle que la forme \mathcal{E}_F -réduite de $w' a_{i-1}$ est $w'_1 a_j w'_2$ avec $j = i - 1 - |w'_2|$. Or $w'_1 a_j w'_2$ est \mathcal{E}_F -réduit et $w'_2 a_k$ est \mathcal{E}_F -réduit car c'est un facteur du mot \mathcal{E}_F -réduit $w'_1 w'_2 a_k$. Donc le mot $w'_1 a_j w'_2 a_k$ est réduit puisqu'on a $j \geq k + 1 - |w'_2|$. Par conséquent, la forme \mathcal{E}_F -réduite de wa_i est $w'_1 a_j w'_2 a_k$ et la décomposition $(w_1, w_2) = (w'_1, w'_2 a_k)$ donne le résultat puisque $j = i - 1 - |w'_2| = i - |w_2|$.

Il reste à montrer l'unicité de la décomposition. Supposons qu'il existe deux décompositions (w_1, w_2) et (w'_1, w'_2) de w telle que la forme réduite de

wa_i est $w_1a_jw_2$ avec $j = i - |w_2|$ et $w'_1a_{j'}w'_2$ avec $j' = i - |w'_2|$. Supposons $j \neq j'$. On peut supposer $j < j'$. Alors, on obtient $|w_2| = i - j > i - j' = |w'_2|$ et, de là, $|w_1| < |w'_1|$. Donc w_1 est un préfixe de w'_1 et w'_2 est un suffixe de w_2 . On écrit $w'_1 = w_1a_jw''_1$. On trouve $w_1a_jw_2 = w'_1a_{j'}w'_2 = w_1a_jw''_1a_{j'}w'_2$, d'où $w_2 = w''_1a_{j'}w'_2$. Par conséquent, on a les égalités

$$w = w_1w_2 = w_1w''_1a_{j'}w'_2 = w'_1w'_2 = w_1a_jw''_1w'_2,$$

d'où $w''_1a_{j'} = a_jw''_1$. Par le lemme 2.11, on a une contradiction à $j \neq j'$ et on trouve $j = j'$. De là, on obtient $|w_2| = |w'_2|$, d'où $w_2 = w'_2$ et $w_1 = w'_1$. \square

Pour terminer, on note que l'existence de la fonction ρ de (2.5) permet de borner supérieurement le nombre de réécritures nécessaires pour transformer un mot quelconque en un mot réduit.

LEMME 2.13. *Si on a $w \Rightarrow_F w'$, alors toute suite de réductions de w à w' a pour longueur $\rho(w) - \rho(w')$.*

DÉMONSTRATION. Chaque réécriture de \mathcal{E}_F diminue la valeur de la fonction ρ d'exactly une unité. Il faut donc exactement ℓ réécritures pour passer d'un mot w à un mot w' vérifiant $\rho(w') = \rho(w) - \ell$. \square

PROPOSITION 2.14 (**nombre de réductions**). *Pour w dans A^* , posons $N(w) := \rho(w) - \rho(\text{red}_F(w))$. Alors toute suite de \mathcal{E}_F -réductions menant de w à $\text{red}_F(w)$ a pour longueur $N(w)$, et on a $N(w) \leq \binom{|w|}{2}$.*

DÉMONSTRATION. Le lemme 2.13 implique directement que le nombre de réductions de w à $\text{red}_F(w)$ est égal à $\rho(w) - \rho(\text{red}_F(w))$.

On montre que ce nombre est au plus $\binom{|w|}{2}$ par induction sur $|w|$. Pour $|w| \leq 1$, le résultat est clair. Supposons $|w| \geq 2$. Écrivons $w = w_0a_k$. On a alors $w \Rightarrow_F \text{red}_F(w_0)a_k \Rightarrow_F \text{red}_F(w)$. Par hypothèse de récurrence, le nombre de réductions de w_0 à $\text{red}_F(w_0)$ est au plus $\binom{|w_0|}{2}$. Il reste à réduire $\text{red}_F(w_0)a_k$ en $\text{red}_F(w)$. La proposition 2.7 montre que ceci se fait en poussant a_k vers la gauche autant que faire se peut, donc en au plus $|w_0|$ étapes. Le nombre maximal de réductions de w à $\text{red}_F(w)$ est donc borné supérieurement par $\binom{|w_0|}{2} + |w_0| - 1$, c'est-à-dire par $\binom{|w|}{2}$. \square

3. Le cas du monoïde H^+

On développe maintenant une approche similaire pour le monoïde H^+ , en partant de la présentation (\mathcal{P}) .

3.1. Le système \mathcal{E}_H . On commence par définir un système de réécriture sur Θ^* associé à la présentation (\mathcal{P}) .

NOTATION 3.1 (**système \mathcal{E}_H**). On pose $\Theta := \{\theta_i \mid i \geq 1\}$, et on définit \mathcal{E}_H comme le système de réécriture sur Θ^* associé à la présentation (\mathcal{P}) du monoïde H^+ via l'orientation

$$(3.2) \quad \theta_i\theta_j \rightarrow \theta_{j-1}\theta_i \quad \text{pour } i \geq 1 \text{ et } j \geq i + 3,$$

$$(3.3) \quad \theta_i\theta_{i+1}\theta_{i+3} \rightarrow \theta_{i+1}\theta_i\theta_{i+1} \quad \text{pour } i \geq 1.$$

On notera \rightarrow_H et \Rightarrow_H pour les relations associées à \mathcal{E}_H , voire \rightarrow et \Rightarrow si aucune ambiguïté n'est possible.

Noter que les réécritures (3.2) sont des réécritures du système \mathcal{E}_F , mais on n'a pas (au changement de nom près) $\mathcal{E}_F \subseteq \mathcal{E}_H$ puisque les réécritures $\theta_i\theta_{i+2} \rightarrow \theta_{i+1}\theta_i$ sont absentes de \mathcal{E}_H , et on n'a pas non plus $\mathcal{E}_H \subseteq \mathcal{E}_F$ puisque les réécritures $\theta_i\theta_{i+1}\theta_{i+3} \rightarrow \theta_{i+1}\theta_i\theta_{i+1}$ sont absentes de \mathcal{E}_F . Néanmoins, on peut écrire (toujours au remplacement de a_i par θ_i près)

$$\theta_i\theta_{i+1}\theta_{i+3} \rightarrow_F \theta_i\theta_{i+2}\theta_{i+1} \rightarrow_F \theta_{i+1}\theta_i\theta_{i+1},$$

d'où $\theta_i\theta_{i+1}\theta_{i+3} \Rightarrow_F \theta_{i+1}\theta_i\theta_{i+1}$. De là, une induction immédiate donne

PROPOSITION 3.4 (projection). *Soit π l'isomorphisme de Θ^* sur A^* envoyant θ_i sur a_i pour tout i . Alors, pour tout mot w de Θ^* ,*

$$(3.5) \quad w \Rightarrow_H w' \text{ entraîne } \pi(w) \Rightarrow_F \pi(w').$$

Plus précisément, $w \xrightarrow{m}_H w'$ entraîne $\pi(w) \xrightarrow{p}_F \pi(w')$ avec $m \leq p \leq 2m$.

Comme dans la section 2.1, on va démontrer :

PROPOSITION 3.6 (convergence). *Le système \mathcal{E}_H est convergent.*

Au vu du lemme 1.15, il suffit, pour établir le résultat, de montrer que \mathcal{E}_H est à la fois noethérien et localement confluent. Le premier point est facile.

LEMME 3.7. *Le système \mathcal{E}_H est noethérien.*

DÉMONSTRATION. L'argument est le même que pour \mathcal{E}_F . Pour w dans Θ^* , on a défini au chapitre I l'aire de w par

$$(3.8) \quad \mathbf{a}(\varepsilon) := 0 \quad \text{et} \quad \mathbf{a}(w\theta_i) = \mathbf{a}(w) + i :$$

autrement dit, $\mathbf{a}(w)$ est la somme des indices des générateurs θ_i présents dans w . Alors $w \rightarrow_H w'$ entraîne $\mathbf{a}(w) > \mathbf{a}(w')$. En effet, pour tous w_1, w_2 dans Θ^* , on trouve pour $j \geq i + 3$

$$\begin{aligned} \mathbf{a}(w_1\theta_i\theta_j w_2) &= \mathbf{a}(w_1) + \mathbf{a}(w_2) + i + j \\ &> \mathbf{a}(w_1) + \mathbf{a}(w_2) + i + j - 1 = \mathbf{a}(w_1\theta_{j-1}\theta_i w_2). \end{aligned}$$

Par ailleurs, on trouve

$$\begin{aligned} \mathbf{a}(w_1\theta_i\theta_{i+1}\theta_{i+3} w_2) &= \mathbf{a}(w_1) + \mathbf{a}(w_2) + 3i + 4 \\ &> \mathbf{a}(w_1) + \mathbf{a}(w_2) + 3i + 2 = \mathbf{a}(w_1\theta_{i+1}\theta_i\theta_{i+1} w_2). \end{aligned}$$

Comme l'ordre usuel de \mathbb{N} est bien fondé, il ne peut donc exister de suite infinie pour \rightarrow_H . \square

REMARQUE 3.9. Au lieu de faire une démonstration directe pour \mathcal{E}_H , on peut aussi utiliser la noethérianité de \mathcal{E}_F et l'existence de la projection π de la proposition 3.4 : une suite infinie pour \rightarrow_H entraînerait une suite infinie pour \rightarrow_F , qu'on sait ne pouvoir exister.

LEMME 3.10. *Le système \mathcal{E}_H est localement confluent.*

DÉMONSTRATION. Le principe est le même que dans le cas du système \mathcal{E}_F . On suppose donc qu'on a $w \rightarrow_H w'$ et $w \rightarrow_H w''$, et on essaie de construire un réduit commun pour w' et w'' . Comme plus haut, les cas où les facteurs, ici de longueur 2 ou 3, mis en jeu sont ou bien égaux, ou bien disjoints, sont triviaux. Il s'agit donc d'étudier les cas où les facteurs en question ont au moins une lettre en commun et ne sont pas égaux. Pour alléger les calculs, on omet les préfixes et suffixes qui n'interviennent pas dans les réductions. Il y a quatre cas à étudier selon que les deux réécritures concernées sont de type (3.2) ou (3.3).

Cas 1 : deux fois (3.2). Alors on a $w = \theta_i \theta_j \theta_k$ avec $j \geq i + 3$ et $k \geq j + 3$. On trouve alors

$$\begin{array}{ccccc} & & \theta_{j-1} \theta_i \theta_k & \longrightarrow & \theta_{j-1} \theta_{k-1} \theta_i \\ & \nearrow & & & \searrow \\ \theta_i \theta_j \theta_k & & & & \theta_{k-2} \theta_{j-1} \theta_i \\ & \searrow & & & \nearrow \\ & & \theta_i \theta_{k-1} \theta_j & \longrightarrow & \theta_{k-2} \theta_i \theta_j \end{array}$$

d'où la confluence pour $w''' := \theta_{k-2} \theta_{j-1} \theta_i$.

Cas 2 : deux fois (3.3). La seule position possible des facteurs correspond alors à $w = \theta_i \theta_{i+1} \theta_{i+3} \theta_{i+4} \theta_{i+6}$. On trouve alors

$$\begin{array}{ccccccc} & & & & \theta_{i+1} \theta_i \theta_{i+3} \theta_{i+1} \theta_{i+6} & \longrightarrow & \theta_{i+1} \theta_{i+2} \theta_i \theta_{i+1} \theta_{i+6} & \longrightarrow & \theta_{i+1} \theta_{i+2} \theta_i \theta_{i+5} \theta_{i+1} \\ & & & & \nearrow & & & & \searrow \\ & & & & \theta_{i+1} \theta_i \theta_{i+1} \theta_{i+4} \theta_{i+6} & & & & \theta_{i+1} \theta_{i+2} \theta_{i+4} \theta_i \theta_{i+1} \\ & \nearrow & & & & & & & \searrow \\ \theta_i \theta_{i+1} \theta_{i+3} \theta_{i+4} \theta_{i+6} & & & & & & & & \theta_{i+2} \theta_{i+1} \theta_{i+2} \theta_i \theta_{i+1} \\ & \searrow & & & & & & & \nearrow \\ & & & & \theta_i \theta_{i+1} \theta_{i+4} \theta_{i+3} \theta_{i+4} & & & & \theta_{i+2} \theta_{i+1} \theta_i \theta_{i+3} \theta_{i+1} \\ & & & & \searrow & & & & \nearrow \\ & & & & \theta_i \theta_{i+3} \theta_{i+1} \theta_{i+3} \theta_{i+4} & \longrightarrow & \theta_{i+2} \theta_i \theta_{i+1} \theta_{i+3} \theta_{i+4} & \longrightarrow & \theta_{i+2} \theta_{i+1} \theta_i \theta_{i+1} \theta_{i+4} \end{array}$$

d'où la confluence pour $w''' := \theta_{i+2} \theta_{i+1} \theta_{i+2} \theta_i \theta_{i+1}$.

Cas 3 : une fois (3.2) puis une fois (3.3). La seule possibilité est alors $w = \theta_i \theta_j \theta_{j+1} \theta_{j+3}$ avec $j \geq i + 3$. On trouve alors

$$\begin{array}{ccccccc} & & & & \theta_{j-1} \theta_i \theta_{j+1} \theta_{j+3} & \longrightarrow & \theta_{j-1} \theta_j \theta_i \theta_{j+3} & \longrightarrow & \theta_{j-1} \theta_j \theta_{j+2} \theta_i \\ & & & & \nearrow & & & & \searrow \\ & & & & \theta_i \theta_j \theta_{j+1} \theta_{j+3} & & & & \theta_j \theta_{j-1} \theta_j \theta_i \\ & \searrow & & & & & & & \nearrow \\ & & & & \theta_i \theta_{j+1} \theta_j \theta_{j+1} & \longrightarrow & \theta_j \theta_i \theta_j \theta_{j+1} & \longrightarrow & \theta_j \theta_{j-1} \theta_i \theta_{j+1} \end{array}$$

d'où la confluence pour $w''' := \theta_j \theta_{j-1} \theta_j \theta_i$.

Cas 4 : une fois (3.3) puis une fois (3.2). La seule possibilité est alors $w = \theta_i \theta_{i+1} \theta_{i+3} \theta_j$ avec $j \geq i + 6$. On trouve alors

$$\begin{array}{ccccccc}
 & & \theta_{i+1} \theta_i \theta_{i+1} \theta_j & \longrightarrow & \theta_{i+1} \theta_i \theta_{j-1} \theta_{i+1} & \longrightarrow & \theta_{i+1} \theta_{j-2} \theta_i \theta_{i+1} \\
 & \nearrow & & & & & \searrow \\
 \theta_i \theta_{i+1} \theta_{i+3} \theta_j & & & & & & \theta_{j-3} \theta_{i+1} \theta_i \theta_{i+1} \\
 & \searrow & & & & & \nearrow \\
 & & \theta_i \theta_{i+1} \theta_{j-1} \theta_{i+3} & \longrightarrow & \theta_i \theta_{j-2} \theta_{i+1} \theta_{i+3} & \longrightarrow & \theta_{j-3} \theta_i \theta_{i+1} \theta_{i+3}
 \end{array}$$

d'où la confluence pour $w''' := \theta_{j-3} \theta_{i+1} \theta_i \theta_{i+1}$. La démonstration de confluence locale est donc complète. \square

Comme dans la section 2.1, la démonstration de la convergence du système \mathcal{E}_H en résulte, via le lemme du losange 1.15

Appliquant la proposition 1.10, on obtient un résultat de forme normale dans le monoïde H^+ :

PROPOSITION 3.11 (forme normale). *Les mots \mathcal{E}_H -réduits fournissent une forme normale unique pour les éléments du monoïde H^+ .*

NOTATION 3.12 (forme normale). Dans toute la suite, pour a dans le monoïde H^+ , on note $\text{NF}(a)$ l'unique mot \mathcal{E}_H -réduit de Θ^* représentant a .

REMARQUE 3.13. Si on considère d'autres choix d'orientations que celui de la définition (3.1), par exemple,

$$(3.14) \quad \theta_j \theta_i \rightarrow \theta_i \theta_{j+1} \quad \text{pour } i \geq 1 \text{ et } j \geq i + 2,$$

$$(3.15) \quad \theta_{i+1} \theta_i \theta_{i+1} \rightarrow \theta_i \theta_{i+1} \theta_{i+3} \quad \text{pour } i \geq 1,$$

ou bien

$$(3.16) \quad \theta_i \theta_j \rightarrow \theta_{j-1} \theta_i \quad \text{pour } i \geq 1 \text{ et } j \geq i + 3,$$

$$(3.17) \quad \theta_{i+1} \theta_i \theta_{i+1} \rightarrow \theta_i \theta_{i+1} \theta_{i+3} \quad \text{pour } i \geq 1,$$

ou bien

$$(3.18) \quad \theta_j \theta_i \rightarrow \theta_i \theta_{j+1} \quad \text{pour } i \geq 1 \text{ et } j \geq i + 2,$$

$$(3.19) \quad \theta_i \theta_{i+1} \theta_{i+3} \rightarrow \theta_{i+1} \theta_i \theta_{i+1} \quad \text{pour } i \geq 1,$$

alors les systèmes de réécritures résultant de ces choix d'orientation ne sont pas confluents. Par exemple, pour le choix de (3.14) et (3.15), on a à la fois $\theta_2 \theta_1 \theta_2 \theta_1 \theta_2 \Rightarrow \theta_1 \theta_1 \theta_2 \theta_4 \theta_6$ et $\theta_2 \theta_1 \theta_2 \theta_1 \theta_2 \Rightarrow \theta_2 \theta_1 \theta_1 \theta_2 \theta_4$ et les mots $\theta_1 \theta_1 \theta_2 \theta_4 \theta_6$ et $\theta_2 \theta_1 \theta_1 \theta_2 \theta_4$ sont réduits. Pour le choix de (3.16) et (3.17), on a $\theta_1 \theta_4 \theta_3 \theta_4 \Rightarrow \theta_3 \theta_1 \theta_3 \theta_4$ et $\theta_1 \theta_4 \theta_3 \theta_4 \Rightarrow \theta_1 \theta_3 \theta_4 \theta_6$ et les mots $\theta_3 \theta_1 \theta_3 \theta_4$ et $\theta_1 \theta_3 \theta_4 \theta_6$ sont réduits. Pour le choix de (3.18) et (3.19), on a $\theta_3 \theta_1 \theta_2 \theta_4 \Rightarrow \theta_1 \theta_2 \theta_5 \theta_4$ et $\theta_3 \theta_1 \theta_2 \theta_4 \Rightarrow \theta_3 \theta_2 \theta_1 \theta_2$ et les mots $\theta_1 \theta_2 \theta_5 \theta_4$ et $\theta_3 \theta_2 \theta_1 \theta_2$ sont réduits.

3.2. Les mots \mathcal{E}_H -réduits. Comme dans le cas du système \mathcal{E}_F , il est facile de caractériser les mots \mathcal{E}_H -réduits en termes de facteurs interdits. En effet, la définition du système de réécriture \mathcal{E}_H implique directement :

PROPOSITION 3.20 (**mots réduits**). *Posons*

$$(3.21) \quad \mathcal{I} := \{\theta_i\theta_j \mid i \geq 1 \text{ et } j \geq i + 3\} \cup \{\theta_i\theta_{i+1}\theta_{i+3} \mid i \geq 1\}.$$

Alors, un mot de Θ^* est \mathcal{E}_H -réduit si, et seulement si, il évite l'ensemble \mathcal{I} .

On en déduit que le langage formé par les mots \mathcal{E}_H -réduits est « quasi-régulier » [4] : à ceci près que l'alphabet Θ est infini, le langage est reconnu par le « quasi-automate » excluant les facteurs de \mathcal{I} , lesquels sont de longueur bornée 2 ou 3. Sur le modèle du corollaire 2.10, on peut énoncer

COROLLAIRE 3.22 (**régulier**). *Pour tout n , l'intersection de l'ensemble des mots \mathcal{E}_H -réduits avec $\{\theta_1, \dots, \theta_n\}^*$ est un langage régulier.*

Pour le cas général, on peut définir une représentation de Θ^* utilisant un alphabet fini comme suit :

DÉFINITION 3.23 (**code, complexité**). Pour $i \geq 1$, on note $\text{code}(\theta_i)$ le mot de longueur $\lceil \log_2(i) \rceil + 2$ formé de la lettre θ et de la suite des deux lettres $_0$ et $_1$ formant le développement binaire de i . On définit le code d'un Θ -mot $\theta_{i_1} \dots \theta_{i_\ell}$ comme la concaténation des codes de ses lettres, et la *complexité* $\|w\|$ de w comme la longueur du mot $\text{code}(w)$.

EXEMPLE 3.24. Le code du mot $\theta_3\theta_1\theta_{12}$ est (avec des virgules de séparation entre les lettres) le mot $\theta_{,1,1}, \theta_{,1}, \theta_{,1,0,1,0}$, de longueur 10. La complexité du mot $\|\theta_3\theta_1\theta_{12}\|$ est donc 10.

Alors le critère de la proposition 3.20 entraîne l'existence d'un algorithme qui, partant du code d'un mot w de Θ^* , décide en temps linéaire si w est ou non \mathcal{E}_H -réduit. On peut donc énoncer précisément— voir par exemple [14] :

COROLLAIRE 3.25 (**complexité**). *L'ensemble des codes des mots \mathcal{E}_H -réduits de Θ^* est décidable de complexité $O(\|w\|)$.*

(On a bien entendu un résultat semblable dans le cas du monoïde de Thompson F^+ et du système de réécriture \mathcal{E}_F .)

De la caractérisation de la proposition 3.20, on déduit immédiatement les conséquences suivantes, souvent utilisées dans la suite :

COROLLAIRE 3.26 (**mots réduits**). (i) *Tout facteur d'un mot \mathcal{E}_H -réduit est \mathcal{E}_H -réduit.*

(ii) *Un mot de Θ^* est \mathcal{E}_H -réduit si, et seulement si, tous ses facteurs de longueur 3 sont \mathcal{E}_H -réduits.*

(iii) *Si uv et vw sont \mathcal{E}_H -réduits, alors uvw est \mathcal{E}_H -réduit, sauf si on est dans un des cas suivants :*

- $|v| = 0$, $u = u'\theta_i$ et $w = \theta_j w'$ avec $j \geq i + 3$,
- $|v| = 0$, $u = u'\theta_i$ et $w = \theta_{i+1}\theta_{i+3}w'$,
- $|v| = 0$, $u = u'\theta_i\theta_{i+1}$ et $w = \theta_{i+3}w'$,
- $|v| = 1$, $u = u'\theta_i$, $v = \theta_{i+1}$ et $w = \theta_{i+3}w'$.

DÉMONSTRATION. Seul le point (iii) mérite une démonstration. Il est clair que si on est dans les cas listés ci-dessus, alors uvw n'est pas réduit. Inversement, on suppose que uvw n'est pas réduit et on va montrer qu'on est forcément dans un des quatre cas ci-dessus. Comme uvw n'est pas réduit, on peut appliquer une réécriture de type (3.2) ou (3.3) à uvw . Supposons qu'on peut appliquer une réécriture de type (3.2) à uvw . Donc il existe deux mots u' et w' vérifiant $uvw = u'\theta_i\theta_jw'$ avec $j \geq i + 3$. Or $\theta_i\theta_j$ ne peut pas être un facteur de uv car uv est réduit. Pour la même raison, $\theta_i\theta_j$ n'est pas un facteur de vw . Donc θ_i est un suffixe de uv et θ_j est un préfixe de vw . Comme on a $i \neq j$, la seule possibilité est $|v| = 0$, $u = u'\theta_i$ et $w = \theta_jw'$.

Supposons maintenant qu'on peut appliquer une réécriture de type (3.3) à uvw . Donc il existe deux mots u' et w' vérifiant $uvw = u'\theta_i\theta_{i+1}\theta_{i+3}w'$. Pour les mêmes raisons que ci-dessus, $\theta_i\theta_{i+1}\theta_{i+3}$ ne peut pas être un facteur de uv ni de vw . Donc soit θ_i est un suffixe de uv et $\theta_{i+1}\theta_{i+3}$ est un préfixe de vw . Comme on a $i \neq i + 1$, on a, dans ce cas, $|v| = 0$, $u = u'\theta_i$ et $w = \theta_{i+1}\theta_{i+3}w'$. Soit $\theta_i\theta_{i+1}$ est un suffixe de uv et θ_{i+3} est un préfixe de vw . Comme on a $i + 1 \neq i + 3$, on a, dans ce cas, $|v| = 0$, $u = u'\theta_i\theta_{i+1}$ et $w = \theta_{i+3}w'$. Soit $\theta_i\theta_{i+1}$ est un suffixe de uv et $\theta_{i+1}\theta_{i+3}$ est un préfixe de vw . Comme on a $i \neq i + 3$, on a, dans ce cas, $|v| = 1$, $u = u'\theta_i$, $v = \theta_{i+1}$ et $w = \theta_{i+3}w'$. \square

Comme dans le cas de \mathcal{E}_F , on va maintenant montrer qu'il existe une stratégie simple permettant de construire de façon inductive la forme \mathcal{E}_H -réduite d'un mot : si w est un mot \mathcal{E}_H -réduit, on obtient la forme \mathcal{E}_H -réduite de $w\theta_i$ en poussant θ_i le plus possible vers la gauche. On commence par un résultat préparatoire.

LEMME 3.27. *Toute relation du type $w\theta_k = \theta_jw$ dans S^* implique $j = k$.*

DÉMONSTRATION. On montre l'implication par récurrence sur $|w|$. Pour $|w| = 0$, soit $w = \varepsilon$, l'hypothèse est $\theta_k = \theta_j$, et le résultat est vrai. Supposons $|w| \geq 1$. Comme les mots $w\theta_k$ et θ_jw sont égaux, on a nécessairement que θ_j est la première lettre de w , et que θ_k est la dernière lettre de w . Donc il existe w' vérifiant $w = \theta_jw'\theta_k$. L'hypothèse $w\theta_k = \theta_jw$ s'écrit alors $\theta_jw'\theta_k\theta_k = \theta_j\theta_jw'\theta_k$, qui implique $w'\theta_k = \theta_jw'$ en retirant θ_j à gauche et θ_k à droite. Or on a $|w'| < |w|$, donc l'hypothèse de récurrence implique $j = k$. \square

PROPOSITION 3.28 (**réduction**). *Si w est mot \mathcal{E}_H -réduit, alors, pour tout i , il existe une unique décomposition (w_1, w_2) de w telle que la forme réduite de $w\theta_i$ est $w_1\theta_jw_2$ avec $j = i - |w_2|$.*

DÉMONSTRATION. On montre l'existence par récurrence sur la longueur de w . Pour $|w| = 0$, on a $w = \varepsilon$ et le résultat est vrai pour $(w_1, w_2) = (\varepsilon, \varepsilon)$.

On suppose $|w| \geq 1$. Alors il existe un mot positif w' et un générateur θ_k vérifiant $w = w'\theta_k$. Comme $w'\theta_k$ est \mathcal{E}_H -réduit, les possibles réécritures de type (3.2) et (3.3) qui peuvent s'appliquer sur $w'\theta_k\theta_i$ font nécessairement intervenir la lettre θ_i .

Pour $i \leq k + 1$, on ne peut appliquer aucune réécriture de type (3.2) et (3.3) à $w'\theta_k\theta_i$. Donc le mot $w\theta_i$ est \mathcal{E}_H -réduit et le résultat est vrai pour $(w_1, w_2) = (w, \varepsilon)$.

Pour $i \geq k + 3$, on a $w'\theta_k\theta_i \rightarrow_H w'\theta_{i-1}\theta_k$. Or w' est \mathcal{E}_H -réduit et vérifie $|w'| < |w|$, donc on peut appliquer l'hypothèse de récurrence à w' . Ceci implique qu'il existe une décomposition $w' = w'_1w'_2$ telle que la forme réduite de $w'\theta_{i-1}$ est $w'_1\theta_jw'_2$ avec $j = i - 1 - |w'_2|$. Or $w'_1\theta_jw'_2$ est \mathcal{E}_H -réduit et $w'_2\theta_k$ est \mathcal{E}_H -réduit car c'est un facteur du mot \mathcal{E}_H -réduit $w'_1w'_2\theta_k$. Donc par le corollaire 3.26, le mot $w'_1\theta_jw'_2\theta_k$ est \mathcal{E}_H -réduit car $j \geq k + 2 - |w'_2|$. Par conséquent, la forme réduite de $w\theta_i$ est $w'_1\theta_jw'_2\theta_k$ et on a le résultat pour $(w_1, w_2) = (w'_1, w'_2\theta_k)$ car on a bien $j = i - 1 - |w'_2| = i - |w_2|$.

Il reste la possibilité $i = k + 2$. Pour $w' = \varepsilon$, on a $w\theta_i = \theta_{i-2}\theta_i$, qui est \mathcal{E}_H -réduit et on a le résultat pour $(w_1, w_2) = (w, \varepsilon)$. On suppose w' non vide. Alors il existe un mot positif w'' et un générateur θ_ℓ vérifiant $w' = w''\theta_\ell$.

Pour $\ell \neq i - 3$, on a $w\theta_i = w''\theta_\ell\theta_{i-2}\theta_i$ est \mathcal{E}_H -réduit car, par hypothèse, $w''\theta_\ell\theta_{i-2}$ est \mathcal{E}_H -réduit. Donc on a le résultat pour $(w_1, w_2) = (w, \varepsilon)$.

Pour $\ell = i - 3$, on a $w''\theta_{i-3}\theta_{i-2}\theta_i \equiv w''\theta_{i-2}\theta_{i-3}\theta_{i-2}$. Or w'' est \mathcal{E}_H -réduit et vérifie $|w''| < |w|$, donc on peut appliquer l'hypothèse de récurrence à w'' . Ceci implique qu'il existe une décomposition $w'' = w''_1w''_2$ telle que la forme réduite de $w''\theta_{i-2}$ est $w''_1\theta_jw''_2$ avec $j = i - 2 - |w''_2|$. Il reste à montrer que $w''_1\theta_jw''_2\theta_{i-3}\theta_{i-2}$ est \mathcal{E}_H -réduit. Or $w''_1\theta_jw''_2$ est \mathcal{E}_H -réduit et $w''_2\theta_{i-3}\theta_{i-2}$ est \mathcal{E}_H -réduit car c'est un facteur du mot \mathcal{E}_H -réduit $w''_1w''_2\theta_{i-3}\theta_{i-2}$. Donc par le corollaire 3.26, le mot $w''_1\theta_jw''_2\theta_{i-3}\theta_{i-2}$ est \mathcal{E}_H -réduit car $j = i - 2 - |w''_2|$. Par conséquent, la forme réduite de $w\theta_i$ est $w''_1\theta_jw''_2\theta_{i-3}\theta_{i-2}$ et on a le résultat pour $(w_1, w_2) = (w''_1, w''_2\theta_{i-3}\theta_{i-2})$ car on a bien $j = i - 2 - |w''_2| = i - |w_2|$.

Il reste à montrer l'unicité de la décomposition. Supposons qu'il existe deux décompositions (w_1, w_2) et (w'_1, w'_2) de w telle que la forme réduite de $w\theta_i$ est $w_1\theta_jw_2$ avec $j = i - |w_2|$ et $w'_1\theta_{j'}w'_2$ avec $j' = i - |w'_2|$. Supposons $j \neq j'$. On peut supposer $j < j'$. Alors, on obtient $|w_2| = i - j > i - j' = |w'_2|$ et, de là, $|w_1| < |w'_1|$. Donc w_1 est un préfixe de w'_1 et w'_2 est un suffixe de w_2 . On écrit $w'_1 = w_1\theta_jw''_1$. On trouve $w_1\theta_jw_2 = w'_1\theta_{j'}w'_2 = w_1\theta_jw''_1\theta_{j'}w'_2$, d'où $w_2 = w''_1\theta_{j'}w'_2$. Par conséquent, on a les égalités

$$w = w_1w_2 = w_1w''_1\theta_{j'}w'_2 = w'_1w'_2 = w_1\theta_jw''_1w'_2,$$

d'où $w''_1\theta_{j'} = \theta_jw''_1$. Par le lemme 3.27, on a une contradiction à $j \neq j'$ et on trouve $j = j'$. De là, on obtient $|w_2| = |w'_2|$, d'où $w_2 = w'_2$ et $w_1 = w'_1$. \square

EXEMPLE 3.29. Considérons le mot $w := \theta_1\theta_2\theta_4\theta_5\theta_7$. La normalisation mettant en pratique la stratégie de la proposition 3.28 consiste à partir de $w_0 := \varepsilon$, puis à normaliser $w_1 := \text{red}_H(w_0)\theta_1$, soit $w_1 = \theta_1$, parvenant à $\text{red}_H(\theta_1) = \theta_1$.

Ensuite, on normalise $w_2 := \text{red}_H(\theta_1)\theta_2$, soit $w_2 = \theta_1 \cdot \theta_2$, parvenant à $\text{red}_H(\theta_1\theta_2) = \theta_1\theta_2$: on ne peut pas pousser θ_2 à travers θ_1 .

Ensuite, on normalise $w_3 := \text{red}_H(\theta_1\theta_2)\theta_4$, soit $w_3 = \theta_1\theta_2 \cdot \theta_4$, parvenant à $\text{red}_H(\theta_1\theta_2\theta_4) = \theta_2\theta_1\theta_2$: on a poussé θ_4 à travers $\theta_1\theta_2$, et il est devenu θ_2 .

Ensuite, on normalise $w_4 := \text{red}_H(\theta_1\theta_2\theta_4)\theta_5$, soit $w_4 = \theta_2\theta_1\theta_2 \cdot \theta_5$, parvenant à $\text{red}_H(\theta_1\theta_2\theta_4\theta_5) = \theta_2\theta_3\theta_1\theta_2$: on a poussé θ_5 à travers $\theta_1\theta_2$, et il est devenu θ_3 , mais on ne peut pas aller plus loin.

Enfin, on normalise $w_5 := \text{red}_H(\theta_1\theta_2\theta_4\theta_5)\theta_7$, soit $w_5 = \theta_2\theta_3\theta_1\theta_2 \cdot \theta_7$, parvenant à $\text{red}_H(\theta_1\theta_2\theta_4\theta_5\theta_7) = \theta_3\theta_2\theta_3\theta_1\theta_2$: on a poussé θ_7 à travers $\theta_2\theta_3\theta_1\theta_2$, et il est devenu θ_3 .

3.3. Applications. Une première application de la forme normale est de permettre de montrer que des éléments n'ont *pas* de multiple commun, en l'occurrence à gauche :

PROPOSITION 3.30 (pas de multiple commun). *Les éléments θ_1 et θ_2 , non plus que θ_1 et θ_3 , ou que θ_2 et θ_3 , n'ont pas de multiple commun à gauche.*

DÉMONSTRATION. Si a est un multiple à gauche de θ_1 , noté $a = b\theta_1$, alors on a $\text{NF}(a) = \text{NF}(b)\theta_1$, puisqu'il n'existe aucune relation de réécriture de la forme $\dots\theta_1 \rightarrow_H \dots$. De même, si a est un multiple à gauche de θ_2 (*resp.*, θ_3), noté $a = b\theta_2$ (*resp.*, $a = b\theta_3$), alors on a $\text{NF}(a) = \text{NF}(b)\theta_2$ (*resp.*, $\text{NF}(a) = \text{NF}(b)\theta_3$), puisqu'il n'existe aucune relation de réécriture de la forme $\dots\theta_2 \rightarrow_H \dots$ (*resp.*, $\dots\theta_3 \rightarrow_H \dots$). Donc il ne peut pas exister de multiple commun à gauche de θ_1 et θ_2 : sinon, la forme normale de ce multiple commun aurait à la fois θ_1 et θ_2 comme dernière lettre, ce qui est impossible. Pour les mêmes raisons, il n'existe pas de multiple commun à gauche entre θ_1 et θ_3 , ni entre θ_2 et θ_3 . \square

Parmi les questions ouvertes sur le monoïde H^+ , l'une des plus importantes est celle de la simplification, à gauche et à droite. Comme application de la forme normale déduite du système de réécriture \mathcal{E}_H , on va montrer ici un résultat de simplification conditionnel, qui déduit la simplifiabilité à droite de la simplifiabilité à gauche — mais n'établit, seul, aucune des deux. Dans ce qui suit, on écrit $\text{red}(w)$ pour $\text{red}_H(w)$.

PROPOSITION 3.31 (simplifiabilité conditionnelle). *S'il est simplifiable à gauche, alors le monoïde H^+ est aussi simplifiable à droite.*

DÉMONSTRATION. Dans toute la démonstration, on suppose que H^+ est simplifiable à gauche, et on cherche à établir la simplifiabilité à droite. Comme les atomes θ_i engendrent le monoïde H^+ , il suffit de montrer que, pour tout a, b dans H^+ , la relation $a\theta_i = b\theta_i$ implique $a = b$. Supposons donc que a et b sont dans H^+ et qu'on a $a\theta_i = b\theta_i$. Posons $u := \text{NF}(a)$ et $v := \text{NF}(b)$. Par la proposition 3.28, il existe des mots u_1, u_2, v_1, v_2 vérifiant

$$(3.32) \quad u = u_1u_2 \quad \text{et} \quad \text{red}(u\theta_i) = u_1\theta_ju_2 \quad \text{avec} \quad j = i - |u_2|,$$

$$(3.33) \quad v = v_1v_2 \quad \text{et} \quad \text{red}(v\theta_i) = v_1\theta_kv_2 \quad \text{avec} \quad k = i - |v_2|.$$

Par hypothèse, on a $a\theta_i = b\theta_i$, donc $\text{red}(u\theta_i) = \text{red}(v\theta_i)$, soit $u_1\theta_ju_2 = v_1\theta_kv_2$. On considère les différents cas possibles.

Supposons d'abord $j \neq k$. On peut supposer $j < k$. Alors, par (3.32) et (3.33), on obtient

$$|u_2| = i - j > i - k = |v_2| \quad \text{et, de là,} \quad |u_1| < |v_1|.$$

Donc u_1 est un préfixe propre de v_1 , et v_2 est un suffixe propre de v_1 . Le mot u_1 est préfixe strict de v_1 , donc $u_1\theta_j$ est préfixe (strict ou non) de v_1 et il existe un mot w vérifiant $v_1 = u_1\theta_jw$. On trouve $u_1\theta_ju_2 = u_1\theta_jw\theta_kv_2$, donc $u_2 = w\theta_kv_2$. Par conséquent, on a les égalités

$$u = u_1w\theta_kv_2, \quad v = u_1\theta_jwv_2 \quad \text{et} \quad \text{red}(u\theta_i) = \text{red}(v\theta_i) = u_1\theta_jw\theta_kv_2.$$

L'égalité $\text{red}(v\theta_i) = u_1\theta_jw\theta_kv_2$ entraîne en particulier $v\theta_i \equiv u_1\theta_jw\theta_kv_2$, soit $u_1\theta_jwv_2\theta_i \equiv u_1\theta_jw\theta_kv_2$. Comme on a supposé H^+ simplifiable à gauche, on déduit $v_2\theta_i \equiv \theta_kv_2$ en simplifiant $u_1\theta_jw$ à gauche. Par hypothèse, le mot u_1 est réduit, donc, par le corollaire 3.26(i), il en est de même de son suffixe θ_kv_2 . L'équivalence $v_2\theta_i \equiv \theta_kv_2$ entraîne donc $\text{red}_H(v_2\theta_i) = \theta_kv_2$, donc $v_2\theta_i \Rightarrow_H \theta_kv_2$ et, de là, $u\theta_i = u_1w\theta_kv_2\theta_i \Rightarrow_H u_1w\theta_k\theta_kv_2$. Or $u_1w\theta_k$ est réduit comme préfixe de u , qui est réduit, et $\theta_k\theta_k$ est réduit par définition. Le corollaire 3.26(iii) implique alors que $u_1w\theta_k\theta_k$ est réduit. D'un autre côté, θ_kv_2 est réduit comme suffixe de u_1 qui est réduit, donc, toujours par le corollaire 3.26(iii), le mot $\theta_k\theta_kv_2$ est réduit. Finalement, $u_1w\theta_k\theta_k$ et $\theta_k\theta_kv_2$ sont réduits, donc, par le corollaire 3.26(ii), $u_1w\theta_k\theta_kv_2$ est réduit. Les deux mots $u_1\theta_jw\theta_kv_2$ et $u_1w\theta_k\theta_kv_2$ sont donc réduits, et ils sont tous deux équivalents à $u\theta_i$, donc ils sont égaux : on a $u_1w\theta_k\theta_kv_2 = u_1\theta_jw\theta_kv_2$, d'où, en retirant le préfixe u_1 et le suffixe θ_kv_2 des deux côtés,

$$(3.34) \quad w\theta_k = \theta_jw.$$

Par le lemme 3.27, on déduit $j = k$, qui contredit l'hypothèse $j \neq k$.

Le seul cas possible est donc le cas $j = k$. Mais alors, de (3.32) et (3.33), on déduit $|u_2| = |v_2|$, d'où $u_2 = v_2$, et, de là, $u_1 = v_1$. Donc on a $u = v$, qui entraîne $a = b$. \square

REMARQUE 3.35. Dans la démonstration ci-dessus (comme en d'autres endroits), on utilise plusieurs fois la simplifiabilité dans le monoïde libre Θ^* , à savoir qu'une égalité de mots $su = sv$ entraîne $u = v$: celle-ci est triviale, puisqu'un élément de Θ^* n'est représenté que par un seul mot, à savoir lui-même. Par contre, ce qui est non trivial est la simplifiabilité dans le monoïde (non libre) H^+ , c'est-à-dire le fait qu'une équivalence $su \equiv_{\mathcal{P}} sv$ entraîne $u \equiv_{\mathcal{P}} v$.

Une autre application de la forme normale définie dans la section 3.1 est l'existence d'une nouvelle solution au problème de mots pour la présentation (\mathcal{P}) du monoïde H^+ , bien plus efficace que la solution « stupide » donnée dans la proposition I.3.19.

PROPOSITION 3.36 (**problème de mots II**). *Le problème de mot pour la présentation (\mathcal{P}) du monoïde H^+ est décidable.*

DÉMONSTRATION. Par la proposition 3.11, deux mots u, v de Θ^* représentent le même élément de H^+ si, et seulement si, les mots $\text{red}_H(u)$ et $\text{red}_H(v)$ coïncident. Or, le système \mathcal{E}_H est un ensemble récursif de règles de réécriture, et donc la fonction qui, à chaque mot u de Θ^* , associe $\text{red}_H(u)$ est une fonction calculable. \square

Si on veut évaluer la complexité algorithmique [14] de la solution au problème de mots ainsi obtenu, il faut pouvoir borner supérieurement le nombre d'étapes de réduction nécessaire pour déterminer les mots \mathcal{E}_H -réduits. Comme dans la section 2.1 pour les \mathcal{E}_F -réductions, on utilise le même paramètre que pour établir la noethérienité du système \mathcal{E}_H , à savoir l'aire.

LEMME 3.37. *Si on a $w \Rightarrow_H w'$, alors toute suite de réductions de w à w' a pour longueur au plus $\mathbf{a}(w) - \mathbf{a}(w')$.*

DÉMONSTRATION. L'argument est le même que pour \mathcal{E}_F , mais on a seulement une borne supérieure, car les réécritures de \mathcal{E}_H diminuent la valeur de ρ soit de 1, soit de 2. \square

PROPOSITION 3.38 (**nombre de réductions**). *Pour tout mot w de Θ^* , toute suite de réductions menant de w à $\text{red}_H(w)$ a une longueur bornée supérieurement par $\mathbf{a}(w) - \mathbf{a}(\text{red}_H(w))$ et par $\binom{|w|}{2}$.*

DÉMONSTRATION. Le lemme 3.37 implique directement que le nombre de réductions de w à $\text{red}_H(w)$ est borné supérieurement par $\mathbf{a}(w) - \mathbf{a}(\text{red}_H(w))$. Pour la borne par $\binom{|w|}{2}$, elle résulte de la proposition 3.28 exactement comme dans le cas de \mathcal{E}_F . \square

Il est facile de voir que les bornes supérieures ci-dessus sont atteintes : par exemple, il faut $\binom{\ell}{2}$ réécritures pour aller de $\theta_1\theta_4\theta_7 \cdots \theta_{3\ell+1}$ à sa forme réduite, qui est $\theta_{2\ell+1} \cdots \theta_5\theta_3\theta_1$.

On déduit que, pour un mot w comportant ℓ lettres de l'alphabet Θ , le nombre d'étapes de réductions nécessaire pour arriver à $\text{red}_H(w)$ est au plus $O(\ell^2)$. Au demeurant, ceci ne montre pas que la solution de la proposition 3.36 a une complexité quadratique : les indices des lettres θ_i sont des entiers non bornés, et, comme dans la définition 3.23, on se ramène par codage à un alphabet fini et on définit la complexité $\|w\|$ d'un Θ -mot w comme la longueur de son code. On peut alors énoncer :

PROPOSITION 3.39 (**complexité**). *La complexité de la solution au problème de mots donnée dans la proposition 3.36 est quadratique en temps, et linéaire en espace.*

DÉMONSTRATION. Supposons que w contient ℓ lettres et a pour complexité n . Par la proposition 3.38, la réduction de w en $\text{red}_H(w)$ requiert au plus ℓ^2 étapes. De plus — et c'est le point important — chaque réduction diminue la valeur de la masse et appliquer une règle à un facteur $\theta_i\theta_j$ avec θ_i et θ_j de complexités p et q ne fait apparaître que des lettres de complexité

au plus p et q , et, pour déterminer le résultat, il suffit de comparer les entiers i et j , donc de les lire une fois, ce qui se fait en temps $O(\max(p, q))$. Il en résulte que, quand on applique la stratégie de l'exemple 3.29 consistant à pousser vers la gauche les lettres du mot initial en partant de la dernière et en revenant vers le début lettre par lettre, et si on appelle $\theta_{i_1}, \dots, \theta_{i_\ell}$ les lettres de w , on rencontre au plus une fois chaque facteur $\theta_{i_p}\theta_{i_q}$ avec $p < q$ ou un facteur où les lettres ont été diminuées, et le coût total est borné supérieurement par la somme $\sum_{1 \leq p < q \leq \ell} \max(\|\theta_{i_p}\|, \|\theta_{i_q}\|)$, laquelle est bornée supérieurement par $(\sum_{1 \leq p \leq \ell} \|\theta_{i_p}\|)(\sum_{1 \leq q \leq \ell} \|\theta_{i_q}\|)$, donc par $O(\|w\|^2)$. \square

Dans toute la suite, on utilisera fréquemment la \mathcal{E}_H -réduction des Θ -mots et la forme \mathcal{E}_H -normale des éléments de H^+ . Pour alléger les notations, on fixe désormais

CONVENTION 3.40 (réduit, forme normale). Pour un mot w sur l'alphabet Θ , « w est réduit » signifie « w est \mathcal{E}_H -réduit », « $\text{red}(w)$ » signifie « $\text{red}_H(w)$ », « $w \Rightarrow w'$ » signifie « $w \Rightarrow_H w'$ », etc. Pour un élément a de H^+ , la « forme normale de a » signifie « la forme \mathcal{E}_H -normale de a », et *tutti quanti*.

La méthode du retournement de facteur

Étudier un monoïde ou un groupe par la méthode du chapitre II, c'est-à-dire en utilisant un système de réécriture est élémentaire et d'usage simple mais, de même que dans le cas des tresses et des monoïdes B_n^+ , cette approche semble insuffisante pour étudier complètement le monoïde H^+ introduit dans le chapitre I. On va donc utiliser pour cela une autre méthode, le retournement de facteur. Réminiscente des approches de Garside [38] et de Brieskorn et Saito [10], celle-ci a été développée depuis une vingtaine d'années pour étudier certains monoïdes présentés [18, 21, 25, 28]. Dans les cas favorables, elle permet notamment d'étudier les questions de simplifiabilité, d'existence de ppcm et de pgcd et de résolution du problème de mots.

Le problème pour appliquer la méthode de retournement à l'étude du monoïde H^+ est que la présentation de celui-ci est infinie et, surtout, qu'à la différence du cas de B_∞^+ par exemple, il n'existe pas toujours de multiples communs dans H^+ . Nous allons donc devoir généraliser les résultats antérieurs et, pour cela, revoir les démonstrations pour les étendre ou les préciser. Ce chapitre contient des résultats généraux qui n'ont rien à voir avec le cas spécifique de H^+ , et sont intéressants en soi pour l'étude des monoïdes par la méthode du retournement. Les deux principaux sont un nouveau critère de complétude qui étend strictement celui de l'article [20] (proposition 2.8), et un nouveau critère de terminaison qui n'avait jamais été explicité dans le cas sans multiple commun (proposition 3.18). Dans les deux cas, les démonstrations sont assez délicates.

Le chapitre est organisé comme suit. Dans la section 1, on rappelle les définitions de base concernant le retournement de facteur dans le cas des présentations complétées, avec notamment les critères classiques de complétude et de terminaison, ici donnés sans reprendre les démonstrations existantes. Dans la section 2, on énonce et on établit un nouveau critère de complétude pour le retournement basé sur l'utilisation d'un ensemble de mots clos par complément. La démonstration requiert de nombreux lemmes préparatoires. Enfin, dans la section 3, on étudie la terminaison du retournement, à nouveau en utilisant le passage par un ensemble de mots clos par complément. On obtient un nouveau critère, et, de là, un résultat de décidabilité dans certains cas favorables qui n'étaient pas couverts par les approches antérieures.

1. Le retournement de facteur

Tout comme la présentation (I.2.2) du monoïde B_∞^+ , la présentation (I.3.2) du monoïde H^+ a une propriété syntaxique simple, à savoir que, pour chaque paire de générateurs s, t , il existe au plus une relation de la forme $s... = t...$ dans la liste de relations considérées. Pour les présentations de ce type, une méthode, dite *retournement de facteur*, a été introduite, qui permet, dans les bons cas, d'étudier efficacement le monoïde associé.

Dans cette première partie, on rappelle les définitions et résultats de base relatifs au retournement de facteur. Les résultats sont présents dans la littérature, et on omettra les démonstrations quand elles sont un peu longues.

1.1. Suites et diagrammes de retournement. Le point de départ ici est la notion de présentation *complémentée à droite*. Dans une présentation de monoïde, on appelle ε -relation une relation du type $u = \varepsilon$ avec u non vide.

DÉFINITION 1.1 (complémentée). Une présentation de monoïde (S, R) est dite *complémentée à droite* si elle ne contient pas de ε -relations, et que, pour tous s, t dans S distincts, il existe au plus une relation de la forme $s... = t...$ et aucune relation de la forme $s... = s...$

On a bien entendu une notion symétrique de présentation *complémentée à gauche*. À l'occasion, on dira qu'une présentation est *complémentée* si elle est complémentée à droite et à gauche. Par exemple, la présentation (I.2.2) du monoïde B_∞^+ est complémentée (à droite et à gauche), et il en est de même de la présentation (I.2.8) du monoïde F^+ , et de la présentation (I.3.2) du monoïde H^+ .

Pour décrire la méthode du retournement, on a besoin de la notion de mot *signé* sur un alphabet S .

DÉFINITION 1.2 (mot signé). Pour S non vide, on appelle S -mot *signé* un mot sur l'alphabet $S \cup \bar{S}$, où \bar{S} est la copie de S obtenue en prenant, pour chaque élément s de S , une copie notée \bar{s} de s . Les lettres de S (*resp.*, \bar{S}) sont dites positives (*resp.*, négatives) et un mot est dit positif (*resp.*, négatif) s'il ne contient que des lettres positives (*resp.*, négatives). Si u est un mot positif $s_1 \cdots s_r$, on définit \bar{u} comme étant le mot négatif $\bar{s}_r \cdots \bar{s}_1$.

Dans toute la suite, nous réservons en principe s, t pour les lettres de l'alphabet S considéré, u, v, u', v' pour les S -mots positifs et w, w' pour les S -mots signés. On rappelle qu'un mot u est un *facteur* de w s'il existe des mots v et v' vérifiant $w = vuv'$.

DÉFINITION 1.3 (retournement I). Soit (S, R) une présentation complémentée à droite et w, w' des S -mots signés. Le mot w se *retourne à droite en w' en une étape*, noté $w \curvearrowright_R^1 w'$, si on peut obtenir w' depuis w :

- soit en supprimant un facteur $\bar{s}s$ avec $s \in S$,
- soit en remplaçant un facteur $\bar{s}t$ avec $s, t \in S$ par le mot $u\bar{v}$ (avec $u, v \in S^*$) s'il existe une relation $su = tv$ dans R .

Puisqu'on considère une présentation complétée à droite, pour deux lettres s et t distinctes, il existe au plus une relation $s... = t...$ et aucune relation $s... = s...$. Donc il n'y a qu'une façon de retourner un facteur $\bar{s}t$ quand c'est possible.

EXEMPLE 1.4. Considérons la présentation

$$(1.5) \quad (\mathbf{a, b, c} \mid \mathbf{aba = bab, aca = cac, bcb = cbc}).$$

(présentation du monoïde d'Artin-Tits de type \tilde{A}_2). Pour $w := \bar{\mathbf{a}}\mathbf{b}^2$, on trouve

$$\bar{\mathbf{a}}\mathbf{b}\mathbf{b} = \bar{\mathbf{a}}\mathbf{b}\mathbf{b} \curvearrowright_R^1 \mathbf{b}\bar{\mathbf{a}}\mathbf{b} \bar{\mathbf{a}}\mathbf{b} \curvearrowright_R^1 \mathbf{b}\bar{\mathbf{a}}\mathbf{b}\bar{\mathbf{a}}\mathbf{b} \bar{\mathbf{a}} \curvearrowright_R^1 \mathbf{b}\bar{\mathbf{a}}\mathbf{b} \bar{\mathbf{a}}.$$

On ne peut pas continuer car $\mathbf{b}\bar{\mathbf{a}}\mathbf{b} \bar{\mathbf{a}}$ n'a pas de facteur de la forme $\bar{s}t$.

DÉFINITION 1.6 (**retournement II**). Si (S, R) est une présentation complétée à droite, on dit qu'un S -mot signé w se retourne à droite en w' en k étapes, noté $w \curvearrowright_R^k w'$, s'il existe des S -mots signés w_0, \dots, w_k satisfaisant $w_0 = w$, $w_k = w'$ et $w_i \curvearrowright_R^1 w_{i+1}$ pour chaque i . Dans ce cas, la suite (w_0, \dots, w_k) est appelée *suite de retournement à droite* de w à w' . On note $w \curvearrowright_R w'$, ou simplement $w \curvearrowright w'$, si $w \curvearrowright_R^k w'$ est vérifié pour un certain k .

Dans la suite, on parlera régulièrement de relation de retournement récursive. On commence par donner une définition d'une présentation de monoïde récursive [23, chapitre 8].

DÉFINITION 1.7 (**présentation récursive**). Une présentation (finie ou infinie dénombrable) (S, R) est dite récursive si, un codage de S par des entiers ayant été fixé, la liste des relations de R , vues comme ensemble de suites finies d'entiers donc, après codage, comme ensemble de mots sur l'alphabet $\{0, 1\}$, est récursive, c'est-à-dire qu'il existe une machine de Turing (ou n'importe quel programme effectif) qui, pour tout entier w , décide si w est ou non le code d'une relation de R .

DÉFINITION 1.8 (**retournement récursif**). La relation de retournement associée à une présentation récursive est récursive au sens où il existe une machine de Turing (ou n'importe quel programme effectif) qui, étant donnés deux mots w, w' , décide si w' est obtenu ou non par une étape de retournement à partir de w .

Dans le contexte précédent, un S -mot signé est dit \curvearrowright -terminal s'il n'existe aucun mot w' satisfaisant $w \curvearrowright_R w'$, soit, de façon équivalente, si w ne contient aucun facteur de la forme $\bar{s}t$ tel que R contienne une relation $s... = t...$. En particulier, tous les S -mots signés positifs-négatifs, c'est-à-dire de la forme $u\bar{v}$ avec u, v positifs, sont \curvearrowright -terminaux.

Le résultat suivant, qui est un outil de base pour des démonstrations par récurrence sur le retournement, affirme que le retournement de la concaténation de deux mots peut toujours être décomposé en trois fragments successifs.

LEMME 1.9. *On suppose $w \curvearrowright^k v\bar{u}$ avec $u, v \in S^*$ et $w \in (S \cup \bar{S})^*$. Alors, pour toute décomposition $w = w_1w_2$, avec $w_1, w_2 \in (S \cup \bar{S})^*$, il existe dans S^* des décompositions $u = u_1u_2$, $v = v_1v_2$ et $u_0, v_0 \in S^*$ satisfaisant $w_1 \curvearrowright^{k_1} v_1\bar{u}_0$, $w_2 \curvearrowright^{k_2} v_0\bar{u}_1$ et $\bar{u}_0v_0 \curvearrowright^{k_0} v_2\bar{u}_2$ avec $k = k_1 + k_2 + k_0$.*

La démonstration apparaît dans [28, lemme II.4.23], et on ne la répète pas.

LEMME 1.10. *Soit u, v_1, v_2, u', v' des S -mots vérifiant $\bar{u}v_1v_2 \curvearrowright v'\bar{u}'$, alors il existe, dans S^* , une décomposition $v' = v'_1v'_2$ et un mot positif u_1 satisfaisant $\bar{u}v_1 \curvearrowright v'_1\bar{u}_1$ et $\bar{u}_1v_2 \curvearrowright v'_2\bar{u}'$.*

DÉMONSTRATION. On applique le lemme 1.9 à $w = \bar{u}v_1v_2 \curvearrowright v'\bar{u}'$ avec $w_1 = \bar{u}v_1$ et $w_2 = v_2$. Du fait que v_2 est positif, le seul retournement possible de w_2 est $w_2 \curvearrowright^0 w_2\varepsilon$. Ainsi, on obtient l'existence d'une décomposition $v' = v'_1v'_2$ et d'un mot positif u_1 satisfaisant $w_1 = \bar{u}v_1 \curvearrowright v'_1\bar{u}_1$ et $\bar{u}_1v_2 \curvearrowright v'_2\bar{u}'$. \square

Diagrammes de retournement, cas particulier. Afin de rendre plus lisibles les suites de retournement, on associe à chaque suite de retournement \vec{w} un graphe orienté $\mathcal{D}(\vec{w})$, appelé *diagramme de retournement*.

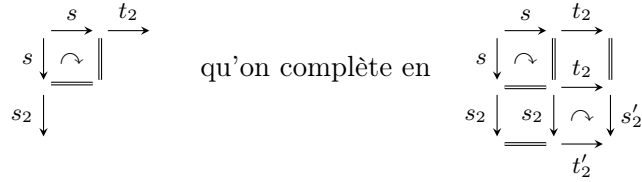
On débute par le cas spécial d'une présentation (S, R) ne possédant que des relations *courtes*, à savoir des relations $u = v$ telles que la longueur de u et v est au plus 2. Soit w_0 un mot négatif-positif, c'est-à-dire $w_0 = \bar{u}v$ avec u et v positifs. On commence le diagramme $\mathcal{D}(\vec{w})$ à partir d'un sommet initial et en dessinant une suite de flèches verticales dirigées vers le bas, étiquetées par les lettres successives de u . Puis, partant encore du même sommet initial, on dessine une suite de flèches horizontales dirigées vers la droite, étiquetées par les lettres de v . Ensuite, on construit $\mathcal{D}(\vec{w})$ par induction. Par définition, w_1 est obtenu de w_0 , soit en remplaçant un facteur $\bar{s}t$ par $s't'$ (qui par hypothèse est de longueur au plus 2) avec $ss' = tt'$ une relation de R , soit en supprimant un facteur $\bar{s}s$. Dans le premier cas, $\bar{s}t$ est associé au motif

$$(1.11) \quad \begin{array}{c} \xrightarrow{t} \\ s \downarrow \end{array} \quad \text{qu'on complète en} \quad \begin{array}{c} \xrightarrow{t} \\ s \downarrow \curvearrowright \downarrow t' \\ \xrightarrow{s'} \end{array}$$

dans le second cas, $\bar{s}s$ est associé au motif

$$(1.12) \quad \begin{array}{c} \xrightarrow{s} \\ s \downarrow \end{array} \quad \text{qu'on complète en} \quad \begin{array}{c} \xrightarrow{s} \\ s \downarrow \curvearrowright \parallel \\ \parallel \end{array}$$

et on continue de la même façon pour w_2 , etc.. Par exemple, après avoir retourné $\bar{s}s$ en ε , l'étape suivante, à savoir le retournement de \bar{s}_2t_2 en $t'_2\bar{s}'_2$, est illustrée en



Voir la figure 1 pour un exemple.

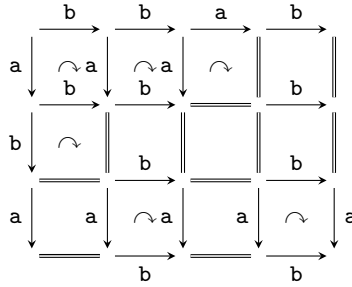


FIGURE 1. Avec la présentation $(a, b \mid ab = ba)$, on trouve $\bar{a}\bar{b}\bar{a}bbab \curvearrowright \bar{a}\bar{b}\bar{b}\bar{a}bab \curvearrowright \bar{a}\bar{a}bab \curvearrowright \bar{a}\bar{b}\bar{a}ab \curvearrowright \bar{a}bb \curvearrowright b\bar{a}b \curvearrowright b\bar{b}\bar{a}$, illustré dans le diagramme ci-dessus.

Diagrammes de retournement, cas général. On étend la construction précédente à des cas plus généraux. Tout d’abord, dans le cas où la suite de retournement \vec{w} ne commence plus par un S -mot négatif-positif, nous dessinons un diagramme similaire, mais en démarrant avec un escalier qui a plus qu’une marche, voir la figure 2.

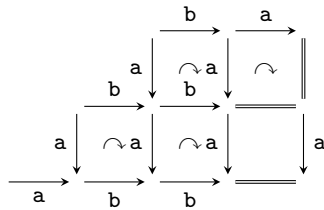


FIGURE 2. Toujours avec la présentation $(a, b \mid ab = ba)$, on forme la suite $a\bar{a}\bar{b}\bar{a}ba \curvearrowright ab\bar{a}\bar{a}ba \curvearrowright ab\bar{a}\bar{b}\bar{a}a \curvearrowright ab\bar{a}b \curvearrowright abb\bar{a}$, correspondant au diagramme ci-dessus.

Ensuite, pour le cas d’une présentation complétée dont les relations ne sont plus nécessairement courtes, les S -mots u et v , vérifiant $su = tv$, ne sont plus de longueur au plus 1. On dessine le diagramme comme précédemment mais, quand c’est nécessaire, on divise les bords des carrés en plusieurs flèches plus courtes, voir un exemple dans la figure 3.

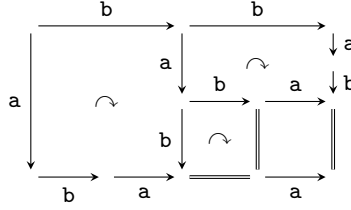


FIGURE 3. Avec la présentation (1.5) du monoïde d'Artin-Tits de type \tilde{A}_2 , on $\bar{a}bb \curvearrowright \bar{b}a\bar{b}a\bar{b} \curvearrowright \bar{b}a\bar{b}b\bar{a}\bar{b}a \curvearrowright \bar{b}a\bar{a}\bar{b}a$, dont le diagramme est représentée ci-dessus.

Le diagramme maximal d'un mot. À partir d'un mot initial w , on peut former plusieurs suites de retournement en choisissant des facteurs $\bar{s}t$ différents, et, de là, des diagrammes de retournement différents. Mais on observe que — à la condition de partir d'une présentation complétée — deux tels diagrammes sont toujours compatibles entre eux, au sens suivant :

LEMME 1.13. *Si (S, R) est une présentation complétée à droite et si \vec{w}_1 et \vec{w}_2 sont deux suites de R -retournement à droite à partir de w , alors les diagrammes $\mathcal{D}(\vec{w}_1)$ et $\mathcal{D}(\vec{w}_2)$ sont compatibles, au sens où leur réunion est encore un diagramme de retournement, qui inclut chacun d'eux.*

DÉMONSTRATION. Soient \vec{w}_1 et \vec{w}_2 deux suites de retournement commençant par w . La seule possibilité pour que les deux diagrammes $\mathcal{D}(\vec{w}_1)$ et $\mathcal{D}(\vec{w}_2)$ ne soient pas compatibles serait qu'il existe deux flèches homologues dans $\mathcal{D}(\vec{w}_1)$ et $\mathcal{D}(\vec{w}_2)$ (même position relative, même étiquette) formant les côtés nord et ouest d'un carré dans $\mathcal{D}(\vec{w}_1)$ et d'un carré distinct dans $\mathcal{D}(\vec{w}_2)$: cela supposerait qu'il existe dans R deux relations du type $s\dots = t\dots$, ce qui est exclu. \square

Comme tous les diagrammes de retournement associés à des suites commençant toutes par w sont compatibles, on peut considérer la réunion de tous ces diagrammes :

DÉFINITION 1.14 (**diagramme maximal**). Si (S, R) est une présentation complétée à droite, le *diagramme maximal* $\mathcal{D}_{\max}(w)$ d'un S -mot signé w est la réunion de tous les diagrammes $\mathcal{D}(\vec{w})$ pour \vec{w} suite de R -retournements commençant par w .

Au moins si la présentation considérée contient des relations non courtes, le diagramme maximal d'un mot peut très bien être infini, voir la figure 4.

Par définition, le diagramme maximal d'un S -mot signé est unique. Le résultat suivant affirme que, fini ou infini, il est toujours un diagramme de retournement.

LEMME 1.15. *Pour tout S -mot signé w , il existe au moins une suite de retournement \vec{w} , commençant par w dont le diagramme est $\mathcal{D}_{\max}(w)$.*

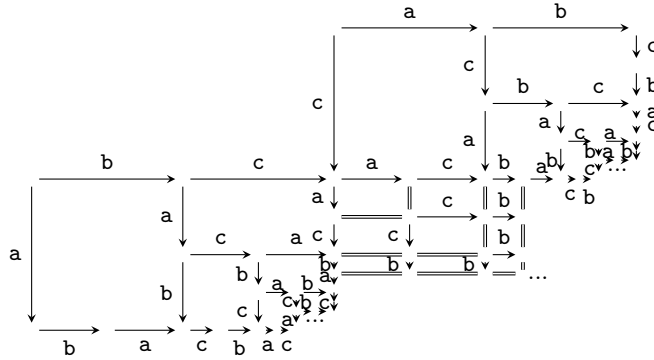


FIGURE 4. Avec la présentation (1.5), le diagramme maximal du mot $\overline{abc}cab$ est infini — et même « multi-infini » : il existe plusieurs nœuds à partir desquels partent une infinité de chemins.

DÉMONSTRATION. Puisque l'ensemble des nœuds de $\mathcal{D}_{\max}(w)$ est fini ou dénombrable et que tous les diagrammes de retournement commençant par w_0 sont compatibles, on peut énumérer les nœuds en N_0, N_1, \dots , etc., de façon à ce qu'un nœud apparaisse toujours après les nœuds à sa gauche et au-dessus, et alors obtenir \vec{w} comme la suite des retournements (uniques) s'appliquant en N_0 , puis N_1 , etc. Alors, par construction, le diagramme $\mathcal{D}_{\max}(w)$ est égal à $\mathcal{D}(\vec{w})$. \square

Il résulte directement de la définition que, pour toute présentation complémentée (S, R) et tout S -mot signé w , le diagramme maximal $\mathcal{D}_{\max}(w)$ ne peut pas être prolongé, puisqu'il est la réunion de tous les diagrammes partant de w . Une conséquence directe est l'unicité d'un éventuel mot terminal :

PROPOSITION 1.16 (**unicité**). *Si (S, R) est une présentation complémentée à droite, alors, pour tout S -mot signé w , il existe au plus un mot \curvearrowright -terminal w' tel que w se retourne à droite en w' .*

DÉMONSTRATION. Considérons le diagramme $\mathcal{D}_{\max}(w)$. S'il est infini, alors il existe une suite infinie d'étapes de retournement à partir de w , et donc il n'existe pas de mot \curvearrowright -terminal w' tel que w se retourne à droite en w' . Sinon, par le lemme 1.15, il existe une suite finie \vec{w} vérifiant $\mathcal{D}_{\max}(w) = \mathcal{D}(\vec{w})$. Soit w' le dernier mot de \vec{w} . Par construction, w se retourne en w' , et w' est \curvearrowright -terminal. De plus, l'unicité du diagramme $\mathcal{D}_{\max}(w)$ entraîne celle du mot w' (mais pas celle de la suite \vec{w}). \square

REMARQUE 1.17. Nous nous sommes ici limité à des présentations complémentées (à droite). En fait, la méthode du retournement de facteur peut être développée pour toute présentation de monoïde ne contenant pas de ε -relation [21]. Mais les détails techniques sont bien plus compliqués dans le cas général, en particulier parce que le résultat d'unicité de la proposition 1.16 n'est pas garanti. Comme nous ne visons ici que des applications dans le cas complémenté, il est suffisant de se restreindre à celui-ci ici.

1.2. Complétude du retournement. Même dans le cas d'une présentation complétée, le retournement de facteur ne permet pas en général d'établir grand chose sur le monoïde associé. Par contre, il existe une situation particulière où le retournement est utile, à savoir lorsqu'une certaine condition dite de complétude est satisfaite. Le but de cette section est de montrer qu'il existe des conditions combinatoires simples, qu'on appellera conditions du cube, qui permettent d'assurer la complétude.

La notion de complétude. Dans toute la suite de cette section, on suppose fixée une présentation complétée à droite (S, R) , et on note \equiv la congruence sur S^* engendrée par R . Le point de départ est la facile implication suivante :

PROPOSITION 1.18 (**retournement implique équivalence**). *Pour tous mots $u, v, u',$ et v' dans S^* ,*

$$(1.19) \quad \bar{u}v \curvearrowright v'\bar{u}' \quad \text{implique} \quad uv' \equiv vu'.$$

En particulier, $\bar{u}v \curvearrowright \varepsilon$ implique $u \equiv v$.

DÉMONSTRATION. On raisonne par récurrence sur k vérifiant $\bar{u}v \curvearrowright_R^k v'\bar{u}'$. Pour $k = 0$, on a $\bar{u}v = v'\bar{u}'$ et la seule possibilité est que u et u' , ou v et v' , soient vides, et on a alors $u' = u$ et $v' = v$, d'où le résultat.

On suppose maintenant $k \geq 1$. Alors nécessairement ni u , ni v ne peut être vide. Posons $u = su_0$ et $v = tv_0$ avec s, t dans S . Comme on a $\bar{u}v = \bar{u}_0 \bar{s}tv_0 \curvearrowright^k v'\bar{u}'$, la première étape de retournement se situe sur $\bar{s}t$, donc il existe des mots u_1, v_1 positifs, vérifiant $sv_1 = tu_1$ dans R , pour $s \neq t$, et $u_1 = v_1 = \varepsilon$, pour $s = t$, tels que $\bar{u}_0 \bar{s}tv_0 \curvearrowright^1 \bar{u}_0v_1\bar{u}_1v_0 \curvearrowright^{k-1} v'\bar{u}'$. Par le lemme 1.9 appliqué à $w_1 = \bar{u}_0v_1$ et $w_2 = \bar{u}_1v_0$, il existe $u_2, u_3, u_4, v_2, v_3, v_4$ satisfaisant $u' = u_2u_3$, $v' = v_2v_3$, $\bar{u}_0v_1 \curvearrowright^{k_2} v_2\bar{u}_4$, $\bar{u}_1v_0 \curvearrowright^{k_3} v_4\bar{u}_2$ et $\bar{u}_4v_4 \curvearrowright^{k_4} v_3\bar{u}_3$ avec $k_2 + k_3 + k_4 = k - 1$. On a donc $k_i < k$ pour tout $i \in \{2, 3, 4\}$, et l'hypothèse de récurrence implique

$$u_0v_2 \equiv v_1u_4, \quad u_1v_4 \equiv v_0u_2, \quad \text{et} \quad u_4v_3 \equiv v_4u_3,$$

d'où $uv' = su_0v_2v_3 \equiv sv_1u_4v_3 \equiv tu_1u_4v_3 \equiv tu_1v_4u_3 \equiv tv_0u_2u_3 = vu'$. \square

La situation intéressante est celle où la réciproque de (1.19) est vérifiée, c'est-à-dire que le retournement à droite détecte toutes les équivalences.

DÉFINITION 1.20 (**complétude**). On dit que le retournement à droite est *complet* pour une présentation (S, R) si, pour tous u, v dans S^* , la relation $u \equiv v$ implique $\bar{u}v \curvearrowright \varepsilon$.

Afin d'établir plus bas des critères de complétude facilement utilisables, on commence par donner une définition alternative.

LEMME 1.21. *Si (S, R) est une présentation complétée à droite, le retournement à droite est complet pour (S, R) si, et seulement si, pour tous mots u, v, u', v' positifs :*

$$(1.22) \quad \text{Si on a } uv' \equiv vu', \text{ alors il existe } u'', v'', w \text{ dans } S^* \text{ vérifiant} \\ \bar{u}v \curvearrowright v''\bar{u}'', \quad u' \equiv u''w \text{ et } v' \equiv v''w.$$

DÉMONSTRATION. On suppose que le retournement à droite est complet pour la présentation (S, R) et $uv' \equiv vu'$. Par complétude du retournement à droite, on a $\overline{(uv')}(vu') \curvearrowright \varepsilon$. On applique le lemme 1.10 à $\overline{uv}u' \curvearrowright v'$. On trouve qu'il existe dans S^* une décomposition $v' = v''w'$ et $u'' \in S^*$ vérifiant $\overline{uv} \curvearrowright v''\overline{u''}$ et $\overline{u''}u' \curvearrowright w'$. Ensuite, l'égalité $v' = v''w'$ implique $\overline{v'}v''w' \curvearrowright \varepsilon$. On applique à nouveau le lemme 1.10 et on trouve l'existence d'un w dans S^* satisfaisant $\overline{v'}v'' \curvearrowright \overline{w}$ et $\overline{w}w' \curvearrowright \varepsilon$. En résumé, on a trouvé que la relation $\overline{(uv')}(vu') \curvearrowright \varepsilon$ implique l'existence de $u'', v'', w, w' \in S^*$ respectant $\overline{uv} \curvearrowright v''\overline{u''}$, $\overline{u''}u' \curvearrowright w'$, $\overline{v'}v'' \curvearrowright \overline{w}$ et $\overline{w}w' \curvearrowright \varepsilon$. La proposition 1.18 implique $u' \equiv u''w'$, $w \equiv w'$ et $v' \equiv v''w \equiv v''w'$.

Réciproquement, supposons $u \equiv v$, autrement dit $u\varepsilon \equiv v\varepsilon$. D'après l'hypothèse, il existe u'', v'', w dans S^* satisfaisant $\overline{uv} \curvearrowright v''\overline{u''}$, $\varepsilon \equiv u''w$ et $\varepsilon \equiv v''w$. Comme (S, R) est complétée à droite, elle n'a pas de ε -relation, donc on a nécessairement $u'' = v'' = w = \varepsilon$. D'où $\overline{uv} \curvearrowright \varepsilon$. \square

La condition du cube. Il existe plusieurs critères effectifs pour vérifier que le retournement est complet pour une présentation, tous basés sur ce qu'on appelle la condition du cube.

DÉFINITION 1.23 (**condition du cube**). [25, définition 2.6] Si (S, R) est une présentation complétée à droite et si u, v, w sont dans S^* , on dit que la *condition du cube* (à droite) est satisfaite pour (u, v, w) si

$$\overline{uw}\overline{wv} \curvearrowright_R v'\overline{u'} \quad \text{implique} \quad \overline{v'}\overline{uv}u' \curvearrowright_R \varepsilon.$$

Il est facile de vérifier que la complétude peut s'énoncer en termes de condition du cube :

LEMME 1.24. *Le retournement à droite est complet pour une présentation complétée à droite (S, R) si, et seulement si, la condition du cube à droite est satisfaite pour tout triplet de mots de S^* .*

DÉMONSTRATION. On suppose le retournement complet et $\overline{uw}\overline{wv} \curvearrowright v'\overline{u'}$. Par le lemme 1.9, il existe $u_0, u_1, u_2, v_0, v_1, v_2$ dans S^* , avec $u' = u_1u_2$, $v' = v_1v_2$, satisfaisant $\overline{uw} \curvearrowright v_1\overline{u_0}$, $\overline{wv} \curvearrowright v_0\overline{u_1}$ et $\overline{u_0}v_0 \curvearrowright v_2\overline{u_2}$. D'où, par la proposition 1.18, les équivalences $uw' = uv_1v_2 \equiv wu_0v_2 \equiv wv_0u_2 \equiv vu_1u_2 = vu'$. Ainsi, on a $uw' \equiv vu'$. Par complétude, ceci implique que $\overline{(uw')}(vu') \curvearrowright \varepsilon$, donc la condition du cube est satisfaite pour le triplet (u, v, w) .

Réciproquement, on suppose que la condition du cube à droite est satisfaite pour tout triplet de mots de S^* . Montrons que la relation « $\overline{uv} \curvearrowright \varepsilon$ » qui, par construction, est réflexive et symétrique, est aussi transitive. Supposons

$\bar{u}w \curvearrowright \varepsilon$ et $\bar{w}v \curvearrowright \varepsilon$. On a $\bar{\varepsilon}\varepsilon \curvearrowright \varepsilon$, donc $\bar{u}w\bar{w}v \curvearrowright \varepsilon$. Par la condition du cube, on déduit $\bar{u}v \curvearrowright \varepsilon$. Donc, « $\bar{u}v \curvearrowright \varepsilon$ » est une relation d'équivalence sur S^* . De plus, elle est compatible avec la multiplication des deux côtés, donc c'est une congruence sur le monoïde S^* . D'autre part, elle inclut R , donc aussi la congruence \equiv engendrée par R . Par conséquent, $u \equiv v$ implique $\bar{u}v \curvearrowright \varepsilon$, et le retournement est complet. \square

La remarque suivante est que, lorsqu'on veut établir la condition du cube, il suffira de considérer des triplets de mots deux à deux distincts :

LEMME 1.25. *Si (u, v, w) est un triplet de mots dont au moins deux coïncident, la condition du cube est satisfaite pour (u, v, w) .*

DÉMONSTRATION. Soit $u, v \in S^*$ vérifiant $\bar{u}v \curvearrowright v'\bar{u}'$ avec $u', v' \in S^*$. Les diagrammes suivants montrent que les triplets (u, u, v) et (u, v, u) satisfont la condition du cube :

$$\begin{array}{ccc}
 \begin{array}{c}
 \begin{array}{ccc}
 & u & \\
 & \rightarrow & \\
 v^v \downarrow & & \downarrow v' \\
 u \downarrow & u' & \downarrow \\
 & \rightarrow & \\
 & v' & \\
 \hline
 & v & \\
 u \downarrow & & \downarrow u' \\
 & \rightarrow & \\
 & u' & \\
 \hline
 & v' & \\
 \hline
 & v' & \\
 \hline
 \end{array}
 & \Rightarrow &
 \begin{array}{ccc}
 & u & v' \\
 & \rightarrow & \rightarrow \\
 u \downarrow & & \downarrow \\
 v' \downarrow & v' & \downarrow \\
 & \rightarrow & \\
 & v & u' \\
 u \downarrow & & \downarrow \\
 v' \downarrow & v' & \downarrow \\
 & \rightarrow & \\
 & v' & \\
 \hline
 & v' & \\
 \hline
 \end{array}
 \end{array}
 \end{array}$$

Le lemme 1.24 ne fournit pas un critère de complétude effectif, car on doit considérer des triplets de mots arbitraires, et, même en se restreignant à des mots deux à deux distincts, il existe une infinité de tels triplets. On peut améliorer le résultat et se restreindre à des triplets beaucoup plus particuliers. Le critère le plus classique concerne le cas des présentations noethériennes.

DÉFINITION 1.26 (**présentation noethérienne**). Une présentation de monoïde (S, R) est dite *noethérienne à droite* s'il existe $\lambda^* : S^* \rightarrow \mathbf{Ord}$ qui est \equiv -invariante et vérifie $\lambda^*(sw) > \lambda^*(w)$ pour tous s dans S et w dans S^* .

Il est immédiat qu'une présentation (S, R) est noethérienne à droite si, et seulement si, le monoïde $\langle S | R \rangle^+$ est noethérien à droite, la fonction λ^* de la définition 1.26 induisant un témoin de noethérianité pour $\langle S | R \rangle^+$. Par ailleurs, toute présentation (S, R) où R ne comporte que des relations $u = v$ avec $|u| = |v|$ est noethérienne (à droite et à gauche, au sens évident), la fonction « longueur » servant alors de fonction-témoin λ^* .

PROPOSITION 1.27 (**critère de complétude I**). *Si (S, R) est une présentation complétée à droite et noethérienne à droite, le retournement à droite est complet pour (S, R) si, et seulement si, la condition du cube à droite est satisfaite pour tout triplet de lettres de S deux à deux distinctes.*

La démonstration, non triviale, consiste à établir l'implication (1.22) par induction sur la valeur de $\lambda^*(uv')$. Elle est détaillée dans [28, lemme II.4.62], et on ne la répète pas ici.

EXEMPLE 1.28. Les relations de tresses de la présentation (I.2.2) du monoïde B_∞^+ sont de la forme $u = v$ avec $|u| = |v|$, donc (I.2.2) est noethérienne à droite. Par la proposition 1.27, il suffit, pour établir que le retournement à droite est complet pour (I.2.2), d'établir la condition du cube pour tout triplet $(\sigma_i, \sigma_j, \sigma_k)$ avec i, j et k deux à deux distincts. Il n'y a en fait qu'un nombre fini de cas réellement distincts à considérer selon l'ordre relatif de i, j, k et le fait qu'ils soient adjacents ou non. Les trois cas correspondants à $i < j < k$ sont illustrés dans la figure 5. Les autres cas seraient traités de même, permettant de conclure que le retournement est complet pour (I.2.2).

1.3. Terminaison du retournement. Si le retournement (à droite) associé à une présentation de monoïde (S, R) est complet, on sait que, si on part de deux mots positifs u, v qui sont \equiv -équivalents, alors le retournement de $\bar{u}v$ mène en un nombre fini d'étapes à un mot terminal. Par contre, l'hypothèse de complétude ne dit rien sur la possible obtention d'un mot terminal partant d'un mot $\bar{u}v$ avec u, v quelconques dans S^* , ou, encore moins, partant d'un mot signé quelconque. Quand on retourne à droite un mot signé w , trois situations peuvent apparaître :

DÉFINITION 1.29 (**réussir, bloquer, terminer**). Si (S, R) est une présentation complétée à droite et w un S -mot signé, on dit que le retournement à droite *réussit pour* w s'il existe un mot positif-négatif w' vérifiant $w \curvearrowright w'$, qu'il *bloque pour* w s'il existe un mot \curvearrowright -terminal w' contenant un facteur $\bar{s}t$ sans relation $s\dots = t\dots$ dans R et vérifiant $w \curvearrowright w'$, et qu'il *ne termine pas pour* w s'il existe une suite infinie de retournements à partir de w . Enfin, on dit que le retournement termine pour w s'il réussit ou bloque pour w .

Par définition du retournement, quel que soit le S -mot signé S , le retournement à droite à partir de w soit réussit, soit bloque, soit ne termine pas et, comme on ne considère que des présentations complétées à droite, ces trois situations s'excluent mutuellement. On dira que le retournement *termine toujours* pour (S, R) s'il termine pour tout S -mot signé.

Dans le cas réussi, le diagramme $\mathcal{D}_{\max}(w)$ est fini et ne possède aucun motif ouvert formé d'une flèche verticale et d'une flèche horizontale de même source. Dans le cas bloquant, le diagramme $\mathcal{D}_{\max}(w)$ est fini et il possède un motif ouvert comme ci-dessus. Dans le cas non-terminant, le diagramme $\mathcal{D}_{\max}(w)$ est infini.

EXEMPLE 1.30. Pour la présentation $(a, b \mid ab = ba)$, le retournement de $\bar{a}bb$ réussit et termine par $ba^2\bar{b}\bar{a}$.

Pour la présentation $(a, b, c \mid ab = ba, bc = cb)$, on trouve $\bar{a}bc \curvearrowright \bar{b}\bar{a}c$, et le dernier mot est \curvearrowright -terminal, car on n'a pas de relation de la forme $a\dots = c\dots$ dans la présentation. Donc le retournement de $\bar{a}bc$ bloque.

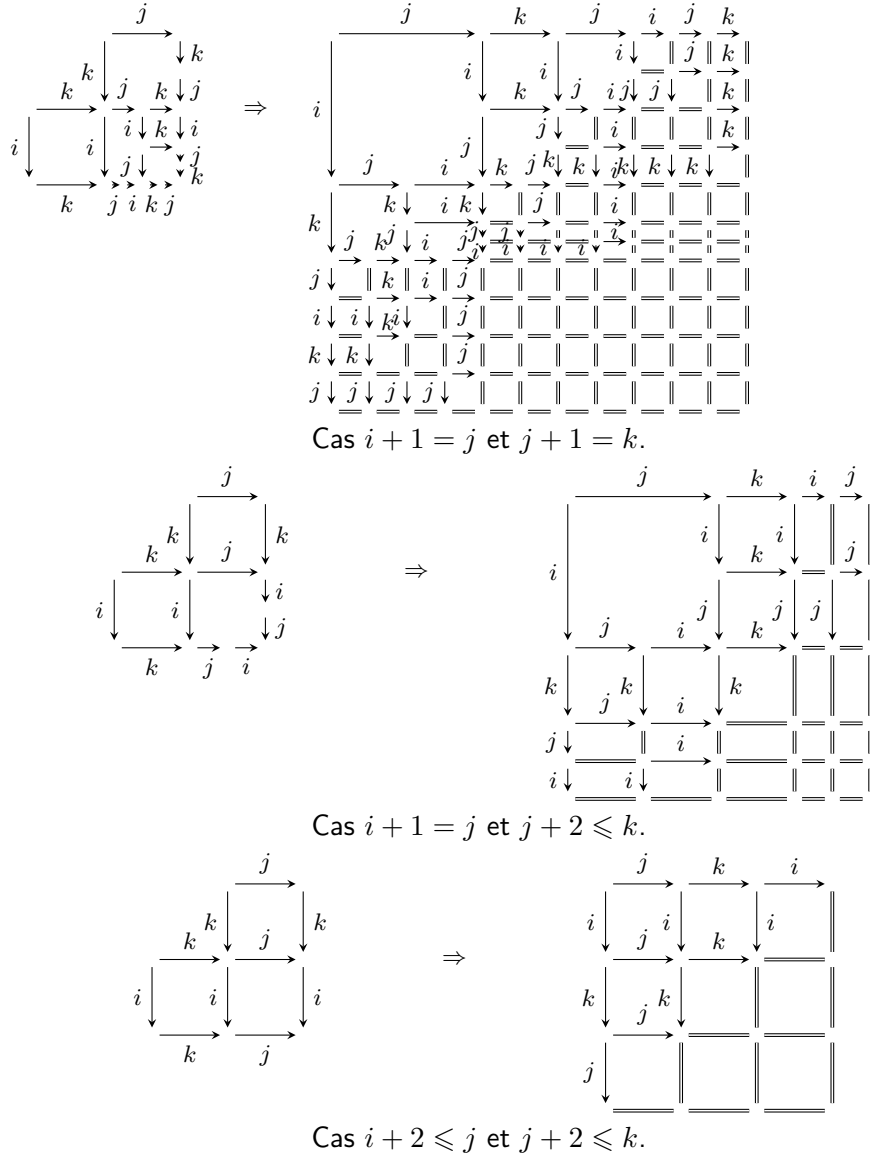


FIGURE 5. Condition du cube pour la présentation (I.2.2) de B_{∞}^+ , dans le cas des triplets $(\sigma_i, \sigma_j, \sigma_k)$ vérifiant $i < j < k$.

Enfin, avec la présentation (1.5) du monoïde d'Artin-Tits de type \tilde{A}_2 , on trouve $\bar{a}bc \curvearrowright \bar{b}a\bar{b}a\bar{c} \curvearrowright^5 \bar{b}ac\bar{b}ac\bar{a}\bar{b}\bar{c}\bar{c}\bar{a}\bar{b}\bar{c}\bar{a}$, et on lit, dans le dernier mot, le facteur $\bar{a}bc$ qui est le mot initial. Il est donc clair que le retournement à droite de $\bar{a}bc$ ne termine pas dans ce cas.

Le cas bloquant ne peut se produire que s'il manque des relations de type $s... = t...$ dans la présentation considérée. Le résultat suivant est donc évident :

LEMME 1.31. *Si une présentation (S, R) est telle que, pour tous s, t distincts dans S , il existe une relation $s\dots = t\dots$, alors, pour tout mot signé w , le retournement à partir de w ou bien réussit, ou bien ne termine pas.*

Déterminer si le retournement est toujours terminant ou non est en général un problème difficile, et il n'existe pas de méthode uniforme pour le résoudre. Par contre, il existe un cas particulier où le problème est facile. On rappelle qu'une relation $u = v$ est dite *courte* si la longueur de u et la longueur de v sont, chacune, au plus égales à 2.

PROPOSITION 1.32 (**critère de terminaison I**). *Si (S, R) est une présentation complétée à droite ne contenant que des relations courtes, alors le retournement à droite pour (S, R) est toujours terminant ; de plus, toute suite de retournement commençant par un mot contenant p lettres négatives et q lettres positives est de longueur au plus pq .*

DÉMONSTRATION. Comme toutes les relations de R sont courtes, appliquer une étape de retournement revient à remplacer un facteur de longueur 2 par un mot de longueur au plus 2. Donc la longueur n'augmente pas lors du retournement, et celui-ci se termine toujours. Si w est un S -mot signé initial composé de p lettres négatives et q lettres positives, alors le diagramme de retournement de w est dessiné sur une grille de taille $p \times q$, donc contenant au plus pq carrés. Donc il y a au plus plus pq étapes de retournement. \square

Le troisième cas de l'exemple 1.30 montre que la terminaison n'est pas garantie quand on retire l'hypothèse sur les relations courtes. Notons qu'à ce point le cas de la présentation (I.2.2) est ouvert, puisqu'elle contient les relations non-courtes $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$: on peut montrer que, dans ce cas, le retournement est terminant, mais, pour le moment, ce n'est pas évident.

Retournement à gauche. Par définition, le retournement à droite remplace un facteur négatif-positif $\bar{s}t$ par un mot positif-négatif $u\bar{v}$. Une approche symétrique est possible et consiste soit à supprimer un facteur positif-négatif $s\bar{s}$, soit à remplacer un facteur positif-négatif $t\bar{s}$ par un mot négatif-positif $\bar{v}u$ tel que $vt = us$ est une relation de la présentation considérée. Cette version symétrique est appelée *retournement à gauche* associé à R , notée \curvearrowright_R ou simplement \curvearrowright .

On notera que le retournement à gauche n'est pas (en tant que relation binaire sur S^*) l'inverse du retournement à droite : $w \curvearrowright w'$ n'implique pas nécessairement $w' \curvearrowright w$. Par exemple, pour chaque lettre s dans S , on a $\bar{s}s \curvearrowright \varepsilon$, mais pas $\varepsilon \curvearrowright \bar{s}s$: le mot vide ne se retourne en aucun autre mot que lui-même.

Les propriétés des retournements à gauche et à droite sont symétriques et tous les résultats pour le retournement à droite ont une version homologue en terme de retournement à gauche. En particulier, on a un critère de complétude analogue à la proposition 1.27 :

PROPOSITION 1.33 (critère de complétude I). *Si (S, R) est une présentation complétée à gauche et noethérienne à gauche, le retournement à gauche est complet pour (S, R) si, et seulement si, la condition du cube à gauche est satisfaite pour tous triplets de lettres de S deux à deux distinctes.*

On pourrait vérifier en refaisant les calculs symétriques de ceux qui ont été indiqués plus haut que le retournement à gauche est complet pour la présentation (I.2.2) du monoïde de tresses B_∞^+ . En fait, l'identité de $\{\sigma_1, \sigma_2, \dots\}$ induisant un antiautomorphisme de B_∞^+ dans lui-même, il n'y a pas besoin de refaire les calculs et il suffit d'alléguer la symétrie ci-dessus.

De la même façon, on peut énoncer pour la terminaison :

PROPOSITION 1.34 (critère de terminaison I). *Si (S, R) est une présentation complétée à gauche ne contenant que des relations courtes, alors le retournement à gauche pour (S, R) est toujours terminant; de plus, toute suite de retournement commençant par un mot contenant p lettres négatives et q lettres positives est de longueur au plus pq .*

2. Un nouveau critère de complétude

Pour étudier le monoïde H^+ introduit au chapitre I, il va être nécessaire d'étendre les résultats de la section 1, et en particulier les critères de complétude et de terminaison des propositions 1.27 et 1.32. Pour cela, la notion d'ensemble clos par complément est fondamentale, et elle permet d'établir des critères plus puissants. Cette méthode a déjà été introduite dans l'article [20], notamment pour couvrir le cas du monoïde de tresses B_∞^+ , mais, pour étudier le monoïde H^+ , nous devons développer une version plus générale, qui est donc formellement nouvelle : en effet, à la différence de la présentation (I.2.2) de B_∞^+ , le retournement n'est pas toujours terminant pour la présentation (I.3.2) de H^+ , et on ne peut pas utiliser tel quel le formalisme de [20]. On va donc reprendre ici l'étude générale sur des bases élargies, et établir un nouveau critère de complétude (dans cette section), et un nouveau critère de terminaison (dans la suivante).

2.1. Ensembles clos par complément. Le point de départ est la notion de fonction « complément » sur les mots. Si (S, R) est une présentation complétée à droite, et si u, v sont des mots de S^* et que le retournement d'un mot de la forme $\bar{u}v$ réussit, il aboutit à un mot positif-négatif de la forme $v'\bar{u}'$ ne dépendant que des mots de départ u et v . Il sera utile de considérer les opérations binaires qui, à deux mots u et v , associent les mots u' et v' .

DÉFINITION 2.1 (R -complément). Si (S, R) est une présentation complétée à droite et u, v appartiennent à S^* , le R -complément à droite de u dans v , noté $C_R(u, v)$, est l'unique S -mot v' tel qu'il existe u' vérifiant $\bar{u}v \sim v'\bar{u}'$, s'il existe.

Lorsqu'il n'y a pas d'ambiguïté, on écrira généralement « complément » pour « R -complément à droite », et on notera $C(u, v)$ pour $C_R(u, v)$. On note qu'en général la fonction complément est une fonction partielle, non nécessairement partout définie : si le R -retournement de $\bar{u}v$ ou bien bloque, ou bien ne termine pas, alors $C_R(u, v)$ n'existe pas.

REMARQUE 2.2. Il n'y a pas besoin d'introduire une seconde opération pour le mot u' tel que $\bar{u}v$ se retourne en $v'\bar{u}'$, car, par la symétrie du retournement, si on a $\bar{u}v \curvearrowright v'\bar{u}'$, on a aussi $\bar{v}u \curvearrowright u'\bar{v}'$, et donc on a $u' = C(v, u)$.

En liaison avec la fonction complément apparaît la notion d'ensemble de mots clos par complément :

DÉFINITION 2.3 (**clos par complément**). Si (S, R) est une présentation complémentée, un sous-ensemble X de S^* est dit *clos par R -complément à droite* si, pour tous u, v dans X , ou bien $C(u, v)$ existe et appartient à X , ou bien $C(u, v)$ n'est pas défini.

Bien noter qu'on n'exige *pas* que le complément soit toujours défini. Par exemple, si R est vide (pas de relation du tout), le complément n'est jamais défini, et *tout* ensemble de mots est clos par complément.

Notre observation de base est que, dans tous les cas, il existe toujours une clôture par complément bien définie :

PROPOSITION 2.4 (**clôture**). *Si (S, R) est une présentation complémentée à droite, alors, pour tout ensemble de mots X , il existe un plus petit ensemble de mots incluant X et clos par complément à droite, à savoir l'ensemble \widehat{X} défini par $\widehat{X} := \bigcup_{n \geq 0} X_n$, avec $X_0 := X$ et, pour $n \geq 1$,*

$$(2.5) \quad X_n := X_{n-1} \cup \{ C(u, v) \mid u, v \in X_{n-1} \text{ et } C(u, v) \text{ est défini} \}.$$

DÉMONSTRATION. Par définition, \widehat{X} est un ensemble de mots incluant X . Soient u, v dans \widehat{X} . Alors, comme pour tout n , on a $X_n \subseteq X_{n+1}$, il existe un entier m tel que u, v appartiennent à X_m . Si $C(u, v)$ est défini, alors il appartient à X_{m+1} , donc à \widehat{X} . Donc \widehat{X} est clos par complément à droite.

Soit Y un ensemble de mots incluant X et clos par complément à droite. Montrons, par récurrence sur $n \geq 0$, que X_n est inclus dans Y . Pour $n = 0$, par définition, X_0 est inclus dans Y . Supposons $n \geq 1$. Alors on a $X_{n-1} \subseteq Y$ par hypothèse de récurrence. D'autre part, soient u et v des éléments de X_{n-1} tels que $C(u, v)$ est défini. Par hypothèse de récurrence, u et v sont dans Y , donc $C(u, v)$ y est aussi puisque Y est clos par complément à droite. Par conséquent, X_n est inclus dans Y . De là, \widehat{X} est inclus dans Y . \square

EXEMPLE 2.6. On considère à nouveau la présentation (1.5) du monoïde d'Artin-Tits de type \widetilde{A}_2 , et on part de $X = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ (ensemble des atomes du monoïde). On construit la clôture par complément à droite de X en appliquant l'induction de (2.5) à partir de $X_0 := \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$. Soient u, v dans X . On a $C(u, u) = \varepsilon$ et, pour $u = s, v = t$ avec $s \neq t$, on trouve $C(u, v) = ts$ et

$C(v, u) = st$. On obtient

$$X_1 = \{\mathbf{a}, \mathbf{b}, \mathbf{c}, \varepsilon, \mathbf{ab}, \mathbf{ba}, \mathbf{ac}, \mathbf{ca}, \mathbf{bc}, \mathbf{cb}\}.$$

Montrons que X_1 est clos par complément à droite. Tout d'abord, on a $C(u, \varepsilon) = \varepsilon$ et $C(\varepsilon, u) = u$, dans X_1 . Ensuite, supposons $|u| = 1$, soit $u = s$, et $|v| = 2$. Il y a 3 cas, suivant que s apparaît ou non dans v . Pour $v = st$, on trouve $C(u, v) = t$ et $C(v, u) = \varepsilon$, qui sont dans X_1 . Pour $v = ts$, on trouve de même $C(u, v) = ts$ et $C(v, u) = t$, qui sont dans X_1 . Enfin, pour $v = tr$ avec $t, r \neq s$, on trouve

$$\bar{s}tr \curvearrowright ts\bar{t}\bar{s}r \curvearrowright^5 tsrtsr\bar{s}tr\bar{r}\bar{s}\bar{t}\bar{r}\bar{s},$$

et on retrouve, dans ce dernier mot, le facteur $\bar{s}tr$. Donc le retournement de $\bar{s}tr$ ne termine pas et les compléments $C(u, v)$ et $C(v, u)$ ne sont pas définis.

Pour finir, supposons $|u| = |v| = 2$, soit $u = st$ et $v = rq$ avec $s \neq t$ et $r \neq q$. Comme on a que trois éléments dans S , les lettres s, t, r et q ne peuvent être distinctes. Pour $s = q$ et $t = r$, on trouve $C(st, ts) = s$ et $C(ts, st) = t$, dans X_1 . Pour $s = r$ et $t \neq q$, on a $C(st, sq) = qt$ et $C(sq, st) = tq$, dans X_1 . Pour $s = q$ et $t \neq r$, comme $C(r, st)$ n'est pas défini, $C(rs, st)$ et $C(st, rs)$ ne sont pas définis non plus. De même, pour $t = q$ et $s \neq r$, comme $C(r, st)$ n'est pas défini, $C(rt, st)$ et $C(st, rt)$ ne sont pas définis non plus. Donc tous les couples d'éléments possibles de X_1 ont été considérés, et X_1 est clos par complément à droite. Donc, la clôture par complément à droite de $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ est l'ensemble (fini) $\{\mathbf{a}, \mathbf{b}, \mathbf{c}, \varepsilon, \mathbf{ab}, \mathbf{ba}, \mathbf{ac}, \mathbf{ca}, \mathbf{bc}, \mathbf{cb}\}$.

L'introduction de la fonction de complément nous permet de donner une nouvelle définition alternative de la complétude.

LEMME 2.7. *Si (S, R) est une présentation complétée à droite, le retournement à droite est complet pour (S, R) si, et seulement si, la relation \equiv est compatible avec l'opération de complément à droite au sens où la conjonction de $u \equiv u'$ et $v \equiv v'$ entraîne soit $C(u, v) \equiv C(u', v')$, soit que ni $C(u, v)$, ni $C(u', v')$ ne sont définis.*

DÉMONSTRATION. Supposons le retournement complet. Puisque la relation \equiv est symétrique et transitive, il suffit de montrer que, si $C(u, v)$ existe et $u' \equiv u$ est vérifié, alors $C(u', v)$ existe aussi et on a

$$C(u', v) \equiv C(u, v) \quad \text{et} \quad C(v, u') \equiv C(v, u).$$

Or, puisque le retournement est complet, on a $C(u, u') = C(u', u) = \varepsilon$, d'où

$$C(C(u, u'), C(u, v)) = C(\varepsilon, C(u, v)) = C(u, v).$$

Par ailleurs, le lemme 1.21 implique que la condition du cube est satisfaite pour (u', u, v) , donc on déduit que

$$\overline{C(C(u, u'), C(u, v))} \overline{C(u', u)} u'vC(v, u)C(C(u, v), C(u, u')) \curvearrowright \varepsilon,$$

et en particulier

$$\overline{C(C(u, u'), C(u, v))} C(C(u', u), C(u', v)) \curvearrowright \varepsilon,$$

d'où $C(C(u', u), C(u', v)) \equiv C(C(u, u'), C(u, v))$. De là, on déduit que $C(u', v)$, et donc aussi $C(v, u')$, existent. De plus, on trouve

$$\begin{aligned} C(u', v) &= C(\varepsilon, C(u', v)) = C(C(u', u), C(u', v)) \\ &\equiv C(C(u, u'), C(u, v)) = C(\varepsilon, C(u, v)) = C(u, v), \end{aligned}$$

ce qui est la compatibilité recherchée.

Réciproquement, supposons que le complément est compatible avec la relation \equiv . Soient u et u' deux S -mots vérifiant $u \equiv u'$. Par construction, on a $\bar{u}u \curvearrowright \varepsilon$, c'est-à-dire $C(u, u) = \varepsilon$. Si (ii) est vrai, on déduit que $u \equiv u'$ entraîne l'existence de $C(u, u')$ et $C(u', u)$ et on a $C(u', u) \equiv C(u, u) = \varepsilon$, d'où $\bar{u}u' \curvearrowright \varepsilon$. Donc le retournement est complet pour la présentation (S, R) . \square

2.2. Énoncé principal et exemple. On va établir un nouveau critère de complétude pour le retournement de facteur, à nouveau fondé sur la condition du cube comme celui de la proposition 1.27, mais indépendant de toute condition de noethérianité. Le prix à payer pour cela est qu'il ne suffit plus de vérifier la condition du cube pour les triplets de lettres, mais qu'il faut la vérifier pour les triplets de mots qui sont dans la clôture des lettres par complément. Le résultat prend la forme suivante :

PROPOSITION 2.8 (critère de complétude II). *Si (S, R) est une présentation complétée à droite, le retournement à droite est complet pour (S, R) si, et seulement si, la condition du cube à droite est satisfaite pour tout triplet de mots sur S deux à deux distincts dans la clôture \widehat{S} de S par complément à droite.*

Dans l'exemple 2.6, la présentation est noethérienne, donc éligible pour la proposition 2.8. On donne ci-dessous un exemple plus intéressant où la proposition 2.8 ne s'applique pas — et où, de surcroît, la clôture requiert plus d'une étape de complémentation, contrairement au cas de l'exemple 2.6.

EXEMPLE 2.9. Considérons la présentation

$$(2.10) \quad (\mathbf{a, b, c} \mid \mathbf{baba = aba, cbc b = bcb, ac = ca}).$$

Le monoïde correspondant est le monoïde d'Artin-Krammer AK_3 [42]. On part de l'ensemble $S := \{\mathbf{a, b, c}\}$ des générateurs de la présentation. On part donc de $S_0 = \{\mathbf{a, b, c}\}$, et on définit inductivement les clôtures jusqu'à ce que la construction se stabilise. On trouve ainsi

$$\begin{aligned} S_1 &= S_0 \cup \{\varepsilon, \mathbf{ba, aba, cb, bcb}\}, \\ S_2 &= S_1 \cup \{\mathbf{bacba, abacba, cba, bcbaba, abcbaba, cbaba}\}, \\ S_3 &= S_2 \cup \{\mathbf{acba, cbabacba, baba, cbacba}\}, \\ S_4 &= S_3 \cup \{\mathbf{babacba, bcbabacba}\}, \end{aligned}$$

puis $S_5 = S_4$. On a donc $\widehat{S} = S_4$ et, finalement, la clôture de $\{\mathbf{a, b, c}\}$ par complément est l'ensemble (fini, à 20 éléments)

$$\{\mathbf{a, b, c, \varepsilon, ba, aba, cb, bcb, bacba, abacba, cba, bcbaba, abcbaba,}$$

$\{cbaba, acba, cbabacba, baba, cbacba, babacba, bcbabacba\}$.

La relation $baba = aba$ implique que aba est un diviseur propre à droite de aba dans le monoïde AK_3 , donc celui-ci n'est pas noethérien à droite et la proposition 1.27 ne peut donc lui être appliquée. Par contre, la proposition 2.8 s'applique et, comme la clôture \widehat{S} de l'ensemble S est finie, on peut effectivement vérifier (à l'aide d'un ordinateur) que le retournement à droite est complet pour la présentation.

2.3. Démonstration de la proposition 2.8. La démonstration est délicate, elle requiert plusieurs lemmes préparatoires qui vont nous occuper jusqu'à la fin de cette section. Le schéma général est celui de la dernière section de l'article [20], mais, comme on l'a dit, il faut faire attention car, ici, on ne suppose pas que les compléments existent nécessairement toujours. Dans toute la suite de la section, on suppose fixée une présentation (S, R) complémentée à droite.

LEMME 2.11. *Pour tous S -mots u, v, w tel que tout triplet d'éléments de $\{u, v, w\}$ satisfait la condition du cube, on a soit*

$$\overline{C(C(w, u), C(w, v))}C(C(u, w), C(u, v)) \curvearrowright \varepsilon,$$

soit le complément $C(C(w, u), C(w, v))$ n'est pas défini.

DÉMONSTRATION. Le seul mot de la forme $v'\overline{u'}$ sur lequel $\overline{uw\overline{wv}}$ peut se retourner est

$$C(u, w)C(C(w, u), C(w, v))\overline{C(C(w, v), C(w, u))}C(v, w).$$

Donc, si $\overline{uw\overline{wv}}$ ne se retourne pas en un mot de la forme $v'\overline{u'}$, le complément $C(C(w, u), C(w, v))$ n'est pas défini. Sinon, comme le triplet (u, v, w) satisfait la condition du cube, on a

$$(2.12) \quad \overline{C(C(w, u), C(w, v))}C(u, w)\overline{wv}C(v, w)C(C(w, v), C(w, u)) \curvearrowright \varepsilon,$$

d'où le diagramme de retournement suivant

$$\begin{array}{ccccc} & & v & \longrightarrow & C(v, w) & \longrightarrow & C(C(w, v), C(w, u)) \\ u \downarrow & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} \\ & & C(v, u) & \longrightarrow & C(C(v, w), C(v, u)) & \longrightarrow & \\ & & C(u, v) & \longrightarrow & C(C(v, u), C(v, w)) & \longrightarrow & \\ C(u, w) \downarrow & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \\ & & C(C(u, v), C(u, w)) & \longrightarrow & C(C(C(u, w), C(u, v))) & \longrightarrow & \\ & & C(C(u, w), C(u, v)) & \longrightarrow & C(C(C(u, w), C(u, v)), C(C(w, u), C(w, v))) & \longrightarrow & \\ C(C(w, u), C(w, v)) \downarrow & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \xrightarrow{\quad} & \\ & & C(C(C(w, u), C(w, v)), C(C(u, w), C(u, v))) & \longrightarrow & & \longrightarrow & \end{array}$$

Le mot positif $C(C(C(w, u), C(w, v)), C(C(u, w), C(u, v)))$ ne peut plus se retourner, donc par (2.12), on a

$$C(C(C(w, u), C(w, v)), C(C(u, w), C(u, v))) = \varepsilon.$$

Par le diagramme ci-dessus, $C(C(u, w), C(u, v))$ et $C(C(u, v), C(u, w))$ existent, et donc le mot $\overline{wu}uv$ se retourne en

$$C(w, u)C(C(u, w), C(u, v))\overline{C(C(u, v), C(u, w))}C(v, u).$$

Puis, comme le triplet (w, v, u) satisfait la condition du cube, on a

$$(2.13) \quad \overline{C(C(u, w), C(u, v))}C(w, u)\overline{w}vC(v, u)C(C(u, v), C(u, w)) \curvearrowright \varepsilon,$$

d'où le diagramme de retournement suivant

$$\begin{array}{ccccc}
 & & v & & C(v, u) & & C(C(u, v), C(v, w)) \\
 & & \longrightarrow & & \longrightarrow & & \longrightarrow \\
 w & \downarrow & & \downarrow & & \downarrow & \\
 & & C(w, v) & & C(C(v, u), C(v, w)) & & C(C(v, w), C(v, u)) \\
 & & \longrightarrow & & \longrightarrow & & \longrightarrow \\
 C(w, u) & \downarrow & & \downarrow & & \downarrow & \\
 & & C(C(w, v), C(w, u)) & & & & \\
 & & \longrightarrow & & & & \\
 C(C(u, w), C(u, v)) & \downarrow & & \downarrow & & \downarrow & \\
 & & C(C(C(w, u), C(w, v)), C(C(u, w), C(u, v))) & & & & \\
 & & \longrightarrow & & & & \\
 & & C(C(C(u, w), C(u, v)), C(C(w, u), C(w, v))) & & & &
 \end{array}$$

Le mot positif $C(C(C(u, w), C(u, v)), C(C(w, u), C(w, v)))$ ne peut plus se retourner, donc par (2.13), on a

$$C(C(C(u, w), C(u, v)), C(C(w, u), C(w, v))) = \varepsilon,$$

d'où

$$\overline{C(C(w, u), C(w, v))}C(C(u, w), C(u, v)) \curvearrowright \varepsilon.$$

□

Pour montrer la complétude dans la proposition 2.8, on va utiliser la forme du lemme 2.7, c'est-à-dire la compatibilité de \equiv avec le complément.

LEMME 2.14. *Supposons que X est un sous-ensemble de S^* , clos par complément à droite et que tout triplet d'éléments de X satisfait la condition du cube. Alors, pour u, v, v' dans X , la relation $\overline{v}v' \curvearrowright \varepsilon$ et l'existence de $C(v, u)$ entraînent que $C(v', u)$ existe, et qu'on a $\overline{C(v, u)}C(v', u) \curvearrowright \varepsilon$ et $\overline{C(u, v)}C(u, v') \curvearrowright \varepsilon$.*

DÉMONSTRATION. Par hypothèse, on a $C(v, v') = C(v', v) = \varepsilon$ et $C(v, u)$ existe. Donc, on trouve

$$C(v, u) = C(\varepsilon, C(v, u)) = C(C(v, v'), C(v, u)).$$

Donc $C(C(v, v'), C(v, u))$ existe. De plus, comme le triplet (v', u, v) satisfait la condition du cube, par le lemme 2.11, on a

$$C(C(C(v, v'), C(v, u)), C(C(v', v), C(v', u))) = \varepsilon.$$

Ceci entraîne que $C(v', u)$ et $C(u, v')$ existent. Avec la même méthode, on trouve

$$C(v', u) = C(\varepsilon, C(v', u)) = C(C(v', v), C(v', u)).$$

Donc $C(C(v', v), C(v', u))$ existe. De plus, comme le triplet (v, u, v') satisfait la condition du cube, par le lemme 2.11, on a

$$C(C(C(v', v), C(v', u)), C(C(v, v'), C(v, u))) = \varepsilon.$$

D'où $\overline{C(v', u)}C(v, u) = \overline{C(C(v', v), C(v', u))}C(C(v, v'), C(v, u)) \curvearrowright \varepsilon$.

Maintenant, on a

$$\varepsilon = C(C(v, u), \varepsilon) = C(C(v, u), C(v, v')).$$

Donc $C(C(v, u), C(v, v'))$ existe. Comme le triplet (u, v', v) satisfait la condition du cube, par le lemme 2.11, on a

$$\overline{C(C(v, u), C(v, v'))}C(C(u, v), C(u, v')) \curvearrowright \varepsilon.$$

Ceci entraîne $C(C(u, v), C(u, v')) = \varepsilon$. On obtient, de façon symétrique, l'égalité $C(C(u, v'), C(u, v)) = \varepsilon$. D'où $\overline{C(u, v')}C(u, v) \curvearrowright \varepsilon$. \square

LEMME 2.15. *Sous les hypothèses du lemme 2.14 :*

- (i) *La relation $\bar{u}v \curvearrowright \varepsilon$ est transitive sur X ;*
- (ii) *Pour u, v, u', v' dans X , si $C(v, u)$ existe, les relations $\bar{u}u' \curvearrowright \varepsilon$ et $\bar{v}v' \curvearrowright \varepsilon$ impliquent que $C(v', u')$ existe et qu'on a $\overline{C(v, u)}C(v', u') \curvearrowright \varepsilon$.*

DÉMONSTRATION. (i) Soient u, v, w dans X vérifiant $\bar{u}v \curvearrowright \varepsilon$ et $\bar{v}w \curvearrowright \varepsilon$. Par hypothèse, on a $C(u, v) = C(v, u) = \varepsilon$. Appliquant le lemme 2.14 à $\bar{v}w \curvearrowright \varepsilon$, on obtient que $C(w, u)$ existe et on a $\overline{C(v, u)}C(w, u) \curvearrowright \varepsilon$ et $\overline{C(u, v)}C(u, w) \curvearrowright \varepsilon$. Donc on a $C(u, w) = C(w, u) = \varepsilon$, soit $\bar{u}w \curvearrowright \varepsilon$.

(ii) Supposons que $C(v, u)$ existe. Appliquant le lemme 2.14 à $\bar{v}v' \curvearrowright \varepsilon$, on obtient que $C(v', u)$ existe et on a $\overline{C(v, u)}C(v', u) \curvearrowright \varepsilon$. L'existence de $C(v', u)$ entraîne que $C(u, v')$ existe. Appliquant le lemme 2.14 à $\bar{u}u'$, on obtient que $C(u', v')$ et, par conséquent, $C(v', u')$, existent, et on déduit $\overline{C(v', u)}C(v', u') \curvearrowright \varepsilon$. Comme X est clos par complément, les mots $\overline{C(v, u)}$, $\overline{C(v', u)}$ et $\overline{C(v', u')}$ appartiennent à X . Par (i), la conjonction de $\overline{C(v, u)}C(v', u) \curvearrowright \varepsilon$ et $\overline{C(v', u)}C(v', u') \curvearrowright \varepsilon$ entraîne $\overline{C(v, u)}C(v', u') \curvearrowright \varepsilon$. \square

On introduit maintenant des raffinements de la relation $\bar{u}v \curvearrowright \varepsilon$.

NOTATION 2.16 (**relation \equiv_X^p**). Pour X inclus dans S^* et u, u' dans S^* , on dit que $u \equiv_X^0 u'$ est vérifié pour $u = u' = \varepsilon$ et, pour $p \geq 1$, on dit que $u \equiv_X^p u'$ est vérifié s'il existe deux décompositions $u = u_1 \cdots u_p$, $u' = u'_1 \cdots u'_p$ telles que u_1, \dots, u'_p appartiennent à X et on a $\bar{u}_j u'_j \curvearrowright \varepsilon$ pour tout j .

La relation $u \equiv_X^1 u'$ est la conjonction de $\bar{u}u' \curvearrowright \varepsilon$ et de $u, u' \in X$.

LEMME 2.17. *Sous les hypothèses du lemme 2.14 :*

- (i) *Toute relation $u \equiv_X^p u'$ entraîne $\bar{u}u' \curvearrowright \varepsilon$.*
- (ii) *Les relations $u \equiv_X^p u'$ et $v \equiv_X^q v'$ entraînent soit $C(u, v) \equiv_X^q C(u', v')$ et $C(v, u) \equiv_X^p C(v', u')$, soit $C(u, v)$ et $C(u', v')$ n'existent pas.*

DÉMONSTRATION. (i) On montre le résultat par récurrence sur p . Pour $p = 0$, on a $u = u' = \varepsilon$, d'où, par définition, $\bar{u}u' \curvearrowright \varepsilon$. On suppose $p \geq 1$. Alors, on peut écrire $u = u_1u_2$ et $u' = u'_1u'_2$ avec $u_1 \equiv_X^1 u'_1$ et $u_2 \equiv_X^{p-1} u'_2$. On applique l'hypothèse de récurrence à $u_2 \equiv_X^{p-1} u'_2$ et on obtient $\bar{u}_2u'_2 \curvearrowright \varepsilon$. Comme, par définition, $u \equiv_X^1 u'$ implique $\bar{u}u' \curvearrowright \varepsilon$, on trouve

$$\bar{u}u' = \bar{u}_2 \bar{u}_1 u'_1 u'_2 \curvearrowright \bar{u}_2 u'_2 \curvearrowright \varepsilon.$$

(ii) Le résultat est vrai pour $p = 0$. En effet, pour $p = 0$, on a $u' = u = \varepsilon$, donc on trouve $C(u, v) \equiv_X^q C(u', v')$ et $C(v, u) = C(v', u') = \varepsilon$. Pour les mêmes raisons, le résultat est vrai pour $q = 0$.

Maintenant, on utilise une récurrence sur $p + q$. D'après ce qui précède, on peut supposer $u \equiv_X^p u'$ et $v \equiv_X^q v'$ avec $p \geq 1$ et $q \geq 1$. Alors, on peut écrire $u = u_1u_2$, $u' = u'_1u'_2$ avec $u_1 \equiv_X^1 u'_1$ et $u_2 \equiv_X^{p-1} u'_2$ et, de même, $v = v_1v_2$, $v' = v'_1v'_2$ avec $v_1 \equiv_X^1 v'_1$ et $v_2 \equiv_X^{q-1} v'_2$. Supposons que $C(u, v)$ existe. Alors, par construction, on a

$$(2.18) \quad C(u, v) = C(u_2, C(u_1, v_1))C(C(C(u_1, v_1), u_2), C(C(v_1, u_1), v_2)),$$

$$(2.19) \quad C(v, u) = C(v_2, C(v_1, u_1))C(C(C(v_1, u_1), v_2), C(C(u_1, v_1), u_2)).$$

L'hypothèse que l'ensemble X est clos par complément implique que $C(u_1, v_1)$ et $C(v_1, u_1)$ appartiennent à X . Or, par (i), on a $\bar{u}_1u'_1 \curvearrowright \varepsilon$ et $\bar{v}_1v'_1 \curvearrowright \varepsilon$. Par le lemme 2.15 (ii), les éléments $C(v'_1, u'_1)$ et $C(u'_1, v'_1)$ existent et on a $C(v_1, u_1) \equiv_X^1 C(v'_1, u'_1)$ et, de même, $C(u_1, v_1) \equiv_X^1 C(u'_1, v'_1)$.

On applique l'hypothèse de récurrence à $C(v_1, u_1) \equiv_X^1 C(v'_1, u'_1)$ et $v_2 \equiv_X^{q-1} v'_2$. Comme l'élément $C(C(v_1, u_1), v_2)$ existe, on trouve que $C(C(v'_1, u'_1), v'_2)$ existe et on a

$$(2.20) \quad C(C(v_1, u_1), v_2) \equiv_X^{q-1} C(C(v'_1, u'_1), v'_2),$$

$$(2.21) \quad C(v_2, C(v_1, u_1)) \equiv_X^1 C(v'_2, C(v'_1, u'_1)).$$

De même, on applique l'hypothèse de récurrence à $C(u_1, v_1) \equiv_X^1 C(u'_1, v'_1)$ et $u_2 \equiv_X^{p-1} u'_2$. Comme $C(C(u_1, v_1), u_2)$ existe, on trouve que $C(C(u'_1, v'_1), u'_2)$ existe et on a

$$(2.22) \quad C(C(u_1, v_1), u_2) \equiv_X^{p-1} C(C(u'_1, v'_1), u'_2),$$

$$(2.23) \quad C(u_2, C(u_1, v_1)) \equiv_X^1 C(u'_2, C(u'_1, v'_1)).$$

À nouveau, appliquant l'hypothèse de récurrence à (2.20) et (2.22), comme $C(C(C(v_1, u_1), v_2), C(C(u_1, v_1), u_2))$ existe, on obtient

$$(2.24) \quad C(C(C(v_1, u_1), v_2), C(C(u_1, v_1), u_2)) \\ \equiv_X^{q-1} C(C(C(v'_1, u'_1), v'_2), C(C(u'_1, v'_1), u'_2)),$$

$$(2.25) \quad C(C(C(u_1, v_1), u_2), C(C(v_1, u_1), v_2)) \\ \equiv_X^{p-1} C(C(C(u'_1, v'_1), u'_2), C(C(v'_1, u'_1), v'_2)).$$

Réunissant les relations (2.18), (2.19), (2.21), (2.23), (2.24) et (2.25), on trouve $C(u, v) \equiv_X^p C(u', v')$ et $C(v, u) \equiv_X^q C(v', u')$. \square

NOTATION 2.26 (**relation** \bowtie_X). Pour X inclus dans S^* et v, v' dans S^* , on dit que $v \bowtie_X v'$ est vérifié s'il existe deux décompositions $v = v_0 v_1 v_2 v_3$, $v' = v'_0 v'_1 v'_2 v'_3$ et deux entiers q et r vérifiant

$$v_0 \equiv_X^q v'_0, \quad v_3 \equiv_X^r v'_3, \quad v_1, v_2, v'_1, v'_2 \in X$$

$$C(v_1, v'_1) \text{ existe, } \overline{v_2} C(v_1, v'_1) \curvearrowright \varepsilon \text{ et } \overline{v'_2} C(v'_1, v_1) \curvearrowright \varepsilon.$$

LEMME 2.27. *Sous les hypothèses du lemme 2.14, la relation $v \bowtie_X v'$ entraîne $\overline{v} v' \curvearrowright \varepsilon$.*

DÉMONSTRATION. Avec les notations de 2.26, par le lemme 2.17, on a d'abord $\overline{v_0} v'_0 \curvearrowright \varepsilon$ et $\overline{v_3} v'_3 \curvearrowright \varepsilon$. On trouve alors

$$\begin{aligned} \overline{v} v' &= \overline{v_3} \overline{v_2} \overline{v_1} \overline{v_0} v'_0 v'_1 v'_2 v'_3 \\ &\curvearrowright \overline{v_3} \overline{v_2} \overline{v_1} v'_1 v'_2 v'_3 \\ &\curvearrowright \overline{v_3} \overline{v_2} C(v_1, v'_1) \overline{C(v'_1, v_1)} v'_2 v'_3 \curvearrowright \overline{v_3} v'_3 \curvearrowright \varepsilon. \end{aligned} \quad \square$$

LEMME 2.28. *Sous les hypothèses du lemme 2.14, les relations $u \equiv_X^p u'$ et $v \bowtie_X v'$ entraînent soit $C(u, v) \bowtie_X C(u', v')$ et $C(v, u) \equiv_X^p C(v', u')$, soit que $C(u, v)$ et $C(u', v')$ ne sont pas définis.*

DÉMONSTRATION. On démontre le résultat par récurrence sur p . Pour $p = 0$, la seule possibilité est $u = u' = \varepsilon$, donc on a $C(u, v) = v \bowtie_X v' = C(u', v')$ et $C(v, u) = C(v', u') = \varepsilon$. D'où le résultat.

Supposons $p = 1$. On fixe des décompositions $v = v_0 v_1 v_2 v_3$, $v' = v'_0 v'_1 v'_2 v'_3$ comme dans la définition 2.26 et on pose $u_0 = u$ et $u'_0 = u'$. Supposons que $C(u, v)$ existe. Alors, on définit de proche en proche $u_j = C(v_{j-1}, u_{j-1})$ et $w_j = C(u_j, v_j)$. Par hypothèse, on a $u_0 \equiv_X^1 u'_0$, $v_0 \equiv_X^q v'_0$ et u_1 existe, donc, par le lemme 2.17 (ii), les éléments $u'_1 = C(v'_0, u'_0)$ et $w'_0 = C(u'_0, v'_0)$ existent et on a $w_0 \equiv_X^q w'_0$ et $u_1 \equiv_X^1 u'_1$.

Ensuite, v_1 et v'_1 sont dans X , donc il en est de même de $C(v_1, v'_1)$ et $C(v'_1, v_1)$. Par hypothèse, on a $\overline{v_2} C(v_1, v'_1) \curvearrowright \varepsilon$, donc, par le lemme 2.17 appliqué à u_2, v_2 et $C(v_1, v'_1)$, comme u_3 existe, l'élément $C(C(v_1, v'_1), u_2)$ existe et on a

$$(2.29) \quad \overline{u_3} C(C(v_1, v'_1), u_2) \curvearrowright \varepsilon,$$

$$(2.30) \quad \overline{w_2} C(u_2, C(v_1, v'_1)) \curvearrowright \varepsilon.$$

Comme (v'_1, u_1, v_1) satisfait la condition du cube et que $C(C(v_1, v'_1), u_2)$ existe, on a

$$(2.31) \quad \overline{C(C(v_1, v'_1), u_2)} C(C(v'_1, v_1), C(v'_1, u_1)) \curvearrowright \varepsilon.$$

Comme tous les éléments de (2.29) et (2.31) sont dans X et que la relation $\overline{u} v \curvearrowright \varepsilon$ est transitive sur X , on en déduit que

$$(2.32) \quad \overline{u_3} C(C(v'_1, v_1), C(v'_1, u_1)) \curvearrowright \varepsilon.$$

Maintenant l'existence de $C(v'_1, u_1)$ et la relation $u_1 \equiv_X^1 u'_1$ impliquent, par le lemme 2.14, que $u'_2 = C(v'_1, u'_1)$ et $w'_1 = C(u'_1, v'_1)$ existent et on a

$$(2.33) \quad \overline{C(v'_1, u_1)}u'_2 \curvearrowright \varepsilon.$$

À nouveau l'existence de $C(C(v'_1, v_1), C(v'_1, u_1))$ et la relation (2.33) impliquent, par le lemme 2.14, que $C(C(v'_1, v_1), u'_2)$ existe et on a

$$(2.34) \quad \overline{C(C(v'_1, v_1), C(v'_1, u_1))}C(C(v'_1, v_1), u'_2) \curvearrowright \varepsilon.$$

Maintenant, par hypothèse, on a $\overline{v'_2}C(v'_1, v_1) \curvearrowright \varepsilon$, donc, par le lemme 2.17 appliqué à u'_2, v'_2 et $C(v'_1, v_1)$, comme $C(C(v'_1, v_1), u'_2)$ existe, les éléments $u'_3 = C(v'_2, u'_2)$ et $w'_2 = C(u'_2, v'_2)$ existent et on a

$$(2.35) \quad \overline{u'_3}C(C(v'_1, v_1), u'_2) \curvearrowright \varepsilon,$$

$$(2.36) \quad \overline{w'_2}C(u'_2, C(v'_1, v_1)) \curvearrowright \varepsilon.$$

Par les équations (2.32), (2.34) et (2.35) et la transitivité de la relation $\overline{uv} \curvearrowright \varepsilon$ dans X , on trouve $\overline{u_3}u'_3 \curvearrowright \varepsilon$, et même $u_3 \equiv_X^1 u'_3$ car u_3 et u'_3 appartiennent à X par construction.

La condition du cube satisfaite par (u_1, v'_1, v_1) et par (u'_1, v_1, v'_1) et la transitivité de X impliquent

$$(2.37) \quad \overline{w_2}C(w_1, C(u_1, v'_1)) \curvearrowright \varepsilon,$$

$$(2.38) \quad \overline{w'_2}C(w'_1, C(u'_1, v_1)) \curvearrowright \varepsilon.$$

De plus, comme on a $u_1 \equiv_X^1 u'_1$, le lemme 2.14 entraîne d'abord $\overline{C(u_1, v'_1)}w'_1 \curvearrowright \varepsilon$, d'où en utilisant (2.37), le lemme 2.14 à nouveau et la transitivité de \overline{uv} sur X ,

$$(2.39) \quad \overline{w_2}C(w_1, w'_1) \curvearrowright \varepsilon,$$

et, par un argument symétrique en utilisant(2.38),

$$(2.40) \quad \overline{w'_2}C(w'_1, w_1) \curvearrowright \varepsilon.$$

On sait que $u_3 \equiv_X^1 u'_3$ est vérifié et, par hypothèse, on a $v_3 \equiv_X^r v'_3$. En appliquant le lemme 2.17 (ii), comme w_3 existe, on trouve

$$(2.41) \quad w_3 \equiv_X^r C(u'_3, v'_3) = w'_3,$$

$$(2.42) \quad u_4 \equiv_X^1 C(v'_3, u'_3) = u'_4.$$

Donc, par construction, on a $C(u, v) = w_0w_1w_2w_3$, $C(u', v') = w'_0w'_1w'_2w'_3$, $C(v, u) = u_4$ et $C(v', u') = u'_4$. Alors, les relations $w_0 \equiv_X^r w'_0$, (2.39), (2.40) et (2.41) donnent $C(u, v) \curvearrowright_X C(u', v')$ et (2.42) donne $C(v, u) \equiv_X^1 C(v', u')$. D'où le résultat.

Pour finir, supposons $p \geq 2$. Donc on peut écrire $u = u_1u_2$, $u' = u'_1u'_2$ avec $u_1 \equiv_X^1 u'_1$ et $u_2 \equiv_X^{p-1} u'_2$. Supposons que $C(u, v)$ existe, alors $C(u_1, v)$ existe également. Donc, en appliquant l'hypothèse de récurrence à u_1, u'_1, v et v' , on obtient

$$(2.43) \quad C(u_1, v) \curvearrowright_X C(u'_1, v'),$$

$$(2.44) \quad C(v, u_1) \equiv_X^1 C(v', u'_1).$$

Ensuite, en utilisant (2.43) et le fait que $C(u_2, C(u_1, v))$, l'hypothèse de récurrence appliquée à $u_2, v_2, C(u_1, v)$ et $C(u'_1, v')$ donne

$$(2.45) \quad C(u_2, C(u_1, v)) \bowtie_X C(u'_2, C(u'_1, v')),$$

$$(2.46) \quad C(C(u_1, v), u_2) \equiv_X^{p-1} C(C(u'_1, v'), u'_2).$$

La relation (2.45) est $C(u, v) \bowtie_X C(u', v')$. De Surcroît, la concaténation de (2.44) et (2.46) donne $C(v, u) \equiv_X^p C(v', u')$. D'où le résultat. \square

On peut maintenant démontrer la proposition 2.8.

DÉMONSTRATION DE LA PROPOSITION 2.8. Supposons d'abord que le retournement à droite est complet pour la présentation (S, R) . Alors, d'après la proposition 1.24, la condition du cube est satisfaite pour tout triplet de S^* , donc, en particulier, pour tout triplet de \widehat{S} .

Réciproquement, on suppose que la condition du cube à droite est vraie pour tout triplet d'éléments deux à deux distincts de \widehat{S} . Par le lemme 1.25, la condition du cube à droite est donc vraie pour tout triplet d'éléments de \widehat{S} . D'après le lemme 2.7, il suffit de montrer que $u \equiv u'$ et $v \equiv v'$ entraînent soit $C(u, v) \equiv C(u', v')$ et $C(v, u) \equiv C(v', u')$, soit $C(u, v)$ et $C(u', v')$ ne sont pas définis. On suppose que $C(u, v)$ existe. Puisque \equiv est transitive, il suffit de le montrer dans le cas où on utilise exactement une relation de R pour passer de uv à $u'v'$. Donc on suppose que $u = u'$ et que v' est obtenu de v en utilisant une relation de R , c'est-à-dire en remplaçant un facteur sw par tw' tel que $sw = tw'$ est une relation de R (le cas $v = v'$ et u' obtenu de u en utilisant une relation de R est symétrique). On a donc des décompositions $v = v_0swv_3$ et $v' = v_0tw'v_3$. Soient p, q et r les longueurs des mots u, v_0 et v_3 . Par hypothèse, S est inclus dans \widehat{S} , donc $u = u'$ entraîne $u \equiv_{\widehat{S}}^p u'$ et, de même, on a $v_0 \equiv_{\widehat{S}}^q v_0$ et $v_3 \equiv_{\widehat{S}}^r v_3$, et, par conséquent, on a $v \bowtie_{\widehat{S}} v'$ par définition. Comme $C(u, v)$ existe, par le lemme 2.28, on obtient $C(u, v) \bowtie_{\widehat{S}} C(u, v')$ et $C(v, u) \equiv_{\widehat{S}}^p C(v', u)$. Maintenant, le lemme 2.17 (i) implique $\overline{C(v, u)C(v', u)} \curvearrowright \varepsilon$ d'où $C(v, u) \equiv C(v', u)$. De même, le lemme 2.27 implique $\overline{C(u, v)C(u, v')}$ $\curvearrowright \varepsilon$ d'où $C(u, v) \equiv C(u, v')$. \square

3. Un nouveau critère de terminaison

Avec la proposition 1.32, on a vu que, dans le cas d'une présentation par des relations courtes, le problème de terminaison du retournement est facile : en particulier, il est décidable algorithmiquement en temps fini. Dans le cas général, il n'en est plus de même : partant d'un mot signé w , si le retournement à partir de w réussit ou bloque, on peut le montrer en construisant étape par étape la suite des retournements menant au mot terminal, mais, si le retournement à partir de w ne termine pas, il n'y a *a priori* aucun moyen de le savoir : constater qu'on n'a pas atteint un mot terminal après un nombre fini N d'étapes ne constitue pas une preuve de non-terminaison.

On va établir ici un résultat permettant de résoudre le problème quand la clôture par complément est explicitement connue — en particulier quand elle est finie. Le principe général pour ce faire est, supposant qu'on part d'une présentation (S, R) et que S' est un ensemble de mots de S^* incluant S et clos par complément, de construire une nouvelle présentation (S', R') du monoïde $\langle S \mid R \rangle^+$ dont les relations sont courtes.

3.1. Les présentations (S', R') . Dans la suite, on va travailler avec deux alphabets simultanément, l'un inclus dans l'autre. Pour faire cela précisément, on fixe des notations convenables.

NOTATION 3.1 (**mots \underline{u} et $\text{dev}(w)$**). Si S est un alphabet et si S' est un ensemble de S -mots incluant S , on associe à chaque élément u de S' (qui est un S -mot) une copie disjointe notée \underline{u} et on note \underline{S}' l'ensemble de ces copies. Pour tout S -mot $w = s_1 s_2 \dots s_k$, on pose $\underline{w} := \underline{s}_1 \cdot \underline{s}_2 \cdot \dots \cdot \underline{s}_k$. Dans l'autre direction, si w est un \underline{S}' -mot, on note $\text{dev}(w)$ le S -mot obtenu en remplaçant chaque lettre \underline{u} de w par la valeur de u comme S -mot ("développement de w ").

On étend les correspondances ci-dessus aux mots signés de la façon évidente. Par définition, pour tout S -mot signé w , on a $\text{dev}(\underline{w}) = w$. Dans les exemples de \underline{S}' -mot, on séparera toujours par un point les lettres successives : par exemple, le \underline{S}' -mot \underline{ab} , de longueur 1, doit être distingué du \underline{S}' -mot $\underline{a} \cdot \underline{b}$, de longueur 2. Noter que tout ceci s'applique typiquement au cas où S' est la clôture \widehat{S} de S par complément à droite.

Si (S, R) est une présentation de monoïde et si S' est un ensemble de S -mots, on peut utiliser \underline{S}' comme un nouvel alphabet et définir une nouvelle présentation, dont on verra qu'elle est en un sens équivalente à (S, R) . Le point important ici est que, si S' est clos par retournement à droite, alors la nouvelle présentation n'a que des relations courtes.

DÉFINITION 3.2 (**relations $\text{Rel}(S, R, S')$**). Si (S, R) est une présentation complétée à droite et si S' est un ensemble de mots de S^* incluant S et clos par complément à droite, on note $\text{Rel}(S, R, S')$ l'ensemble des relations $\underline{u} \cdot \underline{v}' = \underline{v} \cdot \underline{u}'$ avec u, v dans S' et $u' = C_R(v, u)$ et $v' = C_R(u, v)$, dans le cas où ces derniers existent.

CONVENTION 3.3. Pour alléger l'écriture, on fait la convention que, dans la situation d'une présentation initiale (S, R) et d'un ensemble de mots noté S' , on écrit R' pour $\text{Rel}(S, R, S')$.

Noter que l'hypothèse que S' est clos par complément à droite est nécessaire pour que, dans la définition 3.2, les mots $C_R(v, u)$ et $C_R(u, v)$ appartiennent à S' .

EXEMPLE 3.4. Dans le contexte de l'exemple 2.6, c'est à dire

$$S = \{a, b, c\} \quad \text{et} \quad R = \{aba = bab, aca = cac, bcb = cbc\},$$

on a vu qu'on a $S' = \{a, b, c, ab, ba, ac, ca, cb, bc, \varepsilon\}$, et on trouve

$$R' = \{\underline{a} \cdot \underline{ba} = \underline{b} \cdot \underline{ab}, \underline{a} \cdot \underline{ca} = \underline{c} \cdot \underline{ac}, \underline{a} \cdot \underline{b} = \underline{ab}, \underline{a} \cdot \underline{ba} = \underline{ba} \cdot \underline{b}, \underline{a} \cdot \underline{c} = \underline{ac},$$

$$\begin{aligned} \underline{a} \cdot \underline{ca} &= \underline{ca} \cdot \underline{c}, \underline{b} \cdot \underline{cb} = \underline{c} \cdot \underline{bc}, \underline{b} \cdot \underline{ab} = \underline{ab} \cdot \underline{a}, \underline{b} \cdot \underline{a} = \underline{ba}, \underline{b} \cdot \underline{cb} = \underline{cb} \cdot \underline{c}, \\ \underline{b} \cdot \underline{c} &= \underline{bc}, \underline{c} \cdot \underline{ac} = \underline{ac} \cdot \underline{a}, \underline{c} \cdot \underline{a} = \underline{ca}, \underline{c} \cdot \underline{b} = \underline{cb}, \underline{c} \cdot \underline{bc} = \underline{bc} \cdot \underline{b}, \\ \underline{ab} \cdot \underline{a} &= \underline{ba} \cdot \underline{b}, \underline{ab} \cdot \underline{cb} = \underline{ac} \cdot \underline{bc}, \underline{ba} \cdot \underline{ca} = \underline{bc} \cdot \underline{ac}, \underline{ac} \cdot \underline{a} = \underline{ca} \cdot \underline{c}, \\ \underline{ca} \cdot \underline{ba} &= \underline{cb} \cdot \underline{ab}, \underline{cb} \cdot \underline{c} = \underline{bc} \cdot \underline{b} \}. \end{aligned}$$

Désormais, on suppose toujours que les présentations (S, R) considérées sont complémentées à droite. Si w est un \underline{S}' -mot, on n'a pas nécessairement $w = \underline{\text{dev}}(w)$; par contre, on a :

LEMME 3.5. *Pour tout \underline{S}' -mot w , on a $[w] = [\underline{\text{dev}}(w)]$ où l'on rappelle que $[w]$ est la classe d'équivalence de w par rapport à $\equiv_{R'}$.*

DÉMONSTRATION. Soit w un \underline{S}' -mot. Alors il existe u_1, \dots, u_r dans S' vérifiant $w = \underline{u_1} \cdot \dots \cdot \underline{u_r}$. On a donc $\text{dev}(w) = u_1 \cdots u_r$. Il suffit donc de montrer que, pour tout $1 \leq i \leq r$, si on note $u_i = s_{i_1} \cdots s_{i_p}$, on a $[u_i] = [s_{i_1} \cdots s_{i_p}]$. Soit u un élément de S' , on note $u = s_1 \cdots s_p$ sa décomposition en S -lettres, montrons par récurrence sur p que $[u] = [s_1 \cdots s_p]$ est vrai. Or on a $\overline{s_1}u \curvearrowright s_2 \cdots s_p$, d'où $C_R(s_1, u) = s_2 \cdots s_p$ et $C_R(u, s_1) = \varepsilon$. Dans R' , on a donc une relation $\underline{s_1} \cdot \underline{C_R(s_1, u)} = \underline{u}$. Ceci implique $[u] = [\underline{s_1} \cdot \underline{C_R(s_1, u)}]$. Maintenant, $C_R(s_1, u)$ est un élément de S' de longueur $p-1$, donc appliquer l'hypothèse de récurrence à $C_R(s_1, u)$ donne $[C_R(s_1, u)] = [s_2 \cdots s_p]$, d'où $[u] = [\underline{s_1} \cdot \underline{C_R(s_1, u)}] = [s_1 \cdots s_p]$. \square

En pratique, pour simplifier, on notera souvent S' pour \underline{S}' , même si, pour les exemples concrets de mots, on continuera de souligner les lettres pour éviter les ambiguïtés. Quoique facile, le résultat suivant est important :

PROPOSITION 3.6 (**présentations**). *Si (S, R) est une présentation complémentée à droite et si S' est un ensemble de S -mots incluant S et clos par R -complément à droite, la présentation (S', R') est complémentée à droite, elle ne contient que des relations courtes, et on a $\langle S' | R' \rangle^+ \simeq \langle S | R \rangle^+$.*

DÉMONSTRATION. Tout d'abord, la présentation (S', R') est complémentée à droite, puisque le (S, R) -retournement est déterministe et donc, pour tous u, v dans S' , il existe au plus un couple de S -mots (u', v') vérifiant $\overline{uv} \curvearrowright_R v'u'$.

Puis, R' est l'ensemble des relations $\underline{u} \cdot \underline{v'} = \underline{v} \cdot \underline{u'}$ pour u, v dans S' et $u' = C_R(v, u)$ et $v' = C_R(u, v)$. Donc R' ne contient que des relations courtes.

Puisque S^* est un monoïde libre, l'application de S dans $\langle S' | R' \rangle^+$ qui envoie chaque lettre s sur $[\underline{s}]$ (qui est \underline{s}) se prolonge en un homomorphisme

$$\phi^* : S^* \longrightarrow \langle S' | R' \rangle^+,$$

et une induction directe donne $\phi^*(w) = [w]$ pour tout w dans S^* .

Supposons que $u = v$ est une relation de R . Par hypothèse, u et v ne sont pas vides, et on peut écrire $u = su'$ et $v = tv'$ avec s, t dans S et u', v' dans S^* . Par définition, on a $u' = C_R(s, t)$, $v' = C_R(t, s)$, et u' et v'

appartiennent à S' car S est inclus dans S' , et S' est clos par complément à droite. Donc $\underline{s} \cdot \underline{u}' = \underline{t} \cdot \underline{v}'$ est une relation de R' et on a $\phi^*(u) = \phi^*(v)$. De là, inductivement, il résulte que, si w et w' sont deux S -mots \equiv_R -équivalents, alors on a $\phi^*(w) = \phi^*(w')$.

Par conséquent, ϕ^* se factorise par la projection canonique de S^* sur le monoïde $\langle S \mid R \rangle^+$, et induit un morphisme de monoïde

$$(3.7) \quad \phi : \langle S \mid R \rangle^+ \longrightarrow \langle S' \mid R' \rangle^+,$$

qui, par construction, envoie $[w]$ sur $[\underline{w}]$ pour tout S -mot w .

De même, puisque $(S')^*$ est un monoïde libre, l'application de S' dans le monoïde $\langle S \mid R \rangle^+$ qui envoie chaque lettre \underline{u} sur $[\text{dev}(\underline{u})]$, qui est $[u]$, se prolonge en un homomorphisme

$$\psi^* : (S')^* \longrightarrow \langle S \mid R \rangle^+,$$

et une induction directe donne $\psi^*(w) = [\text{dev}(w)]$ pour tout w dans S'^* .

Supposons que $\underline{u} \cdot \underline{v}' = \underline{v} \cdot \underline{u}'$ est une relation de R' . Par définition, on a $v' = C_R(u, v)$ et $u' = C_R(v, u)$, d'où

$$\psi^*(\underline{u} \cdot \underline{v}') = [uv'] = [uC_R(u, v)] = [vC_R(v, u)] = [vu'] = \psi^*(\underline{v} \cdot \underline{u}').$$

De là, inductivement, il résulte que, si w et w' sont deux S' -mots \equiv_R -équivalents, alors on a $\psi^*(w) = \psi^*(w')$. Par conséquent, ψ^* se factorise par la projection canonique de S'^* sur $\langle S' \mid R' \rangle^+$ et induit un morphisme de monoïde

$$(3.8) \quad \psi : \langle S' \mid R' \rangle^+ \longrightarrow \langle S \mid R \rangle^+,$$

qui, par construction, envoie $[w]$ sur $[\text{dev}(w)]$ pour tout S' -mot w .

Les définitions explicites et le lemme 3.5 montrent que les morphismes ϕ de (3.7) et ψ de (3.8) sont inverses l'un de l'autre, et sont donc des isomorphismes. \square

Puisque la présentation (S', R') ne contient que des relations courtes, elle est éligible à la proposition 1.32, et celle-ci implique donc directement :

LEMME 3.9. *Si (S, R) est une présentation complétée à droite et si S' est un sous-ensemble de S^* incluant S et clos par R -complément à droite, le R' -retournement termine toujours.*

C'est ce point qu'on va exploiter dans la suite.

3.2. Comparaison des retournements. Dans le contexte précédent, on a deux présentations (S, R) , (S', R') , toutes deux complétées à droite, pour le même monoïde. Il est donc naturel de comparer les retournements associés.

EXEMPLE 3.10. Considérons d'abord la présentation standard (1.5) du monoïde d'Artin-Tits de type \tilde{A}_2 . On a obtenu dans l'exemple 1.30

$$\bar{a}bc \curvearrowright_R \text{ba}\bar{b}\bar{a}c \curvearrowright_R \text{bacbac}\bar{a}b\bar{c}\bar{b}\bar{c} \bar{a}\bar{b}\bar{c} \bar{a},$$

et le R -retournement ne termine pas. En revanche, on trouve

$$\bar{\mathbf{a}} \cdot \mathbf{b} \cdot \mathbf{c} \curvearrowright_{R'} \mathbf{ba} \cdot \overline{\mathbf{ab}} \cdot \mathbf{c}.$$

Or on n'a pas de relation de la forme $\mathbf{ab} \cdot \dots = \mathbf{c} \cdot \dots$ dans R' , car les compléments $C_R(\mathbf{ab}, \mathbf{c})$ et $C_R(\mathbf{c}, \mathbf{ab})$ ne sont pas définies. Donc $\mathbf{ba} \cdot \overline{\mathbf{ab}} \cdot \mathbf{c}$ est $\curvearrowright_{R'}$ -terminal et, cette fois, le R' -retournement de $\bar{\mathbf{a}} \cdot \mathbf{b} \cdot \mathbf{c}$ bloque.

Avec la même présentation, considérons maintenant $w := \bar{\mathbf{a}}\mathbf{b}\bar{\mathbf{c}}\bar{\mathbf{a}}\bar{\mathbf{b}}\mathbf{c}\mathbf{c}$. La figure 6 montre que le R -retournement se termine (en 17 étapes) en le mot

$$\mathbf{baacbacca}\bar{\mathbf{a}}\bar{\mathbf{c}}\bar{\mathbf{b}}\bar{\mathbf{a}}\bar{\mathbf{c}}\bar{\mathbf{b}},$$

tandis que le R' -retournement se termine (en 10 étapes) en le mot

$$\mathbf{ba} \cdot \mathbf{a} \cdot \mathbf{cb} \cdot \mathbf{ac} \cdot \mathbf{ac} \cdot \overline{\mathbf{ca}} \cdot \overline{\mathbf{ab}} \cdot \overline{\mathbf{bc}},$$

et le premier est le développement du second.

L'exemple ci-dessus montre que passer du R -retournement au R' -retournement permet de remplacer la non-terminaison par un blocage. On va montrer que cette situation vaut dans tous les cas.

Dans tous les lemmes suivants, les démonstrations se font par induction sur la taille des diagrammes, définie comme le nombre de carrés élémentaires. Ce nombre est déterminé à partir de la suite des signes des étiquettes bordant le diagramme. Formellement, on considère des suites (finies) de signes $+$ et $-$, et on note $|\vec{\varepsilon}|_+$ (*resp.*, $|\vec{\varepsilon}|_-$) le nombre de $+$ (*resp.*, de $-$) dans une suite $\vec{\varepsilon}$.

DÉFINITION 3.11 (domaine). Pour toute suite de signes $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_\ell)$ finie, avec $\varepsilon_i = \pm$, on appelle *domaine* de $\vec{\varepsilon}$ l'ensemble $\mathcal{D}(\vec{\varepsilon})$ défini par

$$\mathcal{D}(\vec{\varepsilon}) := \begin{cases} \emptyset & \text{pour } \vec{\varepsilon} \text{ de la forme } + \dots + - \dots -, \\ \mathcal{D}(\vec{\varepsilon}') \cup \{(i, j)\} & \text{pour } \vec{\varepsilon} = \vec{\varepsilon}'_1 \frown (-+) \frown \vec{\varepsilon}'_2, \text{ avec } \vec{\varepsilon}' = \vec{\varepsilon}'_1 \frown (+-) \frown \vec{\varepsilon}'_2 \\ & \text{et } i = |\vec{\varepsilon}'_1|_+ \text{ et } j = |\vec{\varepsilon}'_1|_- + 1. \end{cases}$$

Par exemple, pour $\vec{\varepsilon} := + - + - - + - +$, on trouve

$$\begin{aligned} \mathcal{D}(\vec{\varepsilon}) &= \mathcal{D}(+ + - - - + - +) \cup \{(1, 1)\} \\ &= \mathcal{D}(+ + - - + - - +) \cup \{(1, 1), (2, 3)\} \\ &= \mathcal{D}(+ + - + - - - +) \cup \{(1, 1), (2, 3), (2, 2)\} \\ &= \mathcal{D}(+ + + - - - - +) \cup \{(1, 1), (2, 3), (2, 2), (2, 1)\} \\ &= \mathcal{D}(+ + + - - - + -) \cup \{(1, 1), (2, 3), (2, 2), (2, 1), (3, 4)\} \\ &= \mathcal{D}(+ + + - - + - -) \cup \{(1, 1), (2, 3), (2, 2), (2, 1), (3, 4), (3, 3)\} \\ &= \mathcal{D}(+ + + - + - - -) \cup \{(1, 1), (2, 3), (2, 2), (2, 1), (3, 4), (3, 3), (3, 2)\} \\ &= \mathcal{D}(+ + + + - - - -) \cup \{(1, 1), (2, 3), (2, 2), (2, 1), (3, 4), (3, 3), (3, 2), (3, 1)\} \\ &= \{(1, 1), (2, 3), (2, 2), (2, 1), (3, 4), (3, 3), (3, 2), (3, 1)\}. \end{aligned}$$

On associe maintenant à chaque mot signé une suite de signes.

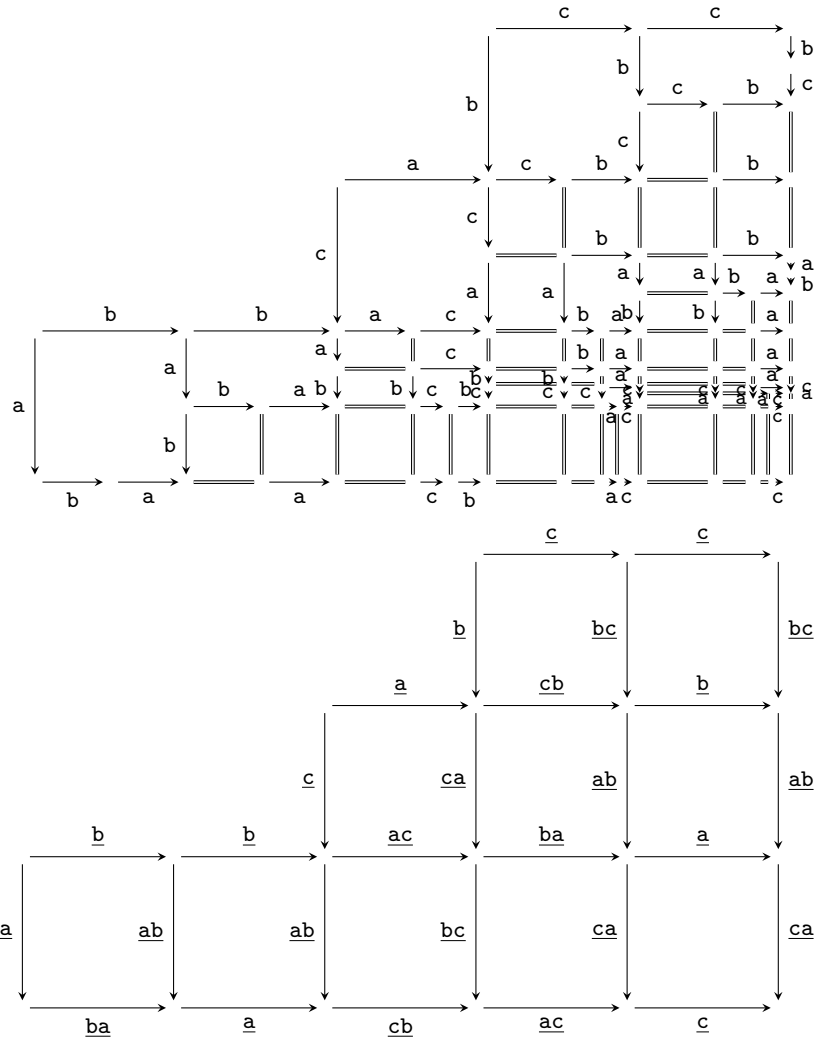


FIGURE 6. Comparaison du R et du R' -retournements du mot $\bar{a} \cdot \bar{b} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{c}$ pour la présentation du monoïde d'Artin-Tits de type A_2 .

DÉFINITION 3.12 ($\text{sign}(w)$). Si w est un mot signé, on note $\text{sign}(w)$ la suite définie par

$$\text{sign}(\varepsilon) := () \quad \text{et} \quad \text{sign}(w) := \begin{cases} + \frown \text{sign}(w') & \text{pour } w = sw', \\ - \frown \text{sign}(w') & \text{pour } w = \bar{s}w'. \end{cases}$$

Par exemple, pour $w = \bar{a}\bar{b}\bar{c}bc$, on a $\text{sign}(w) = + - - + +$.

Si le retournement d'un mot signé w réussit, il existe un diagramme de retournement, fini mais éventuellement très compliqué et dont le nombre de carrés ne peut pas être majoré *a priori*. On va montrer qu'on peut toujours

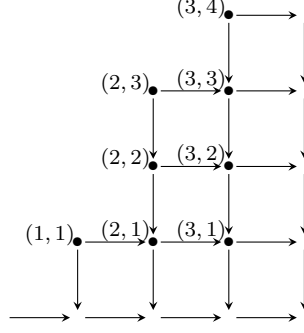


FIGURE 7. Le domaine de la suite $+ - + - - + - +$ possède 8 points, et le diagramme correspondant contient 8 carrés élémentaires.

regrouper ces carrés en une grille régulière, de taille bornée, et dont les étiquettes des côtés appartiennent à la clôture des lettres par complément à droite, formant une sorte de squelette pour le diagramme, sur le modèle de la figure 8. La démonstration formelle repose sur le lemme 1.9, qui permet de découper un diagramme de retournement.

LEMME 3.13. *Supposons que (S, R) est une présentation complétée à droite, que S' est un ensemble de mots de S^* incluant S et clos par R -complément à droite, et qu'on a $w \curvearrowright_R w' = v\bar{u}$ avec u, v dans S^* . Alors il existe des S -mots $u_{i,j}, v_{i,j}$ de S' , pour $0 \leq i \leq p$ et $0 \leq j \leq q$ avec p et q le nombre de $+$ et de $-$ dans $\text{sign}(w)$, vérifiant*

$$w' = v_{0,0}v_{1,0} \cdots v_{p-1,0}\overline{u_{p,1}} \overline{u_{p,2}} \cdots \overline{u_{p,q}}$$

et, pour tout (i, j) dans $\mathcal{D}(\text{sign}(w))$, $\overline{u_{i,j}}v_{i,j} \curvearrowright v_{i,j-1}\overline{u_{i+1,j}}$.

DÉMONSTRATION. On montre le résultat par induction sur l'entier $n := \#\mathcal{D}(\text{sign}(w))$. Supposons $n = 0$. Par définition, $\text{sign}(w)$ est de la forme $+\cdots+ -\cdots-$ et w est un S -mot positif-négatif que l'on note $w = s_{k_1}\cdots s_{k_p}\overline{s_{k_{p+1}}}\cdots\overline{s_{k_{p+q}}}$. Donc le seul retournement possible de w est $w \curvearrowright^0 w$ et on a $w = v\bar{u}$. On pose

$$v_{i,0} = s_{k_{i+1}}, \text{ pour } 0 \leq i \leq p-1, \text{ et } u_{p,j} = s_{k_{p+j}} \text{ pour } 1 \leq j \leq q.$$

On trouve alors $w = v_{0,0}v_{1,0} \cdots v_{p-1,0}\overline{u_{p,1}} \overline{u_{p,2}} \cdots \overline{u_{p,q}}$, ce qui donne le résultat.

Supposons $n \geq 1$. Alors il existe k avec $1 \leq k \leq p+q$ vérifiant $\text{sign}(w)[k] = -$ et $\text{sign}(w)[k+1] = +$. Donc on a $w = w''\bar{s}tw'''$ avec

$$\text{sign}(w'') = \text{sign}(w)[1] \cdots \text{sign}(w)[k-1]$$

$$\text{sign}(w''') = \text{sign}(w)[k+2] \cdots \text{sign}(w)[p+q].$$

Par le lemme 1.9 appliqué à $w \curvearrowright v\bar{u}$ avec $w_1 = w''\bar{s}t$ et $w_2 = w'''$, il existe dans S^* des décompositions $u = u_1u_2$, $v = v_1v_2$ et $u_0, v_0 \in S^*$ satisfaisant $w_1 \curvearrowright v_1\overline{u_0}$, $w_2 \curvearrowright v_0\overline{u_1}$ et $\overline{u_0}v_0 \curvearrowright v_2\overline{u_2}$. À nouveau par le lemme 1.9 appliqué à $w_1 = w''\bar{s}t \curvearrowright v_1u_0$ avec la décomposition $w_1 = w'_1w'_2$ pour $w'_1 = w''$ et

$w'_2 = \bar{s}t$, il existe des décompositions $u_0 = u'_1 u'_2$, $v_1 = v'_1 v'_2$ et $u'_0, v'_0 \in S^*$ satisfaisant $w'' \curvearrowright v'_1 \bar{u}'_0$, $\bar{s}t \curvearrowright v'_0 u'_1$ et $\bar{u}'_0 v'_0 \curvearrowright v'_2 u'_2$. Or, s et t appartiennent à S' et S' est clos par complément à droite, donc v'_0 et u'_1 appartiennent à S' . On pose

$$w_0 := w'' v'_0 \bar{u}'_1 w'''.$$

Par définition de w_0 , on trouve

$$\text{sign}(w) = \text{sign}(w'') \hat{-} + \hat{-} \text{sign}(w''') \text{ et } \text{sign}(w_0) = \text{sign}(w'') \hat{-} + \hat{-} \text{sign}(w'''),$$

d'où $\#\mathcal{D}(\text{sign}(w_0)) = n - 1$. Par l'hypothèse de récurrence appliquée à $w_0 \curvearrowright w'$, il existe des S -mots $u_{i,j}, v_{i,j}$ de S' , pour $0 \leq i \leq p$ et $0 \leq j \leq q$, vérifiant $w' = v_{0,0} v_{1,0} \cdots v_{p-1,0} \bar{u}_{p,1} \bar{u}_{p,2} \cdots \bar{u}_{p,q}$ et, pour tout (i, j) dans $\mathcal{D}(\text{sign}(w_0))$, $\bar{u}_{i,j} v_{i,j} \curvearrowright v_{i,j-1} \bar{u}_{i+1,j}$.

Maintenant, on pose $p'' = |\text{sign}(w'')|_+$, $q'' = |\text{sign}(w'')|_- + 1$ et

$$u_{p'',q''} = s \text{ et } v_{p'',q''} = t.$$

Donc il existe des S -mots $u_{i,j}, v_{i,j}$ de S' , pour tout (i, j) dans $\mathcal{D}(\text{sign}(w))$, vérifiant $\bar{u}_{i,j} v_{i,j} \curvearrowright v_{i,j-1} \bar{u}_{i+1,j}$. \square

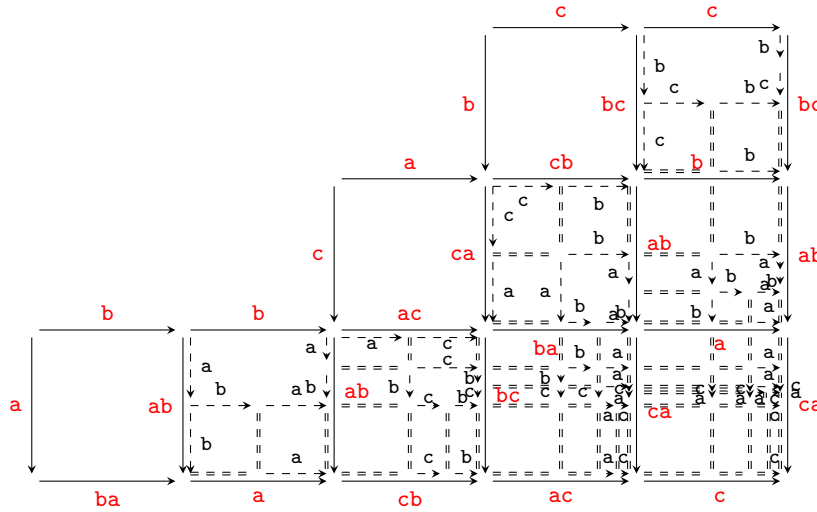


FIGURE 8. Le diagramme de R -retournement de $\bar{a}bb\bar{c}\bar{a}b\bar{c}c$ est inscrit dans une grille dont les côtés sont étiquetés par des éléments de S' . On a par exemple $u_{1,1} = ab$, $v_{2,1} = ac$ et $u_{5,3} = bc$.

On peut maintenant énoncer le résultat principal de comparaison des R - et R' -retournements :

PROPOSITION 3.14 (comparaison). *Si (S, R) est une présentation complétement à droite et S' est un ensemble de mots de S^* incluant S et clos par R -complément à droite, alors, pour tout S -mot signé w , si le R -retournement de w réussit, le R' -retournement de \underline{w} réussit aussi. Réciproquement, pour*

tout S' -mot signé w , si le R' -retournement de w réussit, alors le R -retournement de $\text{dev}(w)$ réussit.

DÉMONSTRATION. Soit w un S -mot signé tel que w se R -retourne en $v\bar{u}$. Soit p et q le nombre de $+$ et de $-$ dans $\text{sign}(w)$, c'est-à-dire le nombre de lettres positives et négatives dans w . Par le lemme 3.13, il existe, pour $0 \leq i \leq p$ et $0 \leq j \leq q$, des S -mots $u_{i,j}$ et $v_{i,j}$, qui sont dans S' et vérifient

$$u = u_{p,q} \cdots u_{p,1}, \quad v = v_{0,0} \cdots v_{p-1,0},$$

et, pour tout (i, j) dans $\mathcal{D}(\text{sign}(w))$,

$$(3.15) \quad \overline{u_{i,j} v_{i,j}} \curvearrow_R v_{i,j-1} \overline{u_{i+1,j}}.$$

Par définition, chaque relation de (3.15) implique

$$(3.16) \quad \overline{u_{i,j}} \cdot \overline{v_{i,j}} \curvearrow_{R'} v_{i,j-1} \cdot \overline{u_{i+1,j}}.$$

d'où, par définition du R' -retournement,

$$(3.17) \quad \underline{w} \curvearrow_{R'} \underline{v_{0,0}} \cdots \cdots \underline{v_{p-1,0}} \cdot \overline{u_{p,1}} \cdots \cdots \overline{u_{p,q}}.$$

Par conséquent, le R' -retournement de \underline{w} réussit.

Réciproquement, on montre par induction sur le nombre d'étapes de retournement m que, si w est un S' -mot signé et que w se R' -retourne en w' , alors $\text{dev}(w)$ se R -retourne en $\text{dev}(w')$. Pour $m = 0$, on a $w' = w$ et $\text{dev}(w') = \text{dev}(w)$, et le résultat est vrai. Supposons $m \geq 1$. Alors il existe w'' vérifiant $w \curvearrow_{R'}^1 w'' \curvearrow_{R'}^{m-1} w'$. Par construction, il existe des S' -mots signés w_1, w_2 et des éléments $\underline{u}, \underline{v}$ de S' satisfaisant $w = w_1 \cdot \overline{u} \cdot \underline{v} \cdot w_2$ et $w'' = w_1 \cdot \overline{C_R(u, v)} \cdot \overline{C_R(v, u)} \cdot w_2$. Par définition, on a $\text{dev}(w'') = \text{dev}(w_1) \overline{C_R(u, v)} \overline{C_R(v, u)} \text{dev}(w_2)$, et donc $\text{dev}(w) \curvearrow_R \text{dev}(w'')$. Ensuite, par hypothèse de récurrence,

$$w'' \curvearrow_{R'}^{m-1} w' \quad \text{entraîne} \quad \text{dev}(w'') \curvearrow_R \text{dev}(w').$$

Par transitivité de \curvearrow_R , on déduit $\text{dev}(w) \curvearrow_R \text{dev}(w')$.

Par le résultat précédent appliqué au cas où w' est un mot positif-négatif, on obtient que, si un S' -mot signé w se R' -retourne en un mot R' -terminal $u\bar{v}$, alors le mot $\text{dev}(w)$ se R -retourne en $\text{dev}(u\bar{v})$, qui est $\text{dev}(u)\overline{\text{dev}(v)}$, un S -mot signé R -terminal. \square

3.3. Application à la terminaison. En égard à la trichotomie « réussit/bloque/ne termine pas » et au lemme 3.9 qui exclut la non-terminaison pour (S', R') , la proposition 3.14 fournit un critère permettant de reconnaître la terminaison grâce à l'étude du R' -retournement :

PROPOSITION 3.18 (critère de terminaison II). *Si (S, R) est une présentation complétée à droite et si S' est un ensemble de mots de S^* incluant S et clos par R -complément à droite, alors le R -retournement d'un S -mot signé w termine si, et seulement si, le R' -retournement du S' -mot signé \underline{w} termine.*

DÉMONSTRATION. Par la proposition 3.14, si le R -retournement de w réussit, alors le R' -retournement de \underline{w} réussit également. Si le R -retournement de w bloque, alors le R' -retournement de \underline{w} bloque également. Enfin, si le R -retournement de w ne termine pas, le R' -retournement de \underline{w} bloque. \square

Le critère de la proposition 3.18 est utile, mais il n'entraîne pas automatiquement l'existence d'un algorithme décidant la terminaison du retournement. En effet, le problème de la récursivité des ensembles S' et R' , c'est-à-dire l'existence d'un algorithme reconnaissant si un mot ou une paire de mots est, respectivement, dans S' ou dans R' , se pose. Même si on part d'une présentation (S, R) finie, donc récursive, le problème est non trivial. Typiquement, il se peut que l'ensemble S' soit infini, et qu'on ne sache pas le déterminer en pratique. Dans ce cas, il en est de même de R' , et on ne peut rien conclure. Par contre, on peut noter :

LEMME 3.19. *Si (S, R) est une présentation complétée à droite, et s'il existe un ensemble fini S' incluant S et clos par R -complément à droite, alors la présentation (S', R') est finie, donc récursive.*

DÉMONSTRATION. Si u et v sont des mots de S' , les seuls mots u', v' susceptibles de vérifier $\bar{u}v \curvearrowright_R v'u'$ sont, par hypothèse, dans S' , et on peut donc tester en temps fini la relation. \square

Noter qu'il existe un ensemble fini S' comme ci-dessus si, et seulement si, la clôture \widehat{S} de S par R -complément à droite est finie, puisque, par définition, elle est le plus petit tel ensemble. On peut donc énoncer :

COROLLAIRE 3.20 (**décidabilité**). *Si (S, R) est une présentation de monoïde complétée à droite et si la clôture de S par R -complément à droite est finie, alors la terminaison du R -retournement est un problème décidable.*

DÉMONSTRATION. Par la proposition 3.18, et étant donné que le blocage du R -retournement est décidable, la décidabilité de la terminaison du R -retournement se réduit à celle du non-blocage du R' -retournement, qui est décidable puisque, par le lemme 3.19, (S', R') est une présentation finie. \square

Ce résultat de décidabilité s'applique donc en particulier aux présentations des exemples 1.30 (monoïde d'Artin–Tits de type \widetilde{A}_2) et 2.9 (monoïde d'Artin–Krammer AK_3).

Utilisation du retournement

Ce chapitre a pour but d'établir de nouveaux résultats, principalement à l'étude du monoïde H^+ qui est notre sujet principal, à l'aide de la méthode du retournement décrite dans le chapitre III. Les principaux résultats obtenus sont des propriétés de simplification, d'existence de multiples communs et de ppcm (plus petit multiple commun), et des solutions au problème de mots.

Le chapitre est organisé en trois sections. Dans la section 1, on montre (il s'agit souvent de rappels de résultats connus) comment le retournement peut, d'une façon générale, être utilisé pour montrer de tels résultats dans le cas d'une présentation quelconque, pour autant qu'il soit complet et décidable. Dans les sections 2 et 3, on considère le cas particulier de la présentation (\mathcal{P}) du monoïde H^+ . Dans la section 2, on établit la complétude du retournement à droite, et on en déduit des résultats de simplifiabilité (proposition A de l'introduction) et de ppcm conditionnel. Dans la section 3, on étudie la terminaison du retournement à droite associé à (\mathcal{P}) grâce à la construction d'un ensemble (infini) de mots clos par complément à droite, et on en déduit des résultats de décidabilité et de complexité algorithmique pour le problème de mots et l'existence de multiples communs à droite (proposition B de l'introduction). Enfin, dans un bref appendice final, on montre que le choix des relations définissant le monoïde H^+ n'est pas arbitraire, tout autre choix pour les relations de longueur 3 sur le modèle de celles de (\mathcal{P}) menant à un retournement à droite non complet, donc essentiellement inutilisable.

1. Principes généraux

On rappelle d'abord quelques résultats généraux valables dès que le retournement est complet et/ou terminant. Les démonstrations sont en général faciles, et on les donne rapidement. On rappelle que, si (S, R) est une présentation de monoïde, alors la congruence sur S^* engendrée par R est notée \equiv_R (ou parfois simplement \equiv). Si u est un mot de S^* , l'élément du monoïde $\langle S \mid R \rangle^+$ qui est la classe d'équivalence de u vis-à-vis de \equiv_R est notée $[u]_R$, ou, simplement, $[u]$.

1.1. Simplifiabilité. La première application du retournement est de fournir un critère de simplifiabilité, problème en général délicat.

PROPOSITION 1.1 (simplifiabilité). *Si (S, R) est une présentation complétée à droite pour laquelle le retournement à droite est complet, le monoïde $\langle S \mid R \rangle^+$ est simplifiable à gauche.*

DÉMONSTRATION. Soient s dans S et u, v dans S^* satisfaisant $su \equiv_R sv$. La complétude implique $\bar{u}\bar{s}sv \curvearrowright \varepsilon$. Le premier retournement se fait forcément en $\bar{s}s$. Or, comme on n'a pas de relation $s\dots = s\dots$, la suite de retournement à partir de $\bar{u}v$ a nécessairement la forme

$$\bar{u}\bar{s}sv \curvearrowright \bar{u}v \curvearrowright \dots \curvearrowright \varepsilon.$$

On a donc $\bar{u}v \curvearrowright \varepsilon$, d'où $u \equiv_R v$. Donc $su \equiv_R sv$ implique $u \equiv_R v$. Autrement dit, dans le monoïde $\langle S \mid R \rangle^+$, la relation $s[u] = s[v]$ implique $[u] = [v]$. De là, $\langle S \mid R \rangle^+$ est simplifiable à gauche. \square

EXEMPLE 1.2. On a vérifié que le retournement à droite est complet pour la présentation (I.2.2) du monoïde de tresses B_∞^+ . On déduit donc immédiatement que B_∞^+ est simplifiable à gauche. La symétrie de la présentation implique alors la simplifiabilité à droite sans nouvelle démonstration.

On a évidemment un résultat symétrique pour la simplifiabilité à droite en utilisant le retournement à gauche :

PROPOSITION 1.3 (**simplifiabilité**). *Si (S, R) est une présentation complétée à gauche pour laquelle le retournement à gauche est complet, le monoïde $\langle S \mid R \rangle^+$ est simplifiable à droite.*

Par contre, aucun résultat notable n'est connu concernant l'utilisation du retournement à droite pour établir des résultats de simplifiabilité à droite, même dans des cas très bien compris comme celui des tresses. Voir [16] pour quelques observations très partielles.

1.2. Multiples communs. Une autre application classique de la méthode du retournement à droite est l'obtention de multiples communs à droite, voire celle de ppcm.

D'abord, la proposition III.1.18 implique directement :

LEMME 1.4. *Si (S, R) est une présentation de monoïde complétée à droite, et si le retournement du S -mot signé $\bar{u}v$ réussit, alors les éléments $[u]$ et $[v]$ admettent un multiple à droite commun dans $\langle S \mid R \rangle^+$.*

DÉMONSTRATION. En effet, $\bar{u}v \curvearrowright_R v'\bar{u}'$ implique $uv' \equiv_R vu'$, donc $[uv']$ est multiple à droite de $[u]$ et $[v]$ dans $\langle S \mid R \rangle^+$. \square

Quand cette situation est générale, on déduit :

PROPOSITION 1.5 (**multiple commun**). *Si (S, R) est une présentation de monoïde complétée à droite pour laquelle le retournement à droite est toujours terminant, alors le monoïde $\langle S \mid R \rangle^+$ admet des multiples communs à droite.*

REMARQUE 1.6. Le résultat ci-dessus n'utilise pas vraiment l'hypothèse que la présentation est complétée : pour peu qu'on étende la définition du retournement au cas d'une présentation sans ε -relation quelconque (voir par exemple [21]), le résultat de la proposition 1.5 reste valable.

Par contre, l'hypothèse de complémentation donne un résultat plus fort, dans le cas où le retournement est complet :

LEMME 1.7. *Si (S, R) est une présentation de monoïde complétement à droite pour laquelle le retournement à droite est complet, et si le retournement du S -mot signé $\bar{u}v$ réussit en menant au mot terminal $v'\bar{u}'$, alors les éléments $[u]$ et $[v]$ admettent dans $\langle S \mid R \rangle^+$ un ppcm à droite, à savoir $[uv']$.*

DÉMONSTRATION. Supposons $\bar{u}v \curvearrowright_R v'\bar{u}'$. On a vu dans le lemme 1.4 que $[uv']$ est multiple à droite de $[u]$ et $[v]$ dans $\langle S \mid R \rangle^+$. Soit $[u][v''] = [v][u''']$ un multiple à droite commun quelconque à $[u]$ et $[v]$. On a alors $uv'' \equiv_R vu'''$, d'où, par complétude, $\bar{v}''\bar{u}v u'' \curvearrowright_R \varepsilon$. Appliquant de façon répétée le lemme III.1.10, on déduit l'existence de deux mots positifs u''', v''' vérifiant

$$\bar{u}v \curvearrowright v'\bar{u}', \quad \bar{u}'u'' \curvearrowright v''', \quad \bar{v}''v' \curvearrowright \bar{u}''', \quad \text{et} \quad \bar{u}''v''' \curvearrowright \varepsilon.$$

La proposition III.1.18 implique alors $uv'' \equiv_R uv'u'''$, donc $[uv''] = [uv'] \cdot [u''']$ dans $\langle S \mid R \rangle^+$: tout multiple à droite commun à $[u]$ et $[v]$ est multiple à droite de $[uv']$, et donc $[uv']$ est ppcm à droite de $[u]$ et $[v]$. \square

On rappelle qu'on dit qu'un monoïde M admet des ppcm à droite conditionnels si deux éléments quelconques de M qui ont au moins un multiple à droite commun ont un ppcm à droite. Le lemme 1.7 entraîne :

PROPOSITION 1.8 (**ppcm conditionnels**). *Si (S, R) est une présentation de monoïde complétement à droite pour laquelle le retournement à droite est complet, alors le monoïde $\langle S \mid R \rangle^+$ admet des ppcm à droite conditionnels. De plus, l'opération partielle $C_R(-, -)$ calcule le complément à droite : pour tous mots u, v de S^* , on a $[u] \setminus [v] = C_R(u, v)$ quand il existe.*

En rapprochant les propositions 1.5 et 1.8, on déduit

COROLLAIRE 1.9 (**ppcm**). *Si (S, R) est une présentation de monoïde complétement à droite pour laquelle le retournement à droite est complet et toujours terminant, alors le monoïde $\langle S \mid R \rangle^+$ admet des ppcm à droite.*

Par ailleurs, on a rappelé dans la proposition I.1.24 que, dans un monoïde noethérien à droite, l'existence de ppcm conditionnels implique celle des pgcd à gauche. On peut donc énoncer :

PROPOSITION 1.10 (**pgcd**). *Si (S, R) est une présentation de monoïde complétement à droite, noethérienne à droite et pour laquelle le retournement à droite est complet, alors le monoïde $\langle S \mid R \rangle^+$ admet des pgcd à gauche ; plus généralement, toute partie non vide de $\langle S \mid R \rangle^+$ admet un pgcd à gauche.*

EXEMPLE 1.11. Comme rappelé dans l'exemple 1.2, le retournement à droite est complet pour la présentation (I.2.2) de B_∞^+ , qui est trivialement noethérienne. On en déduit que B_∞^+ admet des ppcm à droite conditionnels et des pgcd à gauche, puis, par symétrie, des ppcm à gauche conditionnels et des pgcd à droite. Par contre, on n'a pas abordé la terminaison du retournement pour (I.2.2) : les propriétés des éléments de Garside Δ_n impliquent l'existence

de multiples communs, donc celle de ppcm, mais celle-ci n'est pas obtenue ici comme application du retournement.

1.3. Le problème de mots. Si le retournement est récursif, complet et termine toujours, alors on va voir facilement qu'il fournit une solution au problème de mots. Par contre, si le retournement ne termine pas toujours, la question est plus délicate, mais on va voir que, s'il existe un ensemble de mots clos par complément, alors on peut encore obtenir une solution.

Commençons par le cas où le retournement termine toujours.

PROPOSITION 1.12 (problème de mots I). *Si (S, R) est une présentation complétée à droite récursive pour laquelle le retournement à droite est complet et termine toujours, alors le problème de mots pour (S, R) est décidable.*

DÉMONSTRATION. Dès lors que (S, R) est récursive, le retournement est une relation récursive. Soient u, v deux mots de S^* . Par hypothèse, il existe un mot \curvearrowright -terminal w satisfaisant $\bar{u}v \curvearrowright w$. Comme le retournement est complet, les mots u et v sont équivalents si, et seulement si, le mot w est non vide. \square

Pour ce qui est de la complexité de l'algorithme ainsi obtenu, tout dépend de la longueur des relations de la présentation :

PROPOSITION 1.13 (complexité I). *Si (S, R) est une présentation complétée à droite finie ne contenant que des relations courtes et pour laquelle le retournement à droite est complet, alors le problème de mots pour (S, R) a une complexité en $O(n^2)$.*

DÉMONSTRATION. À nouveau, $u \equiv_R v$ équivaut à $\bar{u}v \curvearrowright_R \varepsilon$. Dès lors que toutes les relations de R sont courtes, si les mots u et v ont pour longueur p et q , alors le diagramme de retournement de $\bar{u}v$ contient au plus pq carrés non triviaux, et l'ensemble de la procédure requiert au plus $O(\max(p, q)^2) \cdot N$ étapes élémentaires, où N est une borne supérieure pour le coût en étapes élémentaires d'un R -retournement $\bar{u}v$ pour u, v dans S . Si S , donc R , est fini, la borne N est finie, et on obtient une borne supérieure quadratique. \square

Lorsque S est infini, ou lorsque R contient des relations qui ne sont pas courtes, même dans le cas où la longueur des mots est préservée, il est difficile d'obtenir des bornes de complexité. Signalons l'existence d'une présentation complétée à droite, infinie mais pour laquelle le retournement est complet et toujours terminant, et tel que la seule borne supérieure de complexité pour le retournement, et de là pour le problème de mots associé, est une tour d'exponentielles de hauteur exponentielle [19, chapitre VIII].

Les résultats de la section III.3 permettent d'obtenir de nouveaux énoncés basés sur l'utilisation d'ensembles de mots clos par complément.

PROPOSITION 1.14 (problème de mots II). *Si (S, R) est une présentation complétée à droite, récursive et pour laquelle le R -retournement*

à droite est complet, et s'il existe un sous-ensemble récursif S' de S^* incluant S , clos par R -complément à droite, et tel que la famille de relations associée R' est récursive, alors le problème de mots pour (S, R) est décidable.

DÉMONSTRATION. Soient u, v deux S -mots. Alors u et v représentent le même élément de $\langle S | R \rangle^+$ si, et seulement si, le R -retournement de $\bar{u}v$ termine avec le mot vide, donc, par la proposition III.3.14, si, et seulement si, le R' -retournement du S' -mot signé $\bar{u} \cdot v$ termine avec le mot vide. Par construction, le R' -retournement termine toujours, donc, pour autant que R' soit un ensemble récursif, la relation $\bar{u} \cdot v \curvearrowright_{R'} \varepsilon$ est décidable. \square

À nouveau, on n'en déduit pas directement de borne de complexité, sauf dans le cas où la présentation (S', R') est finie — ce qui ne peut se produire que si (S, R) est elle-même finie.

PROPOSITION 1.15 (complexité II). *Si (S, R) est une présentation complémentée à droite pour laquelle le R -retournement à droite est complet, et qu'il existe un ensemble fini S' de mots de S^* incluant S , clos par R -complément, et tel que l'ensemble R' associé est fini, alors le problème de mots pour (S, R) a une complexité en $O(n^2)$.*

DÉMONSTRATION. L'argument est le même que pour la proposition 1.13 : il s'agit cette fois d'évaluer la complexité de la relation « $\bar{u} \cdot v \curvearrowright_{R'} \varepsilon$ », pour un ensemble de relations R' ne contenant que des relations courtes. Pour autant que S' et R' soient récursifs, cela peut être fait en un nombre d'étapes borné supérieurement par $O(n^2) \cdot N$, où N est le coût maximal du R -retournement de $\bar{u}v$ pour u, v dans S' . Si S' , donc R' , est fini, N est fini, et on obtient une borne supérieure quadratique. \square

EXEMPLE 1.16. Considérons à nouveau la présentation (III.1.5) du monoïde d'Artin-Tits de type \hat{A}_2 . On a donné des exemples de couples de mots (u, v) de S^* pour lesquels le R -retournement de $\bar{u}v$ ne se termine pas, et la proposition 1.12 ne permet pas de résoudre le problème de mots par retournement. Mais, on a vu dans l'exemple III.2.6 que la clôture de $S := \{a, b, c\}$ par R -complément à droite est l'ensemble fini

$$S' = \hat{S} = \{a, b, c, \varepsilon, ab, ba, ac, ca, bc, cb\},$$

et on a donné la présentation (S', R') correspondante, qui est complémentée à droite et n'a que des relations courtes. De plus, on a affirmé que le R -retournement à droite est complet, et il résulte de la proposition III.3.14 qu'il en est de même du R' -retournement. Par conséquent, la présentation (III.1.5) est éligible au critère de la proposition 1.15, et tant la terminaison du R -retournement que son problème de mots peuvent être résolus effectivement en temps quadratique par R' -retournement.

Par exemple, pour $u := abcacbab$ et $v := bacbccbb$, on trouve

$$\begin{aligned} \bar{u} \cdot v &= \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{c} \cdot \bar{b} \cdot \bar{a} \cdot b \cdot a \cdot c \cdot b \cdot c \cdot c \cdot b \cdot b \\ &\curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{c} \cdot \bar{b} \cdot \bar{ba} \cdot \bar{ab} \cdot a \cdot c \cdot b \cdot c \cdot c \cdot b \cdot b \end{aligned}$$

$$\begin{aligned}
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{c} \cdot \underline{a} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{c} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \underline{ac} \cdot \overline{ca} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{c} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \underline{c} \cdot \overline{ca} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{c} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \overline{ca} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{c} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \cdots \curvearrowright_{R'} \bar{b} \cdot \overline{ab} \cdot \underline{c} \cdot \underline{b} \cdot \underline{b} :
\end{aligned}$$

il n'y a pas de relation de la forme $\underline{ab} \cdot \dots = \underline{c} \cdot \dots$ dans R' . Donc le R' -retournement de $\bar{u} \cdot \underline{v}$ bloque : par conséquent, le R -retournement de $\bar{u}v$ ne termine pas, et u et v ne sont pas \equiv_R -équivalents.

Par contraste, pour $u := \text{abcacbab}$ et $v := \text{bacbcabb}$, il vient

$$\begin{aligned}
\bar{u} \cdot \underline{v} &= \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{c} \cdot \bar{b} \cdot \bar{a} \cdot \underline{b} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{a} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{c} \cdot \bar{b} \cdot \underline{ba} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{a} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \bar{c} \cdot \underline{a} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{a} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \bar{a} \cdot \underline{ac} \cdot \overline{ca} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{a} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \bar{c} \cdot \underline{c} \cdot \overline{ca} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{a} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \bar{b} \cdot \bar{a} \cdot \bar{b} \cdot \overline{ca} \cdot \overline{ab} \cdot \underline{a} \cdot \underline{c} \cdot \underline{b} \cdot \underline{c} \cdot \underline{a} \cdot \underline{b} \cdot \underline{b} \\
& \curvearrowright_{R'} \cdots \curvearrowright_{R'} \varepsilon :
\end{aligned}$$

le R' -retournement de $\bar{u} \cdot \underline{v}$ termine avec le mot vide. Par conséquent, il en est de même du R -retournement de $\bar{u}v$, et les mots u et v sont équivalents.

EXEMPLE 1.17. Pour terminer, considérons la présentation (I.2.2) du monoïde de tresses B_∞^+ . Soit Δ_n l'élément de B_∞^+ défini inductivement par les relations

$$\Delta_1 = 1, \quad \Delta_n = \Delta_{n-1} \sigma_{n-1} \dots \sigma_2 \sigma_1 \text{ pour } n \geq 2.$$

On sait, d'après [37, 38], que Δ_n est ce qu'on appelle maintenant un élément de Garside pour le monoïde B_n^+ . Notons $\text{Div}(\Delta_n)$ l'ensemble des diviseurs (à gauche ou à droite, ils coïncident) de Δ_n dans B_∞^+ (ou dans B_n^+), et soit S' l'ensemble de tous les mots de tresses positifs représentant un élément d'au moins un des ensembles $\text{Div}(\Delta_n)$. Alors, S' est infini, mais, pour chaque entier n , l'ensemble $S' \cap \{\sigma_1, \dots, \sigma_{n-1}\}^*$ est fini, car $\text{Div}(\Delta_n)$ est fini (à $n!$ éléments), et chaque élément de B_∞^+ n'a qu'un nombre fini d'expressions.

L'ensemble S' contient chacun des atomes σ_i , et il résulte des propriétés élémentaires des éléments Δ_n que S' est clos par R -retournement à droite (et à gauche). En notant que, pour tout n , l'ensemble des mots signés sur $\{\sigma_1, \dots, \sigma_{n-1}\}$ est clos par retournement, on peut appliquer localement la proposition 1.15 à chacun des ensembles finis $S' \cap \{\sigma_1, \dots, \sigma_{n-1}\}^*$, c'est-à-dire considérer la présentation standard du monoïde B_n^+ , et résoudre en temps quadratique le problème de mots associé par retournement.

On pourra noter que, pour $n \geq 3$, l'ensemble $S' \cap \{\sigma_1, \dots, \sigma_{n-1}\}^*$ n'est pas la clôture de $\{\sigma_1, \dots, \sigma_{n-1}\}$ par retournement : en effet, $S' \cap \{\sigma_1, \sigma_2\}^*$ a 7 éléments, à savoir $\varepsilon, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1$, et $\sigma_2\sigma_1\sigma_2$, alors que la clôture

par complément à droite de $\{\sigma_1, \sigma_2\}$ n'en a que 5, les mots $\sigma_1\sigma_2\sigma_1$ et $\sigma_2\sigma_1\sigma_2$ étant absents.

Quand on repasse au monoïde B_∞^+ , on en déduit la décidabilité du problème de mots par retournement, mais on n'a plus de borne supérieure de complexité, car il faut prendre en compte le coût élémentaire de chaque étape de R' -retournement, c'est-à-dire l'entier N de la démonstration de la proposition 1.15, qui n'existe plus quand n croît indéfiniment. De fait, pour la présentation (I.2.2) du monoïde B_∞^+ , la seule borne supérieure connue pour la solution déduite de la méthode du retournement est en $2^{O(n)}$ [29], avec une borne inférieure prouvée en $O(n^4)$ [31]. Signalons qu'il existe des solutions en $O(n^2)$ basée sur des approches topologiques [33, 34].

2. Le retournement pour H^+ : complétude

On en vient à l'utilisation de la méthode du retournement pour l'étude du monoïde H^+ introduit au chapitre I par la présentation (\mathcal{P}) . Des résultats partiels ont déjà été obtenus au chapitre II par l'utilisation d'un système de réécriture, et il s'agit de voir si le retournement permet d'aller plus loin.

De façon très naturelle, on va étudier l'éventuelle complétude du retournement à droite pour la présentation (\mathcal{P}) dans une première section 2.1. Comme celle-ci va s'avérer, on en tire dans la section 2.2 diverses applications suivant les principes généraux décrits dans la section 1. Enfin, dans la section 2.3, on dit quelques mots du retournement à gauche pour (\mathcal{P}) , à savoir qu'il est non complet, donc *a priori* sans grand intérêt.

2.1. La condition du cube à droite. On rappelle que le monoïde H^+ est défini par la présentation (\mathcal{P}) :

$$H^+ := \left\langle \theta_1, \theta_2, \dots \mid \begin{array}{ll} \theta_j\theta_i = \theta_i\theta_{j+1} & \text{pour } j \geq i + 2 \\ \theta_j\theta_i\theta_j = \theta_i\theta_j\theta_{i+3} & \text{pour } j = i + 1 \end{array} \right\rangle^+.$$

Cette présentation de monoïde n'a pas de ε -relation et est complétée à droite, donc éligible pour le retournement à droite. De surcroît, les deux familles de relations préservent la longueur, et donc la présentation est noéthérienne. D'autre part, on note que, pour chaque couple (i, j) avec $i \neq j$, il existe dans la présentation une relation de la forme $\theta_i\dots = \theta_j\dots$: il n'y a donc jamais blocage du retournement, les seules possibilités étant succès ou non-terminaison.

Par le critère de la proposition III.1.27, l'éventuelle complétude du retournement pour (\mathcal{P}) est donc ramenée à la vérification de la condition du cube à droite pour les triplets de lettres deux à deux distinctes.

LEMME 2.1. *Pour i, j, k deux à deux distincts, la condition du cube à droite est vérifiée pour la présentation (\mathcal{P}) en $(\theta_i, \theta_j, \theta_k)$.*

DÉMONSTRATION. On va considérer tous les triplets $(\theta_i, \theta_j, \theta_k)$ avec i, j, k deux à deux distincts. Pour deux générateurs θ_i, θ_j distincts, le seul facteur influant sur la relation entre θ_i et θ_j est la distance entre i et j , suivant

qu'elle est égale à 1 ou non. Il en résulte qu'il n'y a qu'un nombre fini de types de triplet à traiter.

On rappelle que la condition du cube pour $(\theta_i, \theta_j, \theta_k)$ est l'implication

$$(2.2) \quad \overline{\theta_i} \theta_k \overline{\theta_k} \theta_j \curvearrowright u' v' \implies \overline{u'} \overline{\theta_i} \theta_j v' \curvearrowright \varepsilon.$$

Supposons d'abord $j \geq i + 2$ et $k \geq j + 2$. Utilisant les relations

$$\theta_j \theta_i = \theta_i \theta_{j+1} \quad \theta_k \theta_j = \theta_j \theta_{k+1} \quad \theta_k \theta_i = \theta_i \theta_{k+1},$$

on trouve pour $\overline{\theta_i} \theta_k \overline{\theta_k} \theta_j$ le retournement

$$\begin{array}{ccccc} & & \theta_j & & \\ & & \longrightarrow & & \\ & \theta_k & \downarrow & \theta_j & \downarrow \theta_{k+1} \\ \theta_i & \longrightarrow & \theta_i & \longrightarrow & \theta_i \\ & \theta_{k+1} & \downarrow & \theta_{j+1} & \downarrow \\ & & & & \end{array}$$

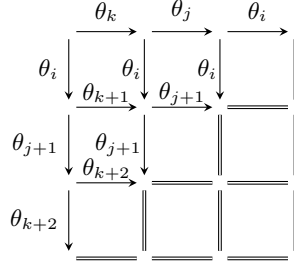
soit $u' = \theta_{k+1} \theta_i$ et $v' = \theta_{k+1} \theta_{j+1}$ dans (2.2). On trouve alors

$$\begin{array}{ccccc} & \theta_j & \theta_{k+1} & \theta_i & \\ \theta_i \downarrow & \longrightarrow & \theta_i & \longrightarrow & \theta_i \\ & \theta_{j+1} & \downarrow \theta_{k+2} & \longrightarrow & \\ \theta_{k+1} \downarrow & \theta_{k+2} & \longrightarrow & \longrightarrow & \\ & \theta_{j+1} & \longrightarrow & \longrightarrow & \\ \theta_{j+1} \downarrow & \longrightarrow & \longrightarrow & \longrightarrow & \end{array}$$

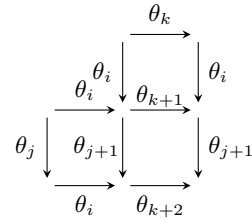
ce qui montre (2.2) dans ce cas. De même, pour $(\theta_i, \theta_k, \theta_j)$, on trouve

$$\begin{array}{ccccc} & & \theta_k & & \\ & & \longrightarrow & & \\ & \theta_j & \downarrow & \theta_j & \downarrow \\ \theta_i & \longrightarrow & \theta_i & \longrightarrow & \theta_i \\ & \theta_{j+1} & \downarrow & \theta_{k+2} & \downarrow \\ & & & & \end{array}$$

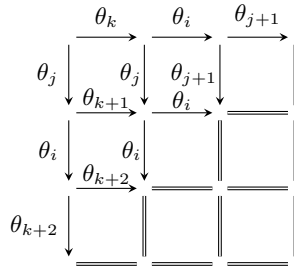
soit $u' = \theta_j \theta_i$ et $v' = \theta_{j+1} \theta_{k+2}$, et on a alors



donc (2.2). Enfin, pour $(\theta_j, \theta_k, \theta_i)$, on trouve



soit $u' = \theta_i \theta_{j+1}$ et $v' = \theta_i \theta_{k+2}$ et on a alors



donc (2.2).

Supposons maintenant $j = i + 1$ et $k = j + 1$. Utilisant les relations

$$\theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{j+2} \quad \theta_k \theta_j \theta_k = \theta_j \theta_k \theta_{k+2} \quad \theta_k \theta_i = \theta_i \theta_{k+1},$$

on trouve pour le cas de $(\theta_i, \theta_j, \theta_k)$ le retournement (à partir de maintenant, on donne les suites de retournements sous forme de mots et non de diagrammes)

$$\begin{aligned}
\overline{\theta_i \theta_k \theta_k \theta_j} &\curvearrowright \theta_{k+1} \overline{\theta_i \theta_k \theta_j} \\
&\curvearrowright \theta_{k+1} \overline{\theta_i \theta_j \theta_k \theta_{k+2} \theta_k} \\
&\curvearrowright \theta_{k+1} \theta_j \theta_{j+2} \overline{\theta_j \theta_i \theta_k \theta_{k+2} \theta_k} \\
&\curvearrowright \theta_{k+1} \theta_j \theta_{j+2} \overline{\theta_j \theta_{k+1} \theta_i \theta_{k+2} \theta_k} \\
&\curvearrowright \theta_{k+1} \theta_j \theta_{j+2} \theta_{k+2} \overline{\theta_j \theta_i \theta_{k+2} \theta_k},
\end{aligned}$$

soit $u' = \theta_k \theta_{k+2} \theta_i \theta_j$ et $v' = \theta_{k+1} \theta_j \theta_{j+2} \theta_{k+2}$ et on a alors

$$\overline{\theta_{k+2} \theta_{j+2} \theta_j \theta_{k+1} \theta_i \theta_j \theta_k \theta_{k+2} \theta_i \theta_j} \curvearrowright \overline{\theta_{k+2} \theta_{j+2} \theta_j \theta_{k+1} \theta_j \theta_{j+2} \theta_j \theta_i \theta_k \theta_{k+2} \theta_i \theta_j}$$

$$\begin{aligned} &\curvearrowright \overline{\theta_j \theta_i \theta_k} \overline{\theta_j \theta_i \theta_j \theta_{j+2} \theta_{k+2}} \\ &\curvearrowright \dots \curvearrowright \varepsilon, \end{aligned}$$

donc (2.2).

Supposons finalement $j = i + 1$ et $k \geq j + 1$. Utilisant les relations

$$\theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{j+2} \quad \theta_k \theta_j = \theta_j \theta_{k+1} \quad \theta_k \theta_i = \theta_i \theta_{k+1},$$

on trouve pour le cas de $(\theta_i, \theta_j, \theta_k)$, le retournement

$$\overline{\theta_i \theta_k \theta_k \theta_j} \curvearrowright \overline{\theta_{k+1} \theta_i \theta_k \theta_j} \curvearrowright \overline{\theta_{k+1} \theta_i \theta_j \theta_{k+1}} \curvearrowright \overline{\theta_{k+1} \theta_j \theta_{j+2} \theta_j \theta_i \theta_{k+1}},$$

soit $u' = \theta_{k+1} \theta_i \theta_j$ et $v' = \theta_{k+1} \theta_j \theta_{j+2}$. On trouve alors

$$\begin{aligned} \overline{\theta_{j+2} \theta_j \theta_{k+1} \theta_i \theta_j \theta_{k+1} \theta_i \theta_j} &\curvearrowright \overline{\theta_{j+2} \theta_j \theta_{k+1} \theta_j \theta_{j+2} \theta_j \theta_i \theta_{k+1} \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{j+2} \theta_j \theta_j \theta_{k+2} \theta_{j+2} \theta_j \theta_i \theta_{k+1} \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{j+2} \theta_{k+2} \theta_{j+2} \theta_j \theta_i \theta_{k+1} \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{j+2} \theta_{j+2} \theta_{k+3} \theta_j \theta_i \theta_{k+1} \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{k+3} \theta_j \theta_i \theta_{k+1} \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{k+3} \theta_j \theta_{k+2} \theta_i \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{k+3} \theta_j \theta_{k+2} \theta_j} \\ &\curvearrowright \overline{\theta_{k+3} \theta_{k+3} \theta_j \theta_j} \curvearrowright \varepsilon, \end{aligned}$$

donc (2.2). De même, pour le triplet $(\theta_i, \theta_k, \theta_j)$, on trouve

$$\begin{aligned} \overline{\theta_i \theta_j \theta_j \theta_k} &\curvearrowright \overline{\theta_j \theta_{j+2} \theta_j \theta_i \theta_j \theta_k} \\ &\curvearrowright \overline{\theta_j \theta_{j+2} \theta_j \theta_i \theta_{k+1} \theta_j} \\ &\curvearrowright \overline{\theta_j \theta_{j+2} \theta_j \theta_{k+2} \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_j \theta_{j+2} \theta_{k+3} \theta_j \theta_i \theta_j}, \end{aligned}$$

soit $u' = \theta_j \theta_i \theta_j$ et $v' = \theta_j \theta_{j+2} \theta_{k+3}$. On trouve alors

$$\begin{aligned} \overline{\theta_{k+3} \theta_{j+2} \theta_j \theta_i \theta_k \theta_j \theta_i \theta_j} &\curvearrowright \overline{\theta_{k+3} \theta_{j+2} \theta_j \theta_{k+1} \theta_i \theta_j \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{k+3} \theta_{j+2} \theta_{k+2} \theta_j \theta_i \theta_j \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{k+3} \theta_{k+3} \theta_{j+2} \theta_j \theta_i \theta_j \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{j+2} \theta_j \theta_i \theta_j \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{j+2} \theta_j \theta_j \theta_{j+2} \theta_j \theta_i \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_{j+2} \theta_{j+2} \theta_j \theta_i \theta_i \theta_j} \\ &\curvearrowright \overline{\theta_j \theta_i \theta_i \theta_j} \curvearrowright \varepsilon, \end{aligned}$$

donc (2.2). Enfin, pour le triplet $(\theta_j, \theta_k, \theta_i)$, on trouve

$$\begin{aligned} \overline{\theta_j \theta_i \theta_i \theta_k} &\curvearrowright \overline{\theta_i \theta_j \theta_{j+2} \theta_j \theta_i \theta_k} \\ &\curvearrowright \overline{\theta_i \theta_j \theta_{j+2} \theta_j \theta_{k+1} \theta_i} \end{aligned}$$

$$\begin{aligned} &\curvearrowright \theta_i \theta_j \overline{\theta_{j+2} \theta_{k+2} \theta_j \theta_i} \\ &\curvearrowright \theta_i \theta_j \theta_{k+3} \overline{\theta_{j+2} \theta_j \theta_i}, \end{aligned}$$

soit $u' = \theta_i \theta_j \theta_{j+2}$ et $v' = \theta_i \theta_j \theta_{k+3}$. On trouve alors

$$\begin{aligned} \overline{\theta_{k+3} \theta_j \theta_i \theta_j \theta_k \theta_i \theta_j \theta_{j+2}} &\curvearrowright \overline{\theta_{k+3} \theta_j \theta_i \theta_{k+1} \theta_j \theta_i \theta_j \theta_{j+2}} \\ &\curvearrowright \overline{\theta_{k+3} \theta_j \theta_{k+2} \theta_i \theta_j \theta_i \theta_j \theta_{j+2}} \\ &\curvearrowright \overline{\theta_{k+3} \theta_{k+3} \theta_j \theta_i \theta_j \theta_i \theta_j \theta_{j+2}} \\ &\curvearrowright \overline{\theta_j \theta_i \theta_j \theta_i \theta_j \theta_{j+2}} \\ &\curvearrowright \overline{\theta_j \theta_i \theta_i \theta_j \theta_{j+2} \theta_j \theta_j \theta_{j+2}} \\ &\curvearrowright \overline{\theta_j \theta_j \theta_{j+2} \theta_j \theta_j \theta_{j+2}} \\ &\curvearrowright \overline{\theta_{j+2} \theta_j \theta_j \theta_{j+2}} \curvearrowright \varepsilon, \end{aligned}$$

donc (2.2). Le cas $j \geq i + 1$ et $k = j + 1$ se traite comme le précédent. On se convaincra facilement que tous les cas ont ainsi été traités. \square

Par la proposition III.1.27, on déduit :

PROPOSITION 2.3 (complétude). *Le retournement à droite est complet pour la présentation (\mathcal{P}) du monoïde H^+ .*

2.2. Applications I : simplifiabilité et ppcm. On a déjà noté dans la proposition I.3.5 que le monoïde H^+ est noethérien, que 1 est le seul élément inversible dans H^+ , et que les atomes sont les éléments θ_i .

Le résultat de complétude de la proposition 2.3 permet d'établir de nouvelles propriétés en appliquant les résultats de la section 1.

PROPOSITION 2.4 (simplifiabilité I). *Le monoïde H^+ admet la simplification à gauche.*

DÉMONSTRATION. Une application directe de la proposition 1.1, puisque, par la proposition 2.3, le retournement à droite est complet pour la présentation (\mathcal{P}) de H^+ . \square

On verra ci-dessous dans la section 2.3 que le retournement à gauche ne permet pas d'établir un résultat symétrique pour la simplification à droite. Mais c'est là qu'on peut appliquer le résultat démontré au chapitre II par utilisation d'un système de réécriture.

PROPOSITION 2.5 (simplifiabilité II). *Le monoïde H^+ admet la simplification à droite.*

DÉMONSTRATION. On applique le résultat de simplifiabilité conditionnelle de la proposition II.3.31 : si le monoïde H^+ admet la simplification à gauche, alors il admet aussi la simplification à droite. Par la proposition 2.4, la prémisse est vraie, et il en est donc de même de la conclusion. \square

La proposition A de l'introduction est donc établie : le monoïde H^+ est simplifiable des deux côtés.

Continuant avec les applications de la complétude du retournement à droite, on obtient :

PROPOSITION 2.6 (ppcm conditionnels). *Le monoïde H^+ admet des plus petits multiples communs à droite conditionnels : deux éléments g et h qui ont un multiple commun à droite ont un ppcm à droite.*

DÉMONSTRATION. On applique la proposition 1.8. □

Il est naturel de se demander ici si l'hypothèse d'existence de multiple commun peut être omise. La réponse, négative, est une autre application de la complétude du retournement à droite.

LEMME 2.7. *Pour tout i , les retournements de $\overline{\theta_{i+1}\theta_i\theta_{i+2}}$ et $\overline{\theta_{i+2}\theta_i\theta_{i+1}}$ ne terminent pas.*

DÉMONSTRATION. Soit $w := \overline{\theta_{i+1}\theta_i\theta_{i+2}}$. On trouve

$$\overline{\theta_{i+1}\theta_i\theta_{i+2}} \curvearrowright \theta_i\theta_{i+1}\overline{\theta_{i+3}\theta_{i+1}\theta_{i+2}} \curvearrowright \theta_i\theta_{i+1}\overline{\theta_{i+3}\theta_{i+2}\theta_{i+4}\theta_{i+2}\theta_{i+1}},$$

d'où l'existence de deux mots positifs $u := \theta_i\theta_{i+1}$ et $v := \theta_{i+1}\theta_{i+2}$ vérifiant

$$w \curvearrowright u \cdot \text{dec}^2(w) \cdot \bar{v},$$

et, de là inductivement,

$$w \curvearrowright u \cdot \text{dec}^2(u) \cdot \dots \cdot \text{dec}^{2p-1}(u) \cdot \text{dec}^{2p}(w) \cdot \overline{\text{dec}^{2p-1}(v)} \cdot \dots \cdot \overline{\text{dec}^2(v)} \cdot \bar{v}$$

pour tout $p \geq 0$. On ne peut donc jamais atteindre un mot terminal. La démonstration est similaire pour $\overline{\theta_{i+2}\theta_i\theta_{i+1}}$. □

PROPOSITION 2.8 (pas de multiple commun I). *Pour tout i , les éléments θ_{i+1} et $\theta_i\theta_{i+2}$ de H^+ n'ont pas de multiple commun à droite.*

DÉMONSTRATION. Le retournement à droite étant complet pour la présentation de H^+ , si les éléments θ_{i+1} et $\theta_i\theta_{i+2}$ avaient un multiple commun à droite, le retournement à droite le détecterait, au sens où le retournement du quotient $\overline{\theta_{i+1}\theta_i\theta_{i+2}}$ se terminerait, ce qui, par le lemme 2.7, n'est pas le cas. □

Donc, par exemple, θ_2 et $\theta_1\theta_3$ n'ont pas de multiple à droite commun dans H^+ — alors que, d'après la présentation, deux atomes θ_i quelconques en ont toujours un. Le résultat de la proposition 2.6 est donc optimal concernant les multiples communs à droite.

On termine avec l'existence de diviseurs communs. Cette fois, le résultat est sans restriction :

PROPOSITION 2.9 (pgcd). *Le monoïde H^+ admet des pgcd à gauche ; plus généralement, toute partie non vide de H^+ admet un pgcd à gauche.*

DÉMONSTRATION. On applique la proposition 1.10. □

2.3. Le retournement à gauche. On rappelle que le retournement à gauche \curvearrowright est la contrepartie du retournement à droite dans laquelle on remplace un facteur positif-négatif de longueur deux $t\bar{s}$ par des mots négatifs-positifs $\bar{v}u$ tel que $ut = vs$ est une relation de la présentation considérée. Il est défini pour les présentations (S, R) complémentées à gauche, c'est-à-dire sans ε -relation ni relation $us = vs$ avec $u \neq v$ et telles que, pour $s \neq t$ dans S , il existe au plus une relation $ut = vs$ dans R .

Considérer le retournement à gauche pour la présentation (\mathcal{P}) du monoïde H^+ a du sens. En effet :

LEMME 2.10. *La présentation (\mathcal{P}) est complémentée à gauche.*

DÉMONSTRATION. Supposons $i < j$. Pour $j = i + 1$, il n'y a aucune relation $...\theta_i = ... \theta_j$ dans (\mathcal{P}) . Pour $j = i + 2$, il n'y a aucune relation $...\theta_i = ... \theta_j$ dans (\mathcal{P}) dans le cas $i = 1$, et il y a exactement une relation $...\theta_i = ... \theta_j$ dans (\mathcal{P}) pour $i \geq 2$, à savoir la relation $\theta_i \theta_{i-1} \theta_i = \theta_{i-1} \theta_i \theta_{i+2}$. Enfin, pour $j \geq i + 3$, il y a exactement une relation $...\theta_i = ... \theta_j$ dans (\mathcal{P}) , à savoir la relation $\theta_{j-1} \theta_i = \theta_i \theta_j$. Donc, dans tous les cas, il y a au plus une relation $...\theta_i = ... \theta_j$ dans (\mathcal{P}) . \square

Le retournement à gauche permet donc toujours, lorsqu'il se termine, de construire des multiples communs à gauche. Par contre, on sait qu'on ne peut tirer de conclusion intéressante du retournement que lorsque celui-ci détecte toutes les équivalences, à savoir lorsqu'il est complet. Or, dans le cas de la présentation (\mathcal{P}) , cette condition est en défaut :

PROPOSITION 2.11 (**non-complétude**). *Le retournement à gauche n'est pas complet pour la présentation (\mathcal{P}) .*

DÉMONSTRATION. Par la contrepartie de la proposition III.1.27, il suffit de trouver un triplet de générateurs tel que la condition du cube à gauche soit fausse. Considérons le triplet $(\theta_5, \theta_7, \theta_3)$. On trouve

$$\begin{aligned} \theta_5 \overline{\theta_3 \theta_3 \theta_7} \curvearrowright \overline{\theta_3 \theta_2 \theta_3 \theta_2 \theta_3 \theta_7} \\ \curvearrowright \overline{\theta_3 \theta_2 \theta_3 \theta_2 \theta_6 \theta_3} \\ \curvearrowright \overline{\theta_3 \theta_2 \theta_3 \theta_5 \theta_2 \theta_3} \curvearrowright \overline{\theta_3 \theta_2 \theta_2 \theta_3 \theta_2 \theta_3 \theta_2 \theta_3}, \end{aligned}$$

et il s'agirait de montrer que le mot signé $\theta_3 \theta_2 \theta_2 \theta_3 \theta_5 \overline{\theta_7 \theta_3 \theta_2 \theta_3 \theta_2}$ se retourne à gauche en le mot vide. Or on trouve

$$\theta_3 \theta_2 \theta_2 \theta_3 \theta_5 \overline{\theta_7 \theta_3 \theta_2 \theta_3 \theta_2} \curvearrowright \theta_3 \theta_2 \theta_2 \theta_3 \overline{\theta_4 \theta_5 \theta_4 \theta_5 \theta_3 \theta_2 \theta_3 \theta_2},$$

et le retournement bloque faute de relation de la forme $...\theta_3 = ... \theta_4$ dans la présentation. La condition du cube à gauche est donc en défaut pour le triplet $(\theta_5, \theta_7, \theta_3)$, et le retournement à gauche ne peut être complet. \square

Plus généralement, on peut vérifier, pour tout $i \geq 1$, le non-retournement

$$\theta_i \theta_{i-1} \theta_{i-1} \theta_i \theta_{i+2} \overline{\theta_{i+4} \theta_i \theta_{i-1} \theta_i \theta_{i-1}} \not\curvearrowright \varepsilon,$$

alors que, par retournement à droite, on voit que les mots $\theta_i\theta_{i-1}\theta_{i-1}\theta_i\theta_{i+2}$ et $\theta_{i-1}\theta_i\theta_{i-1}\theta_i\theta_{i+4}$ sont \equiv -équivalents : on a ainsi un exemple explicite d'équivalence non détectée par le retournement à gauche.

REMARQUE 2.12. Puisque toute obstruction à la condition du cube donne une équivalence non détectée par retournement, on peut, sans changer le monoïde associé, ajouter à la présentation initiale cette équivalence comme relation supplémentaire, et montrer qu'au moins une obstruction à la complétude a été effacée. Dans [21], on donne des exemples où cette procédure, éventuellement itérée, peut mener à une présentation enrichie pour laquelle le retournement est complet. Si on tente cette approche ici, et que, par exemple, on ajoute à la présentation la relation $\theta_i\theta_{i-1}\theta_{i-1}\theta_i\theta_{i+2} = \theta_{i-1}\theta_i\theta_{i-1}\theta_i\theta_{i+4}$, on obtient une nouvelle présentation qui sort du cadre des présentations complémentées, et il est douteux qu'on puisse espérer une complétude du retournement (même étendu au cas non complémenté comme dans [21]).

Notons qu'il est faux que H^+ admette toujours des multiples communs à gauche (noter que le résultat reprend et étend celui de la proposition II.3.30, sauf pour le cas de θ_1 et θ_3 auquel il ne s'applique pas) :

PROPOSITION 2.13 (**pas de multiple commun II**). *Pour tout i , les éléments θ_i et θ_{i+1} de H^+ n'ont pas de multiple commun à gauche.*

DÉMONSTRATION. Supposons qu'on a $a\theta_i = b\theta_{i+1}$ dans H^+ . Utilisant la projection π de H^+ sur le monoïde de Thompson F^+ (proposition I.3.26), on déduit $\pi(a)a_i = \pi(b)a_{i+1}$ dans F^+ . Or on vérifie facilement (toutes les relations sont courtes, et il n'existe qu'un seul type) que le retournement à droite et le retournement à gauche sont complets pour la présentation (I.2.8) du monoïde F^+ . Comme il n'existe pas de relation $\dots a_i = \dots a_{i+1}$ dans (I.2.8), on en déduit que a_i et a_{i+1} n'ont pas de multiple à gauche commun dans F^+ . De là, $\pi(a)a_i = \pi(b)a_{i+1}$ est impossible dans F^+ , donc $a\theta_i = b\theta_{i+1}$ est impossible dans H^+ . \square

Par contre, faute de complétude du retournement à gauche, les questions suivantes restent ouvertes :

QUESTION 2.14. Le monoïde H^+ admet-il des ppcm à gauche conditionnels ? Admet-il des pgcd à droite ?

L'existence de réponses positives à ces questions dans le monoïde F^+ , projection de H^+ , ne suffit pas à y répondre dans H^+ .

3. Le retournement pour H^+ : terminaison

Le second problème naturel pour le retournement à droite associé à la présentation (\mathcal{P}) du monoïde H^+ est celui de la terminaison. Comme le retournement est complet, on sait que la question équivaut à l'existence de multiples communs à droite. On a vu dans la proposition 2.8 que, même si deux atomes de H^+ ont toujours un multiple commun à droite, il existe des

paires d'éléments de H^+ sans multiple commun à droite, et donc la question est certainement non triviale — tout comme elle est non triviale pour le cas du monoïde de tresses B_∞^+ .

Le principal résultat de cette section est l'existence d'un algorithme décidant l'existence de multiples communs à droite et les calculant lorsqu'ils existent — ce qui est le plus qu'on puisse espérer. De façon équivalente, il s'agit d'obtenir une méthode décidant la terminaison du retournement à droite pour (\mathcal{P}) , et, pour cela, on va utiliser la méthode décrite dans la section III.3, à savoir identifier un ensemble de mots clos par complément à droite.

La section est divisée en trois sous-sections. Dans la section 3.1, on décrit explicitement un ensemble de mots clos par complément à droite vis-à-vis de la présentation (\mathcal{P}) . Puis, dans la section 3.2, on utilise cet ensemble pour répondre aux questions sur la terminaison du retournement et l'existence de multiples communs à droite. Enfin, la section 3.3, on observe que le retournement à gauche termine toujours : cela répond à une question naturelle, mais le résultat est de portée limitée puisque le retournement à gauche n'est pas complet, et donc le fait qu'il se termine ne dit pas grand chose sur l'existence de multiples communs à gauche en général.

3.1. Un ensemble clos par complément. On cherche à identifier un ensemble de mots Θ' sur l'alphabet Θ qui inclue Θ et soit clos par complément à droite associé à (\mathcal{P}) . Si on pense au cas du monoïde B_∞^+ , le problème est analogue à trouver un ensemble de mots clos par complément pour la présentation (I.2.2), et on sait qu'alors on peut utiliser les propriétés combinatoires et topologiques des éléments de Garside Δ_n . Pour H^+ , on n'a pas (ou pas encore) de telle interprétation, et il faut donc raisonner à un niveau purement syntaxique, ce qui *a priori* n'est pas facile. De surcroît, on sait déjà qu'il existe des cas où le retournement ne termine pas, et, par ailleurs, et contrairement au cas des tresses, le monoïde H^+ n'est pas réunion d'une suite croissante de monoïdes de type fini : aucune approche expérimentale exhaustive n'est donc possible.

Le résultat principal est alors le suivant :

PROPOSITION 3.1 (**lemme-clé**). *Posons $\Theta' = \Theta_1 \cup \Theta_2 \cup \{\varepsilon\}$, avec*

$$(3.2) \quad \Theta_1 = \{\theta_i \theta_{i+2} \theta_{i+4} \cdots \theta_{i+2k} \mid i \geq 1, k \geq 0\},$$

$$(3.3) \quad \Theta_2 = \{\theta_i \theta_{i+2} \theta_{i+4} \cdots \theta_{i+2k} \theta_{i+2k+1} \mid i \geq 1, k \geq 0\},$$

et soit R' l'ensemble de relations associé suivant la définition III.3.2 (et la convention III.3.3). Alors l'ensemble Θ' est clos par complément à droite vis-à-vis de la présentation (\mathcal{P}) , et le R' -retournement sur $\Theta' \times \Theta'$ est une relation décidable.

Comme au chapitre III, on confond l'alphabet Θ' et sa copie formelle $\underline{\Theta}'$ lorsqu'il n'y a pas d'ambiguïté. Par ailleurs, notant R les relations de (\mathcal{P}) , on écrira $C(u, v)$ pour le complément à droite $C_R(u, v)$.

DÉMONSTRATION. La vérification se fait au cas par cas. On va montrer que, pour tout couple de mots (u, v) dans $\Theta' \times \Theta'$, les compléments à droite $C(u, v)$ et $C(v, u)$ appartiennent à Θ' ou n'existent pas. Soient u, v deux éléments de Θ' , donc de Θ_1 , de Θ_2 , ou vides. Si u ou v est vide, alors l'un des deux compléments, $C(u, v)$ ou $C(v, u)$, est un des deux mots u, v , et l'autre est vide, donc dans Θ' . On considère les cas restants.

Cas 1 : $u \in \Theta_1$ et $v \in \Theta_1$. Écrivons

$$u = \theta_j \theta_{j+2} \cdots \theta_{j+2k} \quad \text{et} \quad v = \theta_\ell \theta_{\ell+2} \cdots \theta_{\ell+2m}.$$

Par symétrie, on peut supposer $m \geq k$.

Sous-cas 1.1 : $\ell = j$. On trouve $C(u, v) = \theta_{j+2k+2} \cdots \theta_{j+2m}$, qui est dans Θ_1 , et $C(v, u) = \varepsilon$, qui est dans Θ' .

Sous-cas 1.2 : $j+1 \leq \ell \leq j+k$. Alors on a $\ell = j+i$ avec $1 \leq i \leq k$ et on trouve

$$\begin{aligned} & \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2i}} \overline{\theta_{j+2i-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+i}} \overline{\theta_{j+i+2}} \cdots \overline{\theta_{j+i+2m}} \\ & \rightsquigarrow \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2i}} \overline{\theta_{j+2i-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_{j+i+1}} \overline{\theta_{j+i+2}} \cdots \overline{\theta_{j+i+2m}} \\ & \rightsquigarrow \cdots \rightsquigarrow \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2i}} \overline{\theta_{j+2i-2}} \overline{\theta_{j+2i-1}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+i+2}} \cdots \overline{\theta_{j+i+2m}} \\ & \rightsquigarrow \cdots \\ & \rightsquigarrow \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2i}} \overline{\theta_{j+2i-1}} \overline{\theta_{j+2i+1}} \overline{\theta_{j+2i-1}} \overline{\theta_{j+2i-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+i+2}} \cdots \overline{\theta_{j+i+2m}}. \end{aligned}$$

Par le lemme 2.7, le retournement de $\overline{\theta_{j+2i}} \overline{\theta_{j+2i-1}} \overline{\theta_{j+2i+1}}$ ne se termine pas, donc de même pour tout mot incluant $\overline{\theta_{j+2i}} \overline{\theta_{j+2i-1}} \overline{\theta_{j+2i+1}}$ comme facteur. Dans ce cas, les compléments ne sont pas définis.

Sous-cas 1.3 : $\ell = j+k+1$. On trouve

$$\begin{aligned} & \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+k+1}} \overline{\theta_{j+k+3}} \cdots \overline{\theta_{j+k+1+2m}} \\ & \rightsquigarrow \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_{j+k+2}} \overline{\theta_j} \overline{\theta_{j+k+3}} \cdots \overline{\theta_{j+k+1+2m}} \\ & \rightsquigarrow \cdots \rightsquigarrow \overline{\theta_{j+2k}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+k+3}} \cdots \overline{\theta_{j+k+1+2m}} \\ & \rightsquigarrow \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+3}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+k+3}} \cdots \overline{\theta_{j+k+1+2m}} \\ & \rightsquigarrow \cdots \\ & \rightsquigarrow \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+3}} \overline{\theta_{j+2k+5}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \\ & \qquad \qquad \qquad \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{j+k+5}} \cdots \overline{\theta_{j+k+1+2m}} \\ & \rightsquigarrow \cdots \rightsquigarrow \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+3}} \cdots \overline{\theta_{j+2k+2m+3}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2}} \overline{\theta_j}. \end{aligned}$$

Alors, on a $C(u, v) = \theta_{j+2k+1} \theta_{j+2k+3} \cdots \theta_{j+2k+2m+3}$, qui appartient à Θ_1 par définition, et $C(v, u) = \theta_j \theta_{j+2} \cdots \theta_{j+2k} \theta_{j+2k+1}$, qui appartient à Θ_2 .

Sous-cas 1.4 : $\ell \geq j+k+2$. On trouve

$$\begin{aligned} & \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_\ell} \overline{\theta_{\ell+2}} \cdots \overline{\theta_{\ell+2m}} \overline{rev} \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2}} \overline{\theta_{\ell+1}} \overline{\theta_j} \overline{\theta_{\ell+2}} \cdots \overline{\theta_{\ell+2m}} \\ & \rightsquigarrow \overline{\theta_{j+2k}} \cdots \overline{\theta_{\ell+2}} \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{\ell+2}} \cdots \overline{\theta_{\ell+2m}} \\ & \rightsquigarrow \cdots \rightsquigarrow \overline{\theta_{\ell+k+1}} \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \overline{\theta_{\ell+2}} \cdots \overline{\theta_{\ell+2m}} \end{aligned}$$

$$\curvearrowright \cdots \curvearrowright \theta_{\ell+k+1} \theta_{\ell+k+3} \cdots \theta_{\ell+k+1+2m} \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2}} \overline{\theta_j},$$

et on déduit $C(u, v) = \theta_{\ell+k+1} \theta_{\ell+k+3} \cdots \theta_{\ell+k+1+2m}$, qui appartient à Θ_1 , et $C(v, u) = \theta_j \theta_{j+2} \cdots \theta_{j+2k}$, qui appartient à Θ_1 .

Sous-cas 1.5 : $\ell + 1 \leq j \leq \ell + m$. Le calcul est le même, *mutatis mutandis*, que pour le sous-cas 1.2.

Sous-cas 1.6 : $j = \ell + m + 1$. Le calcul est le même, *mutatis mutandis*, que pour le sous-cas 1.3.

Sous-cas 1.7 : $j \geq \ell + m + 2$. Le calcul est le même, *mutatis mutandis*, que pour le sous-cas 1.4.

Cas 2 : $u \in \Theta_2$ et $v \in \Theta_2$. Écrivons

$$u = \theta_j \theta_{j+2} \cdots \theta_{j+2k} \theta_{j+2k+1} \quad \text{et} \quad v = \theta_\ell \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}.$$

Par symétrie, on peut supposer $m \geq k$.

Sous-cas 2.1 : $\ell = j$. Alors, pour $m = k$, on a $C(u, v) = v \setminus u = \varepsilon$, et, pour $m \neq k$,

$$\begin{aligned} & \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \theta_{j+2} \cdots \theta_{j+2k} \theta_{j+2k+2} \theta_{j+2k+4} \cdots \theta_{j+2m} \theta_{j+2m+1} \\ & \quad \curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+2}} \overline{\theta_{j+2k+4}} \cdots \overline{\theta_{j+2m}} \overline{\theta_{j+2m+1}} \\ & \quad \curvearrowright \theta_{j+2k+2} \theta_{j+2k+4} \overline{\theta_{j+2k+2}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+4}} \cdots \overline{\theta_{j+2m}} \overline{\theta_{j+2m+1}} \\ & \quad \curvearrowright \theta_{j+2k+2} \theta_{j+2k+4} \overline{\theta_{j+2k+6}} \overline{\theta_{j+2k+2}} \overline{\theta_{j+2k+1}} \cdots \overline{\theta_{j+2m}} \overline{\theta_{j+2m+1}} \\ & \quad \curvearrowright \cdots \\ & \quad \curvearrowright \overline{\theta_{j+2k+2}} \overline{\theta_{j+2k+4}} \overline{\theta_{j+2k+6}} \cdots \overline{\theta_{j+2m+2}} \overline{\theta_{j+2m+3}} \overline{\theta_{j+2k+2}} \overline{\theta_{j+2k+1}}. \end{aligned}$$

Alors on a $C(u, v) = \theta_{j+2k+2} \theta_{j+2k+4} \cdots \theta_{j+2m+2} \theta_{j+2m+3}$, qui est dans Θ_2 , et $C(v, u) = \theta_{j+2k+1} \theta_{j+2k+2}$, qui est dans Θ_2 également.

Sous-cas 2.2 : $j + 1 \leq \ell \leq j + k$. Alors, de même que dans le cas 1.2, les compléments $C(u, v)$ et $C(v, u)$ ne sont pas définis.

Sous-cas 2.3 : $\ell = j + k + 1$. On obtient maintenant

$$\begin{aligned} & \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \theta_{j+k+1} \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2} \\ & \quad \curvearrowright \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_{j+k+2}} \overline{\theta_j} \\ & \quad \quad \quad \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2} \\ & \quad \curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \\ & \quad \quad \quad \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2} \\ & \quad \curvearrowright \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k+3}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \\ & \quad \quad \quad \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2} \\ & \quad \curvearrowright \overline{\theta_{j+2k+3}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \\ & \quad \quad \quad \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2} \\ & \quad \curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k+3}} \overline{\theta_{j+2k+5}} \overline{\theta_{j+2k+1}} \overline{\theta_{j+2k}} \overline{\theta_{j+2k-2}} \cdots \overline{\theta_{j+2}} \overline{\theta_j} \\ & \quad \quad \quad \theta_{j+k+5} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2} \end{aligned}$$

$$\curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k+3}\theta_{j+2k+5} \cdots \theta_{j+2k+2m+3}\theta_{j+2k+2m+4}} \\ \overline{\theta_{j+2k+1}\theta_{j+2k} \cdots \theta_{j+2}\theta_j},$$

d'où, $C(u, v) = \theta_{j+2k+3}\theta_{j+2k+5} \cdots \theta_{j+2k+2m+3}\theta_{j+2k+2m+4}$, qui est dans Θ_2 et $C(v, u) = \theta_j\theta_{j+2} \cdots \theta_{j+2k}\theta_{j+2k+1}$, qui est dans Θ_2 également.

Sous-cas 2.4 : $\ell \geq j + k + 2$. On a le retournement

$$\overline{\theta_{j+2k+1}\theta_{j+2k} \cdots \theta_{j+2}\theta_j\theta_\ell\theta_{\ell+2} \cdots \theta_{\ell+2m}\theta_{\ell+2m+1}} \\ \curvearrowright \overline{\theta_{j+2k+1}\theta_{j+2k} \cdots \theta_{j+2}\theta_{\ell+1}\theta_j\theta_{\ell+2} \cdots \theta_{\ell+2m}\theta_{\ell+2m+1}} \\ \curvearrowright \overline{\theta_{j+2k+1}\theta_{j+2k} \cdots \theta_{\ell+2}\theta_{j+2}\theta_j\theta_{\ell+2} \cdots \theta_{\ell+2m}\theta_{\ell+2m+1}} \\ \curvearrowright \cdots \curvearrowright \overline{\theta_{\ell+k+2}\theta_{j+2k+1}\theta_{j+2k} \cdots \theta_{j+2}\theta_j\theta_{\ell+2} \cdots \theta_{\ell+2m}\theta_{\ell+2m+1}} \\ \curvearrowright \cdots \\ \curvearrowright \overline{\theta_{\ell+k+2}\theta_{\ell+k+4} \cdots \theta_{\ell+2m+k+2}\theta_{\ell+2m+k+3}\theta_{j+2k+1}\theta_{j+2k} \cdots \theta_{j+2}\theta_j},$$

d'où, $C(u, v) = \theta_{\ell+k+2}\theta_{\ell+k+4} \cdots \theta_{\ell+2m+k+2}\theta_{\ell+2m+k+3}$, qui est dans Θ_2 , par définition, et $C(v, u) = \theta_j\theta_{j+2} \cdots \theta_{j+2k}\theta_{j+2k+1}$, qui est dans Θ_2 également.

Sous-cas 2.5 : $\ell + 1 \leq j \leq \ell + m$. Le calcul est le même, *mutatis mutandis*, que pour le sous-cas 2.2.

Sous-cas 2.6 : $j = \ell + m + 1$. Le calcul est le même, *mutatis mutandis*, que pour le sous-cas 2.3.

Sous-cas 2.7 : $j \geq \ell + m + 2$. Le calcul est le même, *mutatis mutandis*, que pour le sous-cas 2.4.

Cas 3 : $u \in \Theta_1$ et $v \in \Theta_2$. Écrivons

$$u = \theta_j\theta_{j+2} \cdots \theta_{j+2k} \quad \text{et} \quad v = \theta_\ell\theta_{\ell+2} \cdots \theta_{\ell+2m}\theta_{\ell+2m+1}.$$

Sous-cas 3.1 : $\ell = j$. Alors pour $m = k$, on a $C(u, v) = \theta_{\ell+2m+1}$, qui est dans Θ_1 et $C(v, u) = \varepsilon$, qui est dans Θ . Pour $k \leq m - 1$, on a $C(u, v) = \theta_{j+2k+2} \cdots \theta_{j+2m}\theta_{j+2m+1}$, qui est dans Θ_2 et $C(v, u) = \varepsilon$, qui est dans Θ' . Pour $m \leq k - 1$, on trouve

$$\overline{\theta_{j+2k} \cdots \theta_{j+2m+4}\theta_{j+2m+2}\theta_{j+2m} \cdots \theta_{j+2}\theta_j\theta_{j+2} \cdots \theta_{j+2m}\theta_{j+2m+1}} \\ \curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k} \cdots \theta_{j+2m+4}\theta_{j+2m+2}\theta_{j+2m+1}} \\ \curvearrowright \overline{\theta_{j+2k} \cdots \theta_{j+2m+4}\theta_{j+2m+1}\theta_{j+2m+2}\theta_{j+2m+4}\theta_{j+2m+2}} \\ \curvearrowright \overline{\theta_{j+2k} \cdots \theta_{j+2m+1}\theta_{j+2m+2}\theta_{j+2m+6}\theta_{j+2m+4}\theta_{j+2m+2}} \\ \curvearrowright \cdots \curvearrowright \overline{\theta_{j+2m+1}\theta_{j+2m+2}\theta_{j+2k+2} \cdots \theta_{j+2m+6}\theta_{j+2m+4}\theta_{j+2m+2}}.$$

Par conséquent, on déduit $C(u, v) = \theta_{j+2m+1}\theta_{j+2m+2}$, qui est dans Θ_2 , et $C(v, u) = \theta_{j+2m+2} \cdots \theta_{j+2k}\theta_{j+2k+2}$, qui est dans Θ_1 .

Sous-cas 3.2 : $j + 1 \leq \ell \leq j + k$. Alors, de même que dans les cas 1.2 et 2.2, les compléments $C(u, v)$ et $C(v, u)$ ne sont pas définis.

Sous-cas 3.3 : $\ell = j + k + 1$. On a le retournement

$$\overline{\theta_{j+2k}\theta_{j+2k-2} \cdots \theta_j\theta_{j+k+1}\theta_{j+k+3} \cdots \theta_{j+k+1+2m}\theta_{j+k+2m+2}}$$

$$\begin{aligned}
&\curvearrowright \overline{\theta_{j+2k} \theta_{j+2k-2} \cdots \theta_{j+2} \theta_{j+k+2} \overline{\theta_j} \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2}} \\
&\curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k} \theta_{j+2k+1} \overline{\theta_{j+2k-2} \cdots \theta_j} \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2}} \\
&\curvearrowright \overline{\theta_{j+2k+1} \theta_{j+2k+3} \overline{\theta_{j+2k+1} \theta_{j+2k} \theta_{j+2k-2} \cdots \theta_j} \theta_{j+k+3} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2}} \\
&\curvearrowright \cdots \\
&\curvearrowright \overline{\theta_{j+2k+1} \theta_{j+2k+3} \theta_{j+2k+5} \overline{\theta_{j+2k+1} \theta_{j+2k} \theta_{j+2k-2} \cdots \theta_j} \theta_{j+k+5} \cdots \theta_{j+k+1+2m} \theta_{j+k+2m+2}} \\
&\curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k+1} \theta_{j+2k+3} \cdots \theta_{j+2k+2m+3} \theta_{j+2k+2m+4} \overline{\theta_{j+2k+1} \theta_{j+2k} \cdots \theta_j}},
\end{aligned}$$

d'où, $C(u, v) = \theta_{j+2k+1} \theta_{j+2k+3} \cdots \theta_{j+2k+2m+3} \theta_{j+2k+2m+4}$, qui est dans Θ_2 ,
et $C(v, u) = \theta_j \theta_{j+2} \cdots \theta_{j+2k} \theta_{j+2k+1}$, qui est dans Θ_2 également.

Sous-cas 3.4 : $\ell \geq j + k + 2$. On a le retournement

$$\begin{aligned}
&\overline{\theta_{j+2k} \cdots \theta_{j+2} \overline{\theta_j} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}} \\
&\quad \curvearrowright \overline{\theta_{j+2k} \cdots \theta_{j+2} \theta_{\ell+1} \overline{\theta_j} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}} \\
&\quad \curvearrowright \overline{\theta_{j+2k} \cdots \theta_{\ell+2} \overline{\theta_{j+2} \theta_j} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}} \\
&\quad \curvearrowright \cdots \curvearrowright \overline{\theta_{\ell+k+1} \overline{\theta_{j+2k} \cdots \theta_{j+2} \theta_j} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}} \\
&\quad \curvearrowright \cdots \curvearrowright \overline{\theta_{\ell+k+1} \theta_{\ell+k+3} \cdots \theta_{\ell+2m+k+1} \theta_{\ell+2m+k+2} \overline{\theta_{j+2k} \cdots \theta_{j+2} \theta_j}},
\end{aligned}$$

d'où, $C(u, v) = \theta_{\ell+k+1} \theta_{\ell+k+3} \cdots \theta_{\ell+2m+k+1} \theta_{\ell+2m+k+2}$, qui est dans Θ_2 , par
définition, et $C(v, u) = \theta_j \theta_{j+2} \cdots \theta_{j+2k}$, qui est dans Θ_1 .

Sous-cas 3.5 : $\ell + 1 \leq j \leq \ell + m$. Alors, de même que dans les cas 1.2
et 2.2, les compléments $C(u, v)$ et $C(v, u)$ ne sont pas définis.

Sous-cas 3.6 : $j = \ell + m + 1$. On a le retournement

$$\begin{aligned}
&\overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+3} \theta_{\ell+m+1} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}}} \\
&\quad \curvearrowright \overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+3} \theta_{\ell} \overline{\theta_{\ell+m+2} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}}} \\
&\quad \curvearrowright \cdots \curvearrowright \overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+3} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m+1} \theta_{\ell+2m} \theta_{\ell+2m+1}}} \\
&\quad \curvearrowright \overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+3} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{\ell+2m+3} \theta_{\ell+2m+1} \theta_{\ell+2m+1}}} \\
&\quad \curvearrowright \overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+3} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{\ell+2m+3}}} \\
&\quad \curvearrowright \cdots \curvearrowright \overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+5} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m+3} \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{\ell+2m+3}}} \\
&\quad \curvearrowright \overline{\theta_{\ell+m+1+2k} \cdots \overline{\theta_{\ell+m+5} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{\ell+2m+5} \theta_{\ell+2m+3}}} \\
&\quad \curvearrowright \cdots \curvearrowright \overline{\theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{\ell+2m+3+2k} \cdots \theta_{\ell+2m+5} \theta_{\ell+2m+3}}}.
\end{aligned}$$

Alors, on a $C(u, v) = \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}$, qui est dans Θ_2 , par définition,
et $C(v, u) = \theta_{\ell+2m+3} \theta_{\ell+2m+5} \cdots \theta_{\ell+2m+3+2k}$, qui est dans Θ_1 .

Sous-cas 3.7 : $j \geq \ell + m + 2$. On obtient le retournement

$$\begin{aligned}
&\overline{\theta_{j+2k} \cdots \theta_{j+2} \overline{\theta_j} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}} \\
&\quad \curvearrowright \overline{\theta_{j+2k} \cdots \overline{\theta_{j+2} \theta_{\ell} \overline{\theta_{j+1} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}}} \\
&\quad \curvearrowright \overline{\theta_{j+2k} \cdots \overline{\theta_{j+2} \theta_{\ell} \theta_{\ell+2} \overline{\theta_{j+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}}} \\
&\quad \curvearrowright \cdots \curvearrowright \overline{\theta_{j+2k} \cdots \overline{\theta_{j+2} \theta_{\ell} \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{j+m+2}}}
\end{aligned}$$

$$\curvearrowright \cdots \curvearrowright \theta_\ell \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1} \overline{\theta_{j+2k+m+2}} \cdots \overline{\theta_{j+m+4}} \overline{\theta_{j+m+2}},$$

Alors, on a $C(u, v) = \theta_\ell \theta_{\ell+2} \cdots \theta_{\ell+2m} \theta_{\ell+2m+1}$, qui est dans Θ_2 , par définition, et $C(v, u) = \theta_{j+m+2} \theta_{j+m+4} \cdots \theta_{j+2k+m+2}$, qui est dans Θ_1 .

À ce point, tous les cas ont été considérés, et, dans chaque cas, les compléments $C(u, v)$ et $C(v, u)$ appartiennent à Θ' ou ne sont pas définis. Donc l'ensemble Θ' est clos par complément à droite.

De plus, la discussion ci-dessus montre que, dans tous les cas, partant de u et v , il existe une recette syntaxique explicite, à savoir la réunion finie des $7 + 4 + 7$ soit 18 recettes, un nombre fini, correspondant aux sous-cas de la démonstration, donnant la valeur du complément si celui-ci existe, ou affirmant qu'il n'existe pas si c'est le cas. Par conséquent, vue comme une relation binaire sur $(\Theta')^4$ ou comme une opération binaire partielle sur $(\Theta')^2$, l'opération R -complément est récursive. \square

On peut dire davantage sur la complexité de la relation de Θ' -retournement sur $(\Theta')^2$: pour w dans Θ' , notons $\text{code}(w)$ le triplet d'entiers (i, k, e) avec $e = 0$ pour le mot vide, $e = 1$ pour un mot de Θ_1 , et $e = 2$ pour un mot de Θ_2 , et i et k comme dans (3.2) et (3.3). Puisque les entiers i et k mis en jeu sont non bornés, il est nécessaire de prendre en compte leur complexité, usuellement le nombre de chiffres du développement binaire, et donc de définir la complexité $\|u\|$ d'un mot u de Θ' comme la somme des nombres de chiffres des indices i et k correspondants. On peut alors énoncer :

PROPOSITION 3.4 (complexité). *La restriction à $\Theta' \times \Theta'$ du R' -complément à droite a une complexité linéaire en temps ; de plus, il existe une constante γ telle qu'on ait*

$$(3.5) \quad \|C(u, v)\| \leq \max(\|u\|, \|v\|) + \gamma.$$

DÉMONSTRATION. Ce que montre la démonstration de la proposition 3.1 est que $\text{code}(C(u, v))$ peut être calculé en temps $O(1)$ (temps constant) à partir de $\text{code}(u)$ et $\text{code}(v)$. De plus, les valeurs explicites des compléments obtenus montrent que les indices apparaissant dans $C(u, v)$ sont toujours au pire des combinaisons affines de coefficients ≤ 2 des quatre indices de départ notés j, k, ℓ, m , déterminés exclusivement par des additions et des multiplications par 2. Il en résulte que $\text{code}(C(u, v))$ peut être déterminé en un nombre linéaire d'opérations élémentaires (table d'addition en binaire !) à partir de $\text{code}(u)$ et $\text{code}(v)$, et qu'on a la relation (3.5) sur les tailles des entiers considérés ($\gamma = 1$ ou 2 doit être suffisant, suivant la façon dont on implémente le codage en pratique). \square

3.2. Application II : résultats de décidabilité. Grâce à l'existence de l'ensemble Θ' et à ses propriétés, on est maintenant en position d'appliquer au cas de la présentation (\mathcal{P}) les résultats de la section III.3. On part du résultat suivant, qui est une conséquence directe de la proposition III.3.18 :

LEMME 3.6. *Pour tout mot signé w sur l'alphabet Θ , le R -retournement à droite de w termine si, et seulement si, le R' -retournement du Θ' -mot signé \underline{w} réussit.*

On en déduit le résultat fondamental :

PROPOSITION 3.7 (**décidabilité I**). *La terminaison du retournement à droite pour la présentation (\mathcal{P}) est décidable.*

DÉMONSTRATION. Par construction, les relations de R' sont courtes, donc décider si le R' d'un Θ' -mot signé de longueur ℓ réussit se fait en au plus $O(\ell^2)$ étapes élémentaires consistant à R' -retourner deux mots de Θ' . Par la proposition 3.1, chacune de ces étapes est décidable, donc le résultat du processus entier l'est aussi. \square

Si on veut évaluer plus finement la complexité, on peut faire appel à la proposition 3.4 :

PROPOSITION 3.8 (**complexité**). *La terminaison du R -retournement à droite pour la présentation (\mathcal{P}) est décidable en espace $O(n^{3/2})$ et en temps $O(n^{5/2})$.*

DÉMONSTRATION. Dans l'argument ci-dessus, il y a un nombre quadratique d'étapes, dont chacune a un coût linéaire par rapport à la taille des codes. Or, les complexités des codes qui apparaissent sont presque constantes : supposons qu'on retourne des mots u et v consistant en p lettres de Θ' dont chacune a une complexité égale à q . Alors les mots successifs apparaissant dans la $p \times p$ -grille de retournement ont des complexités au plus q , $q + \gamma$, ..., $q + p\gamma$, et le coût pour chacun des p^2 retournements élémentaires est au plus $O((q + p\gamma)^2)$. Comme la complexité de u et v est (par définition) pq , le nombre total d'étapes est, dans tous les cas, borné par $p^2 \cdot O(\sqrt{pq})$, donc par $O((pq)^{5/2})$. De même, pour la complexité en espace, les mots qui apparaissent, et en particulier, les mots finaux, ont pour complexité au plus $p \cdot (q + p\gamma)$, donc borné par $p \cdot O(\sqrt{pq})$ et, de là, par $O((pq)^{3/2})$. \square

Une application de ce qui précède est une nouvelle solution au problème de mots pour (\mathcal{P}) :

PROPOSITION 3.9 (**problème de mots III**). *Le problème de mots pour la présentation (\mathcal{P}) du monoïde H^+ est décidable.*

DÉMONSTRATION. Puisque le R -retournement à droite est complet pour la présentation (\mathcal{P}) , deux mots u, v de Θ^* représentent le même éléments du monoïde Θ' si, et seulement si, le R -retournement à droite de $\bar{u}v$ termine avec le mot vide. Par la proposition 3.7, ceci est décidable. \square

En termes de complexité algorithmique, on déduit directement de la proposition 3.8 :

PROPOSITION 3.10 (**complexité**). *La complexité de la solution au problème de mots donnée dans la proposition 3.9 est de complexité $O(n^{5/2})$ en temps, et $O(n^{3/2})$ en espace.*

Quand on le compare avec la proposition II.3.39, ce résultat montre que, en termes de solution au problème de mots, la méthode de forme normale du chapitre II est plus efficace que la méthode du retournement de facteur, au moins asymptotiquement.

Par contre, l'intérêt du retournement est de résoudre également le problème de l'existence de multiples communs à droite :

PROPOSITION 3.11 (**multiples communs**). *Déterminer si deux éléments du monoïde H^+ ont un multiple commun à droite est un problème décidable.*

DÉMONSTRATION. Soient u et v deux mots de Θ^* . Alors les éléments $[u]$ et $[v]$ de H^+ ont un multiple à droite commun dans H^+ si, et seulement si, le retournement à droite du mot $\bar{u}v$ réussit, c'est-à-dire termine avec un mot de la forme $v'\bar{u}'$, auquel cas on sait que $[uv']$ (et $[vu']$) est ppcm à droite de $[u]$ et $[v]$. La proposition 3.7 donne la décidabilité (et un algorithme effectif). \square

Bien entendu, on a les mêmes bornes de complexité que pour le problème de mots.

EXEMPLE 3.12. Considérons les deux mots

$$u := \theta_4\theta_2\theta_1\theta_5\theta_6\theta_3 \quad \text{et} \quad v := \theta_2\theta_4\theta_6\theta_1\theta_3\theta_9.$$

Utilisant l'alphabet Θ' et le R' -retournement, on trouve

$$\bar{u}v \curvearrowright \underline{\theta_3} \cdot \underline{\theta_1} \cdot \underline{\theta_5\theta_7} \cdot \underline{\theta_6} \cdot \underline{\theta_1} \cdot \underline{\theta_3} \cdot \underline{\theta_9}.$$

Or, on n'a pas dans R' de relation de la forme $\underline{\theta_5\theta_7} \cdot \dots = \underline{\theta_6} \cdot \dots$ (cas 1.2 de la démonstration de la proposition 3.1), donc le R' -retournement bloque. On conclut que les mots u et v ne représentent pas le même élément de H^+ , et, de plus, que les éléments $[u]$ et $[v]$ n'ont pas de multiple commun à droite dans H^+ . Par comparaison, on obtient

$$\text{red}_H(u) = \theta_4\theta_2\theta_4\theta_5\theta_1\theta_3 \quad \text{et} \quad \text{red}_H(v) = \theta_2\theta_4\theta_6\theta_7\theta_1\theta_3,$$

ce qui permet aussi de conclure $[u] \neq [v]$, mais ne dit rien sur les éventuels multiples communs.

Considérons maintenant

$$u := \theta_4\theta_2\theta_1\theta_5\theta_6\theta_3 \quad \text{et} \quad v := \theta_2\theta_4\theta_5\theta_1\theta_3\theta_9.$$

On vérifie qu'on a $\bar{u}v \curvearrowright \varepsilon$, d'où $[u] = [v]$. Or, on vérifie de même

$$\text{red}_H(u) = \theta_4\theta_2\theta_4\theta_5\theta_1\theta_3 = \text{red}_H(v).$$

Enfin, considérons

$$u := \theta_4\theta_2\theta_1\theta_5\theta_6\theta_3\theta_7 \quad \text{et} \quad v := \theta_2\theta_4\theta_5\theta_1\theta_3\theta_9\theta_8.$$

Cette fois, on vérifie qu'on a $\bar{u}v \curvearrowright \theta_8\theta_{10} \cdot \overline{\theta_7\theta_8}$: le mot est terminal, mais non vide. Ici on a conclut à nouveau $[u] = [v]$, mais, en plus, on déduit que $[u]$ et $[v]$ ont un ppcm à droite dans H^+ , à savoir $[u] \cdot \theta_8\theta_{10}$, qui est aussi $[v] \cdot \theta_7\theta_8$. Avec la forme normale, on obtient

$$\text{red}_H(u) = \theta_4\theta_2\theta_4\theta_5\theta_5\theta_1\theta_3 \neq \text{red}_H(v) = \theta_4\theta_2\theta_4\theta_5\theta_6\theta_1\theta_3,$$

qui dit que u et v ne représentent pas le même élément de H^+ , mais ne dit rien quant à leurs possibles multiples communs à droite.

3.3. Terminaison du retournement à gauche. Le dernier résultat de cette section concerne le retournement à gauche — dont on sait qu'il n'est pas complet pour la présentation (\mathcal{P}) .

PROPOSITION 3.13 (terminaison). *Le retournement à gauche pour la présentation (\mathcal{P}) est toujours terminant.*

DÉMONSTRATION. On a déjà noté dans la section 2.3 que les relations de la présentation (\mathcal{P}) peuvent se réécrire

$$(3.14) \quad \theta_i\theta_{i-1}\theta_i = \theta_{i-1}\theta_i\theta_j \quad \text{pour } j = i + 2,$$

$$(3.15) \quad \theta_{j-1}\theta_i = \theta_i\theta_j \quad \text{pour } j > i + 2.$$

On note $<^{\text{Lex}}$ l'ordre antilexicographique sur les suites d'entiers de longueur n : la relation $(a_1, \dots, a_n) <^{\text{Lex}} (b_1, \dots, b_p)$ est vraie si, et seulement si, on a $n < p$, ou si on a $n = p$ et il existe k vérifiant $a_k < b_k$ et $\forall i > k (a_i = b_i)$. La relation $<^{\text{Lex}}$ est un ordre strict et, comme on considère des suites de longueur fixée à valeurs dans \mathbb{N} , c'est un bon ordre : il n'existe pas de suite infinie descendante.

Pour w dans $(\Theta \cup \bar{\Theta})^*$, on pose

$$\max(w) := \max\{i \in \mathbb{N}^* \mid \theta_i \text{ ou } \bar{\theta}_i \text{ apparaît dans } w\},$$

et, notant $|w|_{\theta_i}$ le nombre de lettres θ_i et $\bar{\theta}_i$ dans w , on introduit

$$\nu(w) := (|w|_{\theta_1}, \dots, |w|_{\theta_{\max(w)}}).$$

On va montrer l'implication

$$(3.16) \quad w \curvearrowright w' \quad \text{entraîne} \quad \nu(w') <^{\text{Lex}} \nu(w).$$

Par construction, le retournement à gauche ne fait pas apparaître de lettre d'indice plus grand que les indices des lettres initiales, et on reste donc dans les mots sur un alphabet fixe $\{\theta_1, \dots, \theta_n\}$, donc sur un intervalle d'indices $\{1, \dots, n\}$ sur lequel l'ordre lexicographique est bien fondé.

On considérant les divers cas possibles. Retourner à gauche w en w' signifie

- ou bien supprimer un facteur $\theta_i\bar{\theta}_i$: on a alors ou bien $\max(w') < \max(w)$, ou bien $\max(w') = \max(w)$ et

$$\nu(w') = (|w|_{\theta_1}, \dots, |w|_{\theta_i} - 2, \dots, |w|_{\theta_{\max(w)}}),$$

donc $\nu(w') <^{\text{Lex}} \nu(w)$ dans les deux cas ;

- ou bien remplacer un facteur $\theta_i \overline{\theta_j}$ par $\overline{\theta_{j-1}} \theta_i$ ou $\theta_j \overline{\theta_i}$ par $\overline{\theta_i} \theta_{j-1}$ avec $j > i + 2$: on a alors ou bien $\max(w') < \max(w)$, ou bien $\max(w') = \max(w)$ et

$$\nu(w') = (|w|_{\theta_1}, \dots, |w|_{\theta_{j-1}} + 1, |w|_{\theta_j} - 1, \dots, w_{\theta_{\max(w)}}),$$

donc $\nu(w') <^{\text{Lex}} \nu(w)$ dans les deux cas ;

- ou bien remplacer un facteur $\theta_i \overline{\theta_{i+2}}$ par $(\overline{\theta_i \theta_{i-1}}) \theta_{i-1} \theta_i$ ou un facteur $\theta_{i+2} \overline{\theta_i}$ par $(\overline{\theta_{i-1} \theta_i}) \theta_i \theta_{i-1}$: on a alors ou bien $\max(w') < \max(w)$, ou bien $\max(w') = \max(w)$ et

$$\nu(w') = (|w|_{\theta_1}, \dots, |w|_{\theta_{i-1}} + 2, |w|_{\theta_i} + 1, |w|_{\theta_{i+1}}, |w|_{\theta_{i+2}} - 1, \dots, w_{\theta_{\max(w)}}),$$

donc $\nu(w') <^{\text{Lex}} \nu(w)$ dans tous les cas.

Comme $<^{\text{Lex}}$ est bien fondée, on ne peut pas avoir de suite de retournement à gauche infinie. \square

COROLLAIRE 3.17 (décidabilité). *Le retournement à gauche pour la présentation (\mathcal{P}) est décidable.*

DÉMONSTRATION. Quels que soient le mot signé initial w , on arrive en un nombre fini d'étapes soit à un mot terminal, soit à un blocage, et donc, dans tous les cas, à une conclusion en temps fini. \square

Appendice : variantes de la présentation

La présentation (\mathcal{P}) a été introduite au chapitre I comme un hybride plus ou moins naturel des présentations standards du monoïde de Thompson F^+ et du monoïde de tresses B_∞^+ , suivant l'« égalité » (E). On peut se demander si choisir d'autres valeurs du paramètre de décalage (le "3" de la relation $\theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{i+3}$ pour $j = i + 1$) pourrait mener à d'autres monoïdes intéressants. Le résultat suivant suggère une réponse négative : tout autre choix de décalage donne une présentation pour laquelle le retournement à droite n'est pas complet.

Proposition. *Quelle que soit la valeur de k positive différente de 3, le retournement à droite n'est pas complet pour la présentation*

$$(*) \quad \left\langle \theta_1, \theta_2, \dots \left| \begin{array}{ll} \theta_j \theta_i = \theta_i \theta_{j+1} & \text{pour } j \geq i + 2 \\ \theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{i+k} & \text{pour } j = i + 1 \end{array} \right. \right\rangle^+.$$

DÉMONSTRATION. On considère la condition du cube pour $(\theta_1, \theta_2, \theta_3)$. Pour $k = 0$, on trouve

$$\overline{\theta_1} \theta_3 \overline{\theta_3} \theta_2 \curvearrowright \theta_4 \theta_2 \theta_1 \theta_5 \overline{\theta_2} \overline{\theta_1} \overline{\theta_2} \overline{\theta_3},$$

puis

$$\overline{\theta_5} \overline{\theta_1} \overline{\theta_2} \overline{\theta_4} \overline{\theta_1} \theta_2 \theta_3 \theta_2 \theta_1 \theta_2 \curvearrowright \theta_6 \theta_1 \overline{\theta_6} \overline{\theta_7}.$$

Pour $k = 1$, on trouve successivement

$$\overline{\theta_1} \theta_3 \overline{\theta_3} \theta_2 \curvearrowright \theta_4 \theta_2 \theta_2 \theta_5 \overline{\theta_2} \overline{\theta_1} \overline{\theta_3} \overline{\theta_3},$$

$$\overline{\theta_5} \overline{\theta_2} \overline{\theta_2} \overline{\theta_4} \overline{\theta_1} \theta_2 \theta_3 \theta_3 \theta_1 \theta_2 \curvearrowright \theta_6 \theta_5 \overline{\theta_6} \overline{\theta_6}.$$

Pour $k = 2$, on trouve

$$\begin{aligned} \overline{\theta_1 \theta_3 \theta_3 \theta_2} &\curvearrowright \theta_4 \theta_2 \theta_3 \theta_5 \overline{\theta_2 \theta_1 \theta_4 \theta_3}, \\ \overline{\theta_5 \theta_3 \theta_2 \theta_4 \theta_1 \theta_2 \theta_3 \theta_4 \theta_1 \theta_2 \theta_6 \theta_7}. \end{aligned}$$

Pour $k = 4$, on trouve

$$\begin{aligned} \overline{\theta_1 \theta_3 \theta_3 \theta_2} &\curvearrowright \theta_4 \theta_2 \theta_5 \theta_5 \overline{\theta_2 \theta_1 \theta_6 \theta_3}, \\ \overline{\theta_5 \theta_5 \theta_2 \theta_4 \theta_1 \theta_2 \theta_3 \theta_6 \theta_1 \theta_2 \theta_9 \theta_5}. \end{aligned}$$

Pour $k = 5$, on trouve

$$\begin{aligned} \overline{\theta_1 \theta_3 \theta_3 \theta_2} &\curvearrowright \theta_4 \theta_2 \theta_6 \theta_5 \overline{\theta_2 \theta_1 \theta_7 \theta_3}, \\ \overline{\theta_5 \theta_6 \theta_2 \theta_4 \theta_1 \theta_2 \theta_3 \theta_7 \theta_1 \theta_2} &\curvearrowright \theta_{11} \theta_{11} \overline{\theta_5 \theta_6}. \end{aligned}$$

Finalement, pour $k > 5$, on trouve

$$\begin{aligned} \overline{\theta_1 \theta_3 \theta_3 \theta_2} &\curvearrowright \theta_4 \overline{\theta_1 \theta_3 \theta_2} \curvearrowright \theta_4 \theta_2 \theta_{1+k} \theta_5 \overline{\theta_2 \theta_1 \theta_{2+k} \theta_3}, \\ \overline{\theta_5 \theta_{1+k} \theta_2 \theta_4 \theta_1 \theta_2 \theta_3 \theta_{2+k} \theta_1 \theta_2} &\curvearrowright \theta_{3+k} \theta_{2+2k} \theta_{7+k} \overline{\theta_5 \theta_{2+k} \theta_{1+k}}. \end{aligned}$$

Dans chaque cas, on a trouvé à la fin un mot non vide, donc la condition du cube est fautive pour le triplet $(\theta_1, \theta_2, \theta_3)$. Par conséquent, le retournement à droite n'est pas complet pour la présentation considérée. \square

Les éléments simples de H^+

Il a été observé au chapitre II que, pour ce qui concerne la relation de division à droite, le monoïde H^+ a des points communs avec le monoïde de Thompson F^+ , tandis que les résultats du chapitre IV suggèrent que, pour ce qui concerne la division à gauche (donc les multiples à droite), le monoïde H^+ ressemble davantage au monoïde de tresses B_∞^+ , avec notamment la complétude du retournement à droite associé à la présentation (\mathcal{P}) et l'existence de ppcm à droite conditionnels. Dans le cas de B_∞^+ , on sait qu'un rôle très important est joué par les éléments de Garside Δ_n , où Δ_n est défini comme le ppcm à droite (et du reste aussi à gauche) des $n - 1$ atomes $\sigma_1, \dots, \sigma_{n-1}$, et par les diviseurs des éléments Δ_n , usuellement appelés éléments *simples* de B_∞^+ , au nombre de $n!$ dans B_n^+ . En particulier, les éléments simples forment une famille de Garside [28], et sont les briques de base pour la construction d'une forme normale fondamentale pour B_∞^+ , et pour son groupe de fractions B_∞ .

Il est donc très naturel d'étudier l'éventuelle transposition de ces résultats au monoïde H^+ . Le résultat n'est absolument pas évident, puisqu'on a vu qu'il n'est même pas vrai que H^+ admette toujours des multiples communs à droite. Ce qu'on va montrer ici, c'est que, dans H^+ , les atomes $\theta_1, \dots, \theta_{n-1}$ admettent un ppcm à droite, qu'on notera Δ_n comme dans le cas des tresses, et que les diviseurs à gauche des éléments Δ_n qu'on appellera éléments simples de H^+ , forment une famille intéressante — et même *très* intéressante! — aux propriétés directement réminiscentes de celles des familles de Garside, en particulier la famille des tresses simples de B_∞^+ .

Le chapitre comporte quatre sections. Dans la section 1, on introduit les éléments Δ_n à partir d'un représentant explicite, puis les éléments simples, et on établit une majoration explicite de leur plafond. Dans la section 2, on compte les éléments simples divisant Δ_n : ils sont au nombre de $2 \cdot 3^{n-2}$, en liaison avec une riche structure interne où apparaît une sorte de triangle de Pascal généralisé. Dans la section 3, on caractérise les formes normales des éléments simples (au sens du chapitre II) comme celles qui évitent un certain nombre de facteurs interdits explicites. Enfin, dans la section 4, on montre l'existence d'une structure « presque-Garside » sur le monoïde H^+ en construisant des décompositions dites gloutonnes pour les éléments de H^+ à partir des éléments simples, suivant l'approche de la théorie de Garside, mais avec des différences qui limitent la portée des résultats.

Au plan technique, ce sont les sections 2 et 3.2, et en particulier la caractérisation explicite des formes normales des éléments simples (proposition 3.24), qui reposent sur les démonstrations les plus sophistiquées du chapitre, et de toute la thèse Des raisonnements inductifs délicats et nécessitant de nombreuses étapes préparatoires y sont développés.

1. Les éléments Δ_n

Dans cette section, on définit les éléments Δ_n comme ppcm à droite des atomes, et on commence l'étude de leurs diviseurs à gauche, appelés éléments simples. Outre l'existence même des éléments Δ_n , le résultat principal (facile) de cette section préliminaire est la description exhaustive des atomes divisant à gauche Δ_n (proposition 1.25).

La section est divisée en deux sous-sections. Dans la section 1.1, on définit Δ_n à partir d'un représentant explicite et on montre qu'il est le ppcm à droite des atomes en utilisant les résultats du chapitre IV. Dans la sous-section 1.2, on introduit les éléments simples et leur indice, et on établit la proposition 1.25 mentionnée ci-dessus, ainsi qu'une majoration du plafond d'un élément simple en termes de son indice et de sa longueur (lemme 1.26).

1.1. Le ppcm de $\theta_1, \dots, \theta_{n-1}$. On sait que, dans le monoïde H^+ , deux éléments qui ont un multiple commun à droite ont un ppcm à droite, mais on sait aussi qu'il existe des éléments qui n'ont pas de multiple commun à droite. On étudie ici le cas des éléments $\theta_1, \dots, \theta_{n-1}$, dont on va montrer qu'ils ont toujours un multiple commun à droite, donc un ppcm à droite. Pour cela, on introduit directement une famille de mots dont on montrera ensuite qu'ils représentent le ppcm recherché.

DÉFINITION 1.1 (mot $\underline{\Delta}_n$, élément Δ_n). On introduit inductivement

$$(1.2) \quad \underline{\Delta}_1 := \varepsilon, \quad \underline{\Delta}_2 := \theta_1, \quad \text{et} \quad \underline{\Delta}_n := \underline{\Delta}_{n-1}\theta_{3n-7}\theta_{3n-5} \quad \text{pour } n \geq 2,$$

et on note Δ_n la classe de $\underline{\Delta}_n$ dans H^+ .

On trouve ainsi $\underline{\Delta}_1 = \varepsilon$, $\underline{\Delta}_2 = \theta_1$, puis $\underline{\Delta}_3 = \theta_1\theta_2\theta_4$, $\underline{\Delta}_4 = \theta_1\theta_2\theta_4\theta_5\theta_7$, etc. D'une façon générale, $\underline{\Delta}_n$ est le mot de longueur $2n-3$ formé des lettres θ_i pour i croissant de 1 à $3n-5$ et non multiple de 3, soit

$$(1.3) \quad \underline{\Delta}_n = \theta_1\theta_2\widehat{\theta_3} \cdots \theta_{3i-1}\widehat{\theta_{3i}}\theta_{3i+1} \cdots \theta_{3n-7}\widehat{\theta_{3n-6}}\theta_{3n-5}$$

(le chapeau indique les générateurs absents).

Noter que la suite des indices des générateurs apparaissant dans le mot $\underline{\Delta}_n$ est strictement croissante. Par le lemme I.3.13, on déduit immédiatement les valeurs des paramètres numériques associés aux Δ_n dans la section I.3.2 :

LEMME 1.4. *Pour tout $n \geq 2$, on a*

$$(1.5) \quad |\underline{\Delta}_n| = 2n - 3, \quad [\underline{\Delta}_n] = \text{ht}(\underline{\Delta}_n) = 3n - 5, \quad \mathfrak{a}(\underline{\Delta}_n) = 3n^2 - 9n + 7.$$

On en déduit donc pour les éléments Δ_n

$$(1.6) \quad |\Delta_n| = 2n - 3, \quad [\Delta_n] = 3n - 5,$$

d'où $\text{ht}(w) \leq 3n - 5$ pour tout représentant w de Δ_n .

PROPOSITION 1.7 (ppcm). *Pour tout $n \geq 2$, l'élément Δ_n est le ppcm à droite de $\theta_1, \dots, \theta_{n-1}$.*

DÉMONSTRATION. On montre le résultat par récurrence sur $n \geq 2$. Pour $n = 2$, le résultat est trivial. Supposons $n \geq 3$. Considérons le retournement à droite du mot signé $\overline{\theta_{n-1}\Delta_{n-1}}$. On trouve

$$\begin{aligned} \overline{\theta_{n-1}\Delta_{n-1}} &= \overline{\theta_{n-1}\theta_1\theta_2 \cdots \theta_{3n-10}\theta_{3n-8}} \\ &\curvearrowright \overline{\theta_1\theta_n\theta_2 \cdots \theta_{3n-10}\theta_{3n-8}} \\ &\curvearrowright \overline{\theta_1\theta_2\overline{\theta_{n+1}} \cdots \theta_{3n-10}\theta_{3n-8}} \\ &\cdots \curvearrowright \overline{\theta_1\theta_2 \cdots \overline{\theta_{3n-8}}\theta_{3n-10}\theta_{3n-8}} \\ &\curvearrowright \overline{\theta_1\theta_2 \cdots \theta_{3n-10}\overline{\theta_{3n-7}}\theta_{3n-8}} \\ &\curvearrowright \overline{\theta_1\theta_2 \cdots \theta_{3n-10}\theta_{3n-8}\overline{\theta_{3n-7}\theta_{3n-5}}\overline{\theta_{3n-7}}}. \end{aligned}$$

Par conséquent, il existe un mot positif v vérifiant

$$(1.8) \quad \overline{\theta_{n-1}\Delta_{n-1}} \curvearrowright v\overline{\theta_{3n-5}\theta_{3n-7}}.$$

Par la proposition IV.1.8, conjuguée au fait que le retournement à droite pour la présentation (\mathcal{P}) est complet, la relation (1.8) implique que les éléments $[\Delta_{n-1}]$, c'est-à-dire Δ_{n-1} , et θ_{n-1} ont un ppcm à droite dans H^+ , et que celui-ci est $[\Delta_{n-1}]\theta_{3n-7}\theta_{3n-5}$, c'est-à-dire, par définition, $[\Delta_n]$, donc Δ_n . Par hypothèse d'induction, Δ_{n-1} est ppcm à droite de $\theta_1, \dots, \theta_{n-2}$. On déduit que Δ_n est ppcm à droite du ppcm à droite de $\theta_1, \dots, \theta_{n-2}$ et de θ_{n-1} , donc, par associativité du ppcm à droite, Δ_n est ppcm à droite de $\theta_1, \dots, \theta_{n-1}$. \square

Le mot $\underline{\Delta}_3$, c'est-à-dire $\theta_1\theta_2\theta_4$, n'est pas normal au sens du système de réécriture \mathcal{E}_H du chapitre II. Il est donc naturel de déterminer la forme normale des éléments Δ_n . (On rappelle la convention II.3.40 : par défaut, toutes les notions liées à la réécriture réfèrent à \mathcal{E}_H .)

PROPOSITION 1.9 (forme normale). *Pour $n \geq 3$, la forme normale de l'élément Δ_n est*

$$(1.10) \quad \text{NF}(\Delta_n) = \theta_{n-1} \cdot \theta_{n-2}\theta_{n-1} \cdot \theta_{n-3}\theta_{n-2} \cdot \cdots \cdot \theta_2\theta_3 \cdot \theta_1\theta_2.$$

DÉMONSTRATION. On note que le mot de droite dans (1.10) est réduit, puisqu'il évite tous les facteurs de \mathcal{I} . Pour montrer que ce mot est la forme normale de Δ_n , il suffit donc de montrer que $\underline{\Delta}_n$ est réductible au mot en question. On procède par induction sur $n \geq 3$. Pour $n = 3$, on trouve

$$\underline{\Delta}_3 = \theta_1\theta_2\theta_4 \Rightarrow \theta_2\theta_1\theta_2 = \theta_2 \cdot \theta_1\theta_2,$$

ce qui est le résultat annoncé. Supposons $n \geq 4$. On trouve alors

$$\underline{\Delta}_n = \Delta_{n-1}\theta_{3n-7}\theta_{3n-5} \quad \text{par définition,}$$

$$\Rightarrow \theta_{n-2} \cdot \theta_{n-3} \theta_{n-2} \cdot \cdots \cdot \theta_1 \theta_2 \cdot \overline{\theta_{3n-7} \theta_{3n-5}}$$

par hypothèse d'induction,

$$\Rightarrow \theta_{n-2} \cdot \overline{\theta_{n-1}} \cdot \theta_{n-3} \theta_{n-2} \cdot \cdots \cdot \theta_1 \theta_2 \cdot \overline{\theta_{3n-5}}$$

en faisant migrer θ_{3n-7} de $2n - 6$ étapes vers la gauche jusque juste après θ_{n-2} en appliquant des règles $\theta_{j+1}\theta_i \rightarrow \theta_i\theta_j$ avec $j \geq i + 2$,

$$\Rightarrow \theta_{n-2} \cdot \theta_{n-1} \cdot \overline{\theta_{n+1}} \cdot \theta_{n-3} \theta_{n-2} \cdot \cdots \cdot \theta_1 \theta_2$$

en faisant migrer θ_{3n-5} de $2n - 6$ étapes vers la gauche jusque juste après θ_{n-1} en appliquant des règles $\theta_{j+1}\theta_i \rightarrow \theta_i\theta_j$ avec $j \geq i + 2$,

$$\Rightarrow \theta_{n-1} \cdot \theta_{n-2} \theta_{n-1} \cdot \theta_{n-3} \theta_{n-2} \cdot \cdots \cdot \theta_1 \theta_2$$

en appliquant la règle $\theta_{n-2}\theta_{n-1}\theta_{n+1} \rightarrow \theta_{n-1}\theta_{n-2}\theta_{n-1}$,

ce qui est le résultat annoncé. \square

On a donc, par exemple,

$$\text{NF}(\Delta_2) = \theta_1, \text{NF}(\Delta_3) = \theta_2\theta_1\theta_2, \text{NF}(\Delta_4) = \theta_3\theta_2\theta_3\theta_1\theta_2, \text{ etc.}$$

En vue d'utilisations futures, on mentionne une autre écriture des éléments Δ_m et, pour cela, on introduit des mots $\underline{\Delta}_m$ et les éléments associés Δ_m pour m demi-entier. Par définition, pour tout $n \geq 2$, le mot $\underline{\Delta}_n \theta_{3n-4}$ est le préfixe de longueur $2n - 2$ de $\underline{\Delta}_{n+1}$, et c'est donc une sorte de milieu entre $\underline{\Delta}_n$ et $\underline{\Delta}_{n+1}$. La convention suivante est donc naturelle et elle sera très souvent utile dans la suite :

DÉFINITION 1.11 (**mot** $\underline{\Delta}_{n+0,5}$, **élément** $\Delta_{n+0,5}$). Pour $n \geq 2$, on définit

$$(1.12) \quad \underline{\Delta}_{n+0,5} := \underline{\Delta}_n \theta_{3n-4}, \quad \text{et} \quad \Delta_{n+0,5} := [\underline{\Delta}_{n+0,5}].$$

Par exemple, on trouve $\Delta_{2,5} := \theta_1\theta_2$, puis $\Delta_{3,5} := \theta_1\theta_2\theta_4\theta_5$, et, plus généralement

$$(1.13) \quad \underline{\Delta}_{n+0,5} = \theta_1\theta_2\widehat{\theta_3} \cdots \theta_{3i-1}\widehat{\theta_{3i}}\theta_{3i+1} \cdots \theta_{3n-7}\widehat{\theta_{3n-6}}\theta_{3n-5}\theta_{3n-4}.$$

Pour tout $n \geq 2$, on a immédiatement

$$(1.14) \quad \Delta_n \preceq \Delta_{n+0,5} \preceq \Delta_{n+1},$$

et on vérifie facilement la formule, analogue à (1.9),

$$(1.15) \quad \text{NF}(\Delta_{n+0,5}) = \theta_{n-1}\theta_n \cdot \theta_{n-2}\theta_{n-1} \cdot \theta_{n-3}\theta_{n-2} \cdot \cdots \cdot \theta_2\theta_3 \cdot \theta_1\theta_2,$$

donc, par exemple,

$$\text{NF}(\Delta_{2,5}) = \theta_1\theta_2, \text{NF}(\Delta_{3,5}) = \theta_2\theta_3\theta_1\theta_2, \text{NF}(\Delta_{4,5}) = \theta_3\theta_4\theta_2\theta_3\theta_1\theta_2, \text{ etc.}$$

LEMME 1.16. *Pour tout entier $n \geq 3$, on a*

$$(1.17) \quad \underline{\Delta}_n \equiv \theta_{n-1}\underline{\Delta}_{n-0,5}.$$

DÉMONSTRATION. On a établi ci-dessus dans (1.8) la relation

$$\overline{\theta_{n-1}\underline{\Delta}_{n-1}} \curvearrowright \underline{\Delta}_{n-0,5}\overline{\theta_{3n-5}\theta_{3n-7}},$$

qui implique

$$\theta_{n-1} \cdot \underline{\Delta}_{n-0.5} \equiv \underline{\Delta}_{n-0.5} \cdot \theta_{3n-5},$$

soit (1.17) puisque, par définition, $\underline{\Delta}_n$ est $\underline{\Delta}_{n-0.5}\theta_{3n-5}$. \square

Ainsi, on a obtenu (au moins) trois expressions distinctes pour Δ_n , distinctes pour $n \geq 4$, à savoir

$$\begin{aligned} \Delta_4 &= \theta_1\theta_2\theta_4\theta_5\theta_7 = \theta_3\theta_2\theta_3\theta_1\theta_2 = \theta_3\theta_1\theta_2\theta_4\theta_5, \\ \Delta_5 &= \theta_1\theta_2\theta_4\theta_5\theta_7\theta_8\theta_9 = \theta_4\theta_3\theta_4\theta_2\theta_3\theta_1\theta_2 = \theta_4\theta_1\theta_2\theta_4\theta_5\theta_7\theta_8, \quad \text{etc.} \end{aligned}$$

Ces expressions montrent que Δ_n divise à gauche Δ_{n+1} , et y apparaît comme facteur en position 2, mais, pour le moment, rien ne permet de conclure que Δ_n ne divise pas à droite Δ_{n+1} . De façon symétrique, (1.15) montre que, $\Delta_{n+0.5}$ divise à droite $\Delta_{n+1.5}$ pour $n \geq 2$, et on peut montrer, par retournement à droite, qu'il le divise également à gauche.

REMARQUE 1.18. Avant de continuer, une question naturelle est celle de l'existence éventuelle d'un ppcm à gauche pour $\theta_1, \dots, \theta_{n-1}$. On a déjà répondu par la négative en montrant dans la proposition IV.2.13 que, quel que soit i , les éléments θ_i et θ_{i+1} n'ont pas de multiple commun à gauche. Contrairement au cas de B_∞^+ par exemple, il n'y a donc pas de contrepartie de $\underline{\Delta}_n$ à gauche dans H^+ .

1.2. Les diviseurs à gauche de Δ_n . On rappelle (section I.1.2) que, dans un monoïde M , la relation \preccurlyeq est la divisibilité à gauche, telle que $a \preccurlyeq b$ est vraie si, et seulement si, il existe dans M un élément x vérifiant $ax = b$.

DÉFINITION 1.19 (**simple, indice**). Pour $n \geq 1$ et $\ell \geq 0$, on pose

$$(1.20) \quad \Sigma_{n,\ell} := \{a \in H^+ \mid a \preccurlyeq \Delta_n \text{ et } |a| = \ell\},$$

$$(1.21) \quad \Sigma_n := \bigcup_{\ell \geq 0} \Sigma_{n,\ell} = \{a \in H^+ \mid a \preccurlyeq \Delta_n\}, \quad \text{et} \quad \Sigma := \bigcup_{n \geq 1} \Sigma_n.$$

Les éléments de Σ sont dits *simples*. Si a est simple, l'*indice* de a , noté $\text{ind}(a)$, est le plus petit entier $n \geq 1$ tel que a divise à gauche Δ_n .

Donc, un élément a de H^+ est simple si, et seulement si, $a \preccurlyeq \Delta_n$ est vrai pour au moins une valeur de n . Par construction, on a $\Delta_n \preccurlyeq \Delta_{n'}$ pour tout $n' \geq n$, et donc $a \preccurlyeq \Delta_n$ entraîne $a \preccurlyeq \Delta_{n'}$ pour $n' \geq n$. Par conséquent, les entiers pour lesquels a divisent Δ_n forment un intervalle $[p, \infty[$ de \mathbb{N} , et l'indice $\text{ind}(a)$ est le plus petit élément de cet intervalle. Donc :

$$(1.22) \quad \text{ind}(a) \leq n \quad \text{équivaut à} \quad a \preccurlyeq \Delta_n,$$

$$(1.23) \quad \text{ind}(a) = n \quad \text{équivaut à la conjonction} \quad a \preccurlyeq \Delta_n \text{ et } a \not\preccurlyeq \Delta_{n-1}.$$

Les équivalences ci-dessus peuvent suggérer de poser $\text{ind}(a) := \infty$ pour a non simple, mais on n'utilisera pas cette convention en pratique.

EXEMPLE 1.24. On a évidemment $\Sigma_{n,0} = \{1\}$ pour tout n , donc 1 est simple, d'indice 1.

Ensuite, on sait que, pour tout i , l'atome θ_i divise à gauche Δ_{i+1} . Par contre, il ne divise pas Δ_i , qui sinon serait le ppcm à droite de $\theta_1, \dots, \theta_i$, ce qui n'est pas le cas. Donc θ_i est dans $\Sigma_{i+1,1} \setminus \Sigma_{i,1}$, et il est simple, d'indice $i+1$.

À l'autre extrémité, pour $n \geq 2$, d'après (1.5), on a $\Sigma_{n,2n-3} = \{\Delta_n\}$, et, comme $a \preceq b$ implique $|a| \leq |b|$ dans H^+ , il est clair qu'on a $\Sigma_{n,\ell} = \emptyset$ pour $n \geq 2n-2$. Donc Δ_n est simple, d'indice n , et il n'existe pas d'élément simple d'indice n de longueur $\geq 2n-2$.

La première valeur non triviale est $n=3$, et, en plus des valeurs précédentes, on trouve

$$\Sigma_{3,1} = \{\theta_1, \theta_2\}, \quad \Sigma_{3,2} = \{\theta_1\theta_2, \theta_2\theta_1\},$$

d'où finalement $\Sigma_3 = \{1, \theta_1, \theta_2, \theta_1\theta_2, \theta_2\theta_1, \Delta_3\}$, qui a 6 éléments : on a vu que 1 a pour indice 1 et que θ_1 a pour indice 2 ; il est facile de vérifier que les 4 autres éléments de Σ_3 ont pour indice 3 (c'est-à-dire ne divisent pas Δ_2 , qui est θ_1).

Le lecteur pourra vérifier de même que Σ_4 a 18 éléments, et consulter la table 1 page 125 qui donne davantage de valeurs. Noter enfin que, par (1.14), l'élément $\Delta_{n+0,5}$ est simple d'indice $n+1$ pour tout $n \geq 2$.

Par la proposition 1.7, on sait que les atomes $\theta_1, \dots, \theta_{n-1}$ divisent Δ_n à gauche. On va maintenant vérifier que ce sont les seuls atomes divisant Δ_n , et même $\Delta_{n+0,5}$.

PROPOSITION 1.25 (atomes divisant). *Pour $n \geq 2$, les seuls atomes divisant $\Delta_{n+0,5}$ à gauche, donc, en particulier, les seuls atomes divisant Δ_n à gauche, sont $\theta_1, \dots, \theta_{n-1}$.*

DÉMONSTRATION. Comme rappelé ci-dessus, la proposition 1.7 implique $\theta_i \preceq \Delta_n$, donc *a fortiori* $\theta_i \preceq \Delta_{n+0,5}$ pour $i = 1, \dots, n-1$.

Ensuite, on trouve

$$\begin{aligned} \overline{\theta_n \Delta_{n+0,5}} &= \overline{\theta_n \Delta_n \theta_{3n-4}} \curvearrowright \theta_1 \theta_2 \cdots \theta_{3n-7} \theta_{3n-5} \theta_{3n-4} \overline{\theta_{3n-2}} \\ &\quad \cdots \overline{\theta_{3n-4} \theta_{3n-4}} \curvearrowright \Delta_n \theta_{3n-4} \overline{\theta_{3n-2}} = \Delta_{n+0,5} \overline{\theta_{3n-2}}, \end{aligned}$$

donc Δ_{n+1} , qui est $\Delta_{n+0,5} \theta_{3n-2}$, est le ppcm à droite de θ_n et $\Delta_{n+0,5}$. Or on a $|\Delta_{n+1}| = |\Delta_{n+0,5}| + 1$, donc $\Delta_{n+1} \neq \Delta_{n+0,5}$, d'où $\theta_n \not\preceq \Delta_{n+0,5}$.

Maintenant, pour $i \geq n+1$, on trouve de même

$$\begin{aligned} \overline{\theta_i \Delta_{n+0,5}} &= \overline{\theta_i \theta_1 \theta_2 \theta_4 \cdots \theta_{3n-7} \theta_{3n-5} \theta_{3n-4}} \\ &\quad \curvearrowright \cdots \curvearrowright \theta_1 \theta_2 \theta_4 \cdots \theta_{3n-7} \overline{\theta_{i+2n-4} \theta_{3n-5} \theta_{3n-4}} \\ &\quad \curvearrowright \theta_1 \theta_2 \theta_4 \cdots \theta_{3n-7} \theta_{3n-5} \overline{\theta_{i+2n-3} \theta_{3n-4}} \\ &\quad \curvearrowright \theta_1 \theta_2 \theta_4 \cdots \theta_{3n-7} \theta_{3n-5} \theta_{3n-4} \overline{\theta_{i+2n-2}}. \end{aligned}$$

Donc le ppcm à droite de θ_i et $\Delta_{n+0,5}$ est $\Delta_n \theta_{i+2n-2}$, qui n'est pas $\Delta_{n+0,5}$. Par conséquent, on a $\theta_i \not\preceq \Delta_{n+0,5}$. Donc aucun atome θ_i avec $i \geq n$ ne divise à gauche $\Delta_{n+0,5}$. \square

On a donc, pour tout $n \geq 2$, la valeur explicite

$$\Sigma_{n,1} = \{\theta_1, \dots, \theta_{n-1}\},$$

d'où, en notant (ici et partout) $\#A$ le cardinal d'un ensemble (fini) A , la valeur $\#\Sigma_{n,1} = n - 1$.

Par la formule (I.3.21) du chapitre I, le plafond d'un élément de H^+ donne une borne explicite sur les plafonds de ses diviseurs. Appliquant ceci aux éléments simples, ou plutôt à nouveau aux diviseurs à gauche de $\Delta_{n+0,5}$ (qui sont simples comme diviseurs de Δ_{n+1}), on obtient :

LEMME 1.26. *Si on a $a \preccurlyeq \Delta_{n+0,5}$ dans H^+ avec $n \geq 2$, alors on a*

$$(1.27) \quad [a] \leq n + |a| - 2.$$

En particulier, pour tout a dans $\Sigma_{n,\ell}$ et tout Θ -mot w représentant a , on a

$$(1.28) \quad [a] \leq n + \ell - 2 \quad \text{et} \quad \text{ht}(w) \leq n + \ell - 2.$$

DÉMONSTRATION. On montre (1.27) par récurrence sur $|a| \geq 1$. Pour $|a| = 1$, soit quand a est un atome θ_i , la proposition 1.25 implique $i \leq n - 1$, donc $[a] = i \leq n - 1 = n + 1 - 2$.

Supposons $|a| \geq 2$. Soit θ_i un diviseur propre à droite de a , qui existe puisque a n'est pas un atome, et posons $a = b\theta_i$. On a alors $|b| = |a| - 1 < |a|$. Par hypothèse, b est un diviseur à gauche de $\Delta_{n+0,5}$ de longueur $\ell - 1$, donc, par hypothèse de récurrence, on obtient $[b] \leq n + |a| - 3$.

Maintenant, l'hypothèse $a \preccurlyeq \Delta_{n+0,5}$ implique l'existence de c vérifiant $b\theta_i c = \Delta_{n+0,5}$. Alors la contribution de θ_i au plafond $[\Delta_{n+0,5}]$ est

$$i + |c| = i + 2n - |a| - 2.$$

D'un autre côté, comme les indices des générateurs dans le mot $\Delta_{n+0,5}$ sont strictement croissants, le lemme I.3.13 donne $[\Delta_{n+0,5}] = 3n - 4$. De la comparaison on déduit

$$i + 2n - |a| - 2 \leq 3n - 4,$$

donc $i \leq n + |a| - 2$. Finalement, par la formule (I.3.21), on obtient

$$[a] = [b\theta_i] = \max([b] + 1, i) \leq n + \ell - 2,$$

qui est (1.27). L'inégalité pour $\text{ht}(w)$ quand w représente a est alors claire puisque, par le lemme I.3.13, on a toujours $\text{ht}(w) \leq [w] = [a]$. \square

2. Dénombrement des éléments simples

On se propose maintenant de compter les éléments de Σ_n , c'est-à-dire les diviseurs à gauche de Δ_n . Dans le cas du monoïde de tresses B_∞^+ , le nombre est $n!$, car les diviseurs de Δ_n sont en bijection avec les permutations de $\{1, \dots, n\}$. Ici, on va établir un résultat similaire, la valeur étant $2 \cdot 3^{n-2}$, à nouveau exponentielle par rapport à n .

La démonstration est délicate, et requiert d'analyser la structure fine de chacun des ensembles $\Sigma_{n,\ell}$, en partitionnant ces ensembles en quatre sous-ensembles, à savoir $\Sigma_{n-1,\ell}$ et trois sous-ensembles définis inductivement. La

section est divisée en trois parties. Dans la section 2.1, on établit des résultats techniques fins sur la structure des diviseurs de Δ_n , qui constituent le noyau technique de toute l'étude : deviner les énoncés corrects n'est pas facile, et les démontrer requiert ensuite des récurrences souvent délicates nécessitant de considérer des cas très multiples. Dans la section 2.2, on exploite les résultats précédents pour partitionner l'ensemble des diviseurs de Δ_n en quatre familles explicites définies à partir de diviseurs de Δ_{n-1} , pavant le chemin pour une détermination par récurrence sur n . Enfin, dans la section 2.3, on utilise la partition ci-dessus pour obtenir les récurrences numériques voulues sur les nombres de diviseurs de longueur ℓ de Δ_n , qui apparaissent dans un triangle de Pascal généralisé, et, finalement, déduire par sommation le nombre total de diviseurs, soit $2 \cdot 3^{n-2}$ pour Δ_n .

2.1. Résultats préparatoires. Notre but final est de compter les éléments de $\Sigma_{n,\ell}$, c'est-à-dire les diviseurs à gauche de Δ_n de longueur ℓ .

NOTATION 2.1 (**entiers** $N_{n,\ell}$). Pour $n \geq 1$ et $\ell \geq 0$, on pose

$$N_{n,\ell} := \#\Sigma_{n,\ell} = \#\{a \in H^+ \mid a \preceq \Delta_n \text{ et } |a| = \ell\}.$$

Par exemple, on a établi plus haut les valeurs particulières

$$N_{n,0} = 1, \quad N_{n,1} = n - 1, \quad N_{n,2n-3} = 1, \quad N_{n,\ell} = 0 \text{ pour } \ell \geq 2n - 2.$$

Comme la détermination directe de l'ensemble $\Sigma_{n,\ell}$ est délicate, on va le partitionner en ensembles plus simples.

DÉFINITION 2.2 (**familles** $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}, \Sigma_{n,\ell}^{III}$). Pour $n \geq 4$ et $\ell \geq 2$, on pose

$$\text{(type 0)} \quad \Sigma_{n,\ell}^0 := \{a \mid a \preceq \Delta_{n-1} \text{ et } |a| = \ell\},$$

$$\text{(type I)} \quad \Sigma_{n,\ell}^I := \{\theta_{n-1}a \mid a \preceq \Delta_{n-1} \text{ et } |a| = \ell - 1\},$$

$$\text{(type II)} \quad \Sigma_{n,\ell}^{II} := \{\theta_{n-2}\theta_{n-1}a \mid a \preceq \Delta_{n-1,5} \text{ et } |a| = \ell - 2\},$$

$$\text{(type III)} \quad \Sigma_{n,\ell}^{III} := \{\theta_{n-1}\theta_{n-2}\theta_{n-1}a \mid \theta_{n-2}a \preceq \Delta_{n-1} \text{ et } |a| = \ell - 3\}.$$

La notation suggère que le premier type est spécial : les éléments de type 0 sont des diviseurs de Δ_n dont l'indice est $\leq n-1$ et, de fait, le « vrai » résultat est une partition en trois types de l'ensemble des diviseurs de Δ_n d'indice n . Notre but est, à la fin de la section 2.2, le résultat suivant :

PROPOSITION 2.3 (**partition**). Pour $n \geq 4$ et $2 \leq \ell \leq 2n - 3$, les ensembles $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}$, et $\Sigma_{n,\ell}^{III}$ forment une partition de $\Sigma_{n,\ell}$.

Pour cela, on montrera successivement que (i) ces ensembles sont inclus dans $\Sigma_{n,\ell}$, (ii) ils sont disjoints deux à deux, et (iii) ils recouvrent $\Sigma_{n,\ell}$. Chacune de ces trois étapes ci-dessus nécessite des résultats préliminaires, par lesquels on commence ici. Notons que, par définition, on a $\Sigma_{n,\ell}^0 = \Sigma_{n-1,\ell}$ et $\Sigma_{n,\ell}^I = \theta_{n-1}\Sigma_{n-1,\ell-1}$. Par ailleurs, on a

$$\Delta_{n-1} = \Delta_{n-1,5}\theta_{3n-8},$$

donc $\Sigma_{n,\ell}^{\text{II}} \subseteq \theta_{n-2}\theta_{n-1}\Sigma_{n-1,\ell-2}$. Un point technique important sera de montrer que, pour tout a dans $\Sigma_{n-1,\ell-2}$, l'énoncé $a \preccurlyeq \Delta_{n-1,5}$ est équivalent à $\theta_{n-2} \not\preccurlyeq a$, d'où

$$\{a \in \Sigma_{n-1,\ell-2} \mid a \preccurlyeq \Delta_{n-1,5}\} \cup \{a \in \Sigma_{n-1,\ell-2} \mid \theta_{n-2} \preccurlyeq a\} = \Sigma_{n-1,\ell-2},$$

faisant apparaître une relation inductive entre l'ensemble $\Sigma_{n,\ell}$ et les trois ensembles $\Sigma_{n-1,\ell}$, $\Sigma_{n-1,\ell-1}$, et $\Sigma_{n-1,\ell-2}$.

Le premier résultat, déterminant pour étudier les ensembles $\Sigma_{n,\ell}^{\text{II}}$, fournit une forme générale pour les représentants de Δ_n en fonction d'un représentant de $\Delta_{n-0,5}$ (c'est-à-dire de $\Delta_{n-1}\theta_{3n-7}$) et de la dernière lettre θ_{3n-5} poussée vers la gauche (avec un indice décré en conséquence).

LEMME 2.4. *Pour $n \geq 3$, tout représentant de Δ_n est de la forme*

$$(2.5) \quad w_1\theta_{n+|w_1|-1}w_2$$

avec $w_1w_2 \equiv \Delta_{n-0,5}$; de plus, dans ce cas, on a $w_1\theta_{n+|w_1|-1} \equiv \theta_{n-1}w_1$.

DÉMONSTRATION. On montre le résultat pour un représentant w de Δ_n par induction sur la distance combinatoire p entre les mots Δ_n et w , c'est-à-dire le nombre minimal de relations de la présentation (\mathcal{P}) nécessaire pour transformer Δ_n en w , noté $\text{dist}(\Delta_n, w)$.

Pour $p = 0$, on a $w = \Delta_n = \Delta_{n-0,5}\theta_{3n-5}$ et le résultat est vrai pour $w_1 := \Delta_{n-0,5}$ et $w_2 := \varepsilon$.

Supposons $p \geq 1$. Alors il existe w' vérifiant $\text{dist}(\Delta_n, w') = p - 1$ et $\text{dist}(w', w) = 1$. On écrit $w' = u_1v'u_2$ et $w = u_1vu_2$ avec (v', v) relation de (\mathcal{P}) . Par hypothèse de récurrence appliquée à w' , il existe deux mots w'_1 et w'_2 vérifiant $w' = w'_1\theta_{n+|w'_1|-1}w'_2$ avec $w'_1w'_2 \equiv \Delta_{n-0,5}$.

On a plusieurs cas à traiter selon la position de v' dans w' . Si u_1v' est un préfixe de w'_1 , c'est-à-dire qu'il existe u''_1 vérifiant $w'_1 = u_1v'u''_1$, on trouve

$$w' = u_1v'u''_1\theta_{n+|w'_1|-1}w'_2 \quad \text{et} \quad w = u_1vu''_1\theta_{n+|w'_1|-1}w'_2.$$

Or, on a $u_1vu''_1w'_2 \equiv u_1v'u''_1w'_2 = w'_1w'_2 \equiv \Delta_{n-0,5}$, d'où le résultat avec $w_1 := u_1vu''_1$ et $w_2 := w'_2$. Le raisonnement est analogue si $v'u_2$ est un suffixe de w'_2 . Il reste les cas où $\theta_{n+|w'_1|-1}$ apparaît dans v' .

Cas 1 : (v', v) est une relation de type 2. Alors v' est un mot de longueur 2, soit du type $\theta_i\theta_j$ avec $j \geq i + 3$, soit du type $\theta_i\theta_j$ avec $j \leq i - 2$. Comme la lettre $\theta_{n+|w'_1|-1}$ apparaît dans v' soit comme première, soit comme seconde lettre, il y a quatre cas possibles.

Sous-cas 1.1 : θ_i est la dernière lettre de w'_1 et on a $j = n + |w'_1| - 1 \geq i + 3$. Si on pose $w'_1 := w''_1\theta_i$, on obtient

$$w' = w''_1\theta_i\theta_{n+|w'_1|-1}w'_2 \quad \text{et} \quad w = w''_1\theta_{n+|w'_1|-2}\theta_iw'_2 = w''_1\theta_{n+|w'_1|-1}\theta_iw'_2.$$

De plus, on a $w''_1\theta_iw'_2 \equiv \Delta_{n-0,5}$, d'où le résultat pour $w_1 := w''_1$ et $w_2 := \theta_iw'_2$.

Sous-cas 1.2 : θ_i est la dernière lettre de w'_1 et on a $j = n + |w'_1| - 1 \leq i - 2$. Ce cas n'est pas possible car la lettre θ_i dans cette position contribuerait

pour $i + 1 + |w'_2| \geq n + |w'_1| + 1 + 1 + |w'_2| = 3n - 2$ au plafond de w' , qui est celui de Δ_n , à savoir $3n - 5$.

Sous-cas 1.3 : θ_i est $\theta_{n+|w'_1|-1}$ et θ_j est la première lettre de w'_2 , et on a $j \geq i + 3$. Ce cas est impossible comme le sous-cas 1.2.

Sous-cas 1.4 : θ_i est $\theta_{n+|w'_1|-1}$ et θ_j est la première lettre de w'_2 , et on a $j \leq i + 2$. Ce cas est analogue au sous-cas 1.1.

Cas 2 : (v', v) est une relation de type 3. Alors v' est un mot de longueur 3, soit du type $\theta_i\theta_{i+1}\theta_{i+3}$, soit du type $\theta_{i+1}\theta_i\theta_{i+1}$. Comme la lettre $\theta_{n+|w'_1|-1}$ apparaît dans v' comme première, deuxième, ou troisième lettre, il y a six cas possibles.

Sous-cas 2.1 : θ_i et θ_{i+1} sont les dernières lettres de w'_1 , et on a $i + 3 = n + |w'_1| - 1$, soit

$$(v', v) = (\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}\theta_{n+|w'_1|-1}, \theta_{n+|w'_1|-3}\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}).$$

En posant $w'_1 := w''_1\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}$, on obtient

$$\begin{aligned} w' &= w''_1\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}\theta_{n+|w'_1|-1}w'_2 \\ w &= w''_1\theta_{n+|w'_1|-3}\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}w'_2 = w''_1\theta_{n+|w'_1|-1}\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}w'_2. \end{aligned}$$

De plus, on a $w''_1\theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}w'_2 \equiv \underline{\Delta}_{n-0,5}$, d'où le résultat pour $w_1 := w''_1$ et $w_2 := \theta_{n+|w'_1|-4}\theta_{n+|w'_1|-3}w'_2$.

Sous-cas 2.2 : θ_i est la dernière lettre de w'_1 , on a $i + 1 = n + |w'_1| - 1$, et θ_{i+3} est la première lettre de w'_2 , soit

$$(v', v) = (\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}\theta_{n+|w'_1|+1}, \theta_{n+|w'_1|-1}\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}).$$

Ce cas n'est pas possible car $[w'] = 3n - 5$ alors que $\theta_{n+|w'_1|+1}$ contribuerait pour $n + |w'_1| + 1 + |w'_2| - 1 = n + 2n - 3 - 1 = 3n - 4$.

Sous-cas 2.3 : On a $i = n + |w'_1| - 1$, et θ_{i+1} et θ_{i+3} sont les premières lettres de w'_2 , soit

$$(v', v) = (\theta_{n+|w'_1|-1}\theta_{n+|w'_1|}\theta_{n+|w'_1|+2}, \theta_{n+|w'_1|}\theta_{n+|w'_1|-1}\theta_{n+|w'_1|}).$$

Ce cas est impossible comme 2.2.

Sous-cas 2.4 : θ_{i+1} et θ_i sont les dernières lettres de w'_1 et on a $i + 1 = n + |w'_1| - 1$, soit

$$(v', v) = (\theta_{n+|w'_1|-1}\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}, \theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}\theta_{n+|w'_1|+1})$$

avec $w'_1 = w''_1\theta_{n+|w'_1|-1}\theta_{n+|w'_1|-2}$. Ce cas n'est pas possible car $[w] = 3n - 5$ alors que $\theta_{n+|w'_1|+1}$ contribuerait pour $n + |w'_1| + 1 + |w'_2| = n + 2n - 3 = 3n - 3$.

Sous-cas 2.5 : θ_{i+1} est la dernière lettre de w'_1 , on a $i = n + |w'_1| - 1$, et θ_{i+1} est la première lettre de w'_2 , soit

$$(v', v) = (\theta_{n+|w'_1|}\theta_{n+|w'_1|-1}\theta_{n+|w'_1|}, \theta_{n+|w'_1|-1}\theta_{n+|w'_1|}\theta_{n+|w'_1|+2})$$

Ce cas est impossible comme 2.4.

Sous-cas 2.6 : On a $i + 1 = n + |w'_1| - 1$, et θ_i et θ_{i+1} sont les premières lettres de w'_2 , soit

$$(v', v) = (\theta_{n+|w'_1|-1}\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}, \theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}\theta_{n+|w'_1|+1})$$

avec $w'_2 = \theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}w''_2$. On obtient

$$\begin{aligned} w' &= w'_1\theta_{n+|w'_1|-1}\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}w''_2 \\ w &= w'_1\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}\theta_{n+|w'_1|+1}w''_2. \end{aligned}$$

De plus, on a $w'_1\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}w''_2 \equiv \underline{\Delta}_{n-0,5}$, d'où le résultat pour $w_1 := w'_1\theta_{n+|w'_1|-2}\theta_{n+|w'_1|-1}$ et $w_2 := w''_2$.

Ceci complète l'induction. Il reste à montrer $w_1\theta_{n+|w_1|-1} = \theta_{n-1}w_1$. On trouve, d'après (1.17),

$$w_1\theta_{n+|w_1|-1}w_2 \equiv \underline{\Delta}_n \equiv \theta_{n-1}\underline{\Delta}_{n-0,5} \equiv \theta_{n-1}w_1w_2.$$

En simplifiant à droite par w_2 , on a $w_1\theta_{n+|w_1|-1} \equiv \theta_{n-1}w_1$. \square

EXEMPLE 2.6. Considérons le mot $\theta_1\theta_2\theta_4\theta_5\theta_7$, qui est un représentant de Δ_4 . Ce que dit le lemme 2.4, c'est que tout représentant peut s'écrire $w_1\theta_{3+|w_1|}w_2$ avec $w_1w_2 \equiv \theta_1\theta_2\theta_4\theta_5$. Dans le cas présent, on trouve

$$\begin{aligned} \theta_1\theta_2\theta_4\theta_5\theta_7 &\equiv \theta_2\theta_1\theta_2\theta_5\theta_7 \equiv \theta_1\theta_2\theta_5\theta_4\theta_5 \equiv \theta_2\theta_1\theta_4\theta_2\theta_7 \equiv \theta_1\theta_4\theta_2\theta_4\theta_5 \\ &\equiv \theta_2\theta_3\theta_1\theta_2\theta_7 \equiv \theta_2\theta_1\theta_4\theta_6\theta_2 \equiv \theta_3\theta_1\theta_2\theta_4\theta_5 \equiv \theta_2\theta_3\theta_1\theta_6\theta_2 \\ &\equiv \theta_3\theta_2\theta_1\theta_2\theta_5 \equiv \theta_2\theta_3\theta_5\theta_1\theta_2 \equiv \theta_3\theta_2\theta_1\theta_4\theta_2 \equiv \theta_3\theta_2\theta_3\theta_1\theta_2. \end{aligned}$$

On voit en particulier qu'aucune expression de Δ_4 ne finit par $\theta_1\theta_2\theta_4$ ni $\theta_2\theta_1\theta_2$, ce qui démontre que Δ_3 ne divise pas Δ_4 .

On peut donc séparer les diviseurs de Δ_n en deux catégories, ceux qui ne possèdent pas la lettre θ_{n+k-1} dans leurs écritures et ceux qui la possèdent. Dans ce dernier cas, on va montrer que θ_{n-1} est diviseur à gauche.

LEMME 2.7. *Pour $n \geq 3$, tous les diviseurs à gauche de Δ_n soit sont des diviseurs à gauche de $\Delta_{n-0,5}$, soit sont de la forme $a\theta_{n+|a|-1}b$ avec $ab \preccurlyeq \Delta_{n-0,5}$, auquel cas on a $a\theta_{n+|a|-1} = \theta_{n-1}a$.*

DÉMONSTRATION. Si on a $[w] \preccurlyeq \Delta_n$, il existe w' tel que ww' est une écriture de Δ_n , donc, par (2.5), ww' s'écrit $w_1\theta_{n+|w_1|-1}w_2$ avec $w_1w_2 \equiv \underline{\Delta}_{n-0,5}$: ou bien w est un préfixe de w_1 , et on a donc $[w] \preccurlyeq \Delta_{n-0,5}$, ou bien w est de la forme $w_1\theta_{n+|w_1|-1}w'_2$ avec w'_2 préfixe de w_2 , et on a donc $[w] = [w_1]\theta_{n+|w_1|-1}[w'_2]$ avec $[w_1][w'_2] = [w_1w'_2] \preccurlyeq \Delta_{n-0,5}$. De plus, $w_1\theta_{n+|w_1|-1} \equiv \theta_{n-1}w_1$ implique $[w_1]\theta_{n+|w_1|-1} \equiv \theta_{n-1}[w_1]$. \square

Pour $n \geq 4$, les éléments de l'ensemble $\Sigma_{n,\ell}^{\text{II}}$ ont été définis comme de la forme $\theta_{n-2}\theta_{n-1}a$ avec $a \in \Sigma_{n-1,\ell-2}$ et $a \preccurlyeq \Delta_{n-1,5}$. En fait, les éléments a ainsi définis sont les éléments de $\Sigma_{n-1,\ell-2}$ qui vérifient $\theta_{n-2} \not\preccurlyeq a$. La démonstration est facile à partir du lemme 2.7.

LEMME 2.8. *Pour $n \geq 3$ et $a \preccurlyeq \Delta_n$, les conditions $a \preccurlyeq \Delta_{n-0,5}$ et $\theta_{n-1} \not\preccurlyeq a$ sont équivalents.*

DÉMONSTRATION. Supposons $a \preccurlyeq \Delta_{n-0,5}$. Alors, par la proposition 1.25, les diviseurs de taille 1 de $\Delta_{n-0,5}$ sont $\{\theta_1, \dots, \theta_{n-2}\}$. Donc l'atome θ_{n-1} ne divise pas à gauche $\Delta_{n-0,5}$, a fortiori, θ_{n-1} ne divise pas à gauche a .

Maintenant, on suppose $\theta_{n-1} \not\preccurlyeq a$. Comme a divise à gauche Δ_n , le lemme 2.7 montre qu'il y a deux possibilités :

- soit a est un diviseur à gauche de $\Delta_{n-0,5}$, ce qui est le résultat escompté ;
- soit a est de la forme $b\theta_{n+|b|-1}c$ avec $bc \preccurlyeq \Delta_{n-0,5}$; dans ce cas, on trouve $b\theta_{n+|b|-1} = \theta_{n-1}b$, d'où $\theta_{n-1} \preccurlyeq a$, qui contredit l'hypothèse $\theta_{n-1} \not\preccurlyeq a$. La seule possibilité est donc $a \preccurlyeq \Delta_{n-0,5}$. \square

On considère maintenant les éléments de $\Sigma_{n,\ell}^{\text{III}}$.

LEMME 2.9. *Pour $n \geq 4$, si $\theta_{n-1}\theta_{n-2}\theta_{n-1}a$ appartient à $\Sigma_{n,\ell}^{\text{III}}$, alors on a $a \preccurlyeq \underline{\Delta}_{n-1,5}$.*

DÉMONSTRATION. Par définition de l'ensemble $\Sigma_{n,\ell}^{\text{III}}$, on a $\theta_{n-2}a \preccurlyeq \Delta_{n-1}$. Donc, par (1.17), on a $\theta_{n-2}a \preccurlyeq \Delta_{n-1} = \theta_{n-2}\Delta_{n-1,5}$, d'où, en simplifiant à gauche, $a \preccurlyeq \Delta_{n-1,5}$. \square

Dans le lemme 2.4, on s'intéresse aux décompositions de Δ_n . Pour la suite, on a aussi besoin de trouver une forme générale pour les représentants des éléments de la forme $\underline{\Delta}_{n-0,5}$, qui est aussi $\Delta_{n-1,5}\theta_{3n-8}\theta_{3n-7}$. Dans ce cas, on va montrer qu'on peut pousser vers la gauche les deux lettres θ_{3n-8} et θ_{3n-7} . La démonstration est similaire à celle du lemme 2.4, mais, comme on déplace deux lettres, il y a davantage de cas à traiter.

LEMME 2.10. *Pour $n \geq 4$, tout représentant de $\Delta_{n-0,5}$ est de la forme*

$$(2.11) \quad w_1\theta_{n-2+|w_1|}w_2\theta_{n-1+|w_1w_2|}w_3$$

avec $w_1w_2w_3 \equiv \underline{\Delta}_{n-1,5}$; de plus, dans ce cas, le mot $w_1\theta_{n-2+|w_1|}w_2w_3$ représente Δ_{n-1} .

DÉMONSTRATION. Soit w vérifiant $w \equiv \underline{\Delta}_{n-0,5}$. On montre le résultat par récurrence sur la distance combinatoire p entre $\underline{\Delta}_{n-0,5}$ et w .

Pour $p = 0$, on a

$$w = \underline{\Delta}_{n-0,5} = \underline{\Delta}_{n-1,5}\theta_{3n-8}\theta_{3n-7},$$

qui donne (2.11) en posant $w_1 := \underline{\Delta}_{n-1,5}$ et $w_2 := w_3 := \varepsilon$.

Supposons $p \geq 1$. Alors il existe w' vérifiant

$$\text{dist}(\underline{\Delta}_{n-0,5}, w') = p - 1 \quad \text{et} \quad \text{dist}(w', w) = 1.$$

On écrit $w' = u_1v'u_2$ et $w = u_1vu_2$ avec (v', v) relation de (\mathcal{P}) . Par hypothèse de récurrence appliquée à w' , il existe trois mots w'_1, w'_2 et w'_3 vérifiant

$$w' = w'_1\theta_{n-2+|w'_1|}w'_2\theta_{n-1+|w'_1w'_2|}w'_3, \quad \text{avec} \quad w'_1w'_2w'_3 \equiv \underline{\Delta}_{n-1,5}.$$

On a plusieurs cas à traiter selon que les lettres $\theta_{n-2+|w'_1|}$ et $\theta_{n-1+|w'_1w'_2|}$ appartiennent ou non au facteur v' .

(i) On suppose d'abord qu'aucune des deux lettres n'appartient à v' .

Cas 1 : u_1v' est un préfixe de w'_1 , c'est-à-dire il existe u'_1 vérifiant $w'_1 = u_1v'u'_1$. On trouve alors

$$\begin{aligned} w' &= u_1v'u'_1\theta_{n-2+|w'_1|}w'_2\theta_{n-1+|w'_1w'_2|}w'_3 \\ w &= u_1vu'_1\theta_{n-2+|w'_1|}w'_2\theta_{n-1+|w'_1w'_2|}w'_3. \end{aligned}$$

Or, on a $u_1vu'_1w'_2w'_3 \equiv u_1v'u'_1w'_2w'_3 = w'_1w'_2w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := u_1vu'_1$, $w_2 := w'_2$ et $w_3 := w'_3$.

Cas 2 : $v'u_2$ est un suffixe de w'_3 . Le raisonnement est analogue au cas 1.

Cas 3 : v' est un facteur de w'_2 , c'est-à-dire il existe u''_2 et u'''_2 vérifiant $w'_2 = u''_2v'u'''_2$. On trouve alors

$$\begin{aligned} w' &= w'_1\theta_{n-2+|w'_1|}u''_2v'u'''_2\theta_{n-1+|w'_1w'_2|}w'_3, \\ w &= w'_1\theta_{n-2+|w'_1|}u''_2vu'''_2\theta_{n-1+|w'_1w'_2|}w'_3. \end{aligned}$$

Or, on a $w'_1u''_2vu'''_2w'_3 \equiv w'_1u''_2v'u'''_2w'_3 = w'_1w'_2w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := w'_1$, $w_2 := u''_2vu'''_2$ et $w_3 := w'_3$.

(ii) On suppose maintenant que seule la lettre $\theta_{n-2+|w'_1|}$ apparaît dans v' .

Cas 1 : (v', v) est une relation de type 2. Alors v' est un mot de longueur 2, soit du type $\theta_i\theta_j$ avec $j \geq i + 3$, soit du type $\theta_i\theta_j$ avec $j \leq i - 2$. Comme la lettre $\theta_{n-2+|w'_1|}$ apparaît dans v' soit comme première, soit comme seconde lettre, il y a quatre sous-cas possibles.

Sous-cas 1.1 : θ_i est la dernière lettre de w'_1 et on a $j = n - 2 + |w'_1| \geq i + 3$. On pose $w'_1 = w''_1\theta_i$. On obtient

$$w' = w''_1\theta_i\theta_{n-2+|w'_1|}w'_2\theta_{n-1+|w'_1w'_2|}w'_3 \text{ et } w = w''_1\theta_{n-3+|w'_1|}\theta_iw'_2\theta_{n-1+|w'_1w'_2|}w'_3.$$

De plus, on a $w''_1\theta_iw'_2w'_3 = w'_1w'_2w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := w''_1$, $w_2 := \theta_iw'_2$ et $w_3 := w'_3$.

Sous-cas 1.2 : θ_i est la dernière lettre de w'_1 et on a $j = n - 2 + |w'_1| \leq i - 2$. Ce cas n'est pas possible car la lettre θ_i dans cette position contribuerait pour $i + 1 + |w'_2| + 1 + |w'_3| \geq n + |w'_1| + 1 + |w'_2| + 1 + |w'_3| = 3n - 4$ au plafond de w' , qui est celui de $\underline{\Delta}_{n-0,5}$, à savoir $3n - 7$.

Sous-cas 1.3 : θ_i est $\theta_{n-2+|w'_1|}$ et θ_j est la première lettre de w'_2 et on a $j \geq i + 3$. Ce cas est impossible comme 1.2.

Sous-cas 1.4 : θ_i est $\theta_{n-2+|w'_1|}$ et θ_j est la première lettre de w'_2 et on a $j \leq i + 2$. Ce cas est analogue au sous-cas 1.1.

Cas 2 : (v', v) est une relation de type 3. Alors v' est un mot de longueur 3, soit du type $\theta_i\theta_{i+1}\theta_{i+3}$, soit du type $\theta_{i+1}\theta_i\theta_{i+1}$. Comme la lettre $\theta_{n-2+|w'_1|}$ apparaît dans v' comme première, deuxième, ou troisième lettre, il y a six sous-cas possibles.

Sous-cas 2.1 : θ_i et θ_{i+1} sont les dernières lettres de w'_1 et on a $i + 3 = n - 2 + |w'_1|$, soit

$$(v', v) = (\theta_{n-5+|w'_1|}\theta_{n-4+|w'_1|}\theta_{n-2+|w'_1|}, \theta_{n-4+|w'_1|}\theta_{n-5+|w'_1|}\theta_{n-4+|w'_1|}).$$

On pose $w'_1 := w''_1 \theta_{n-5+|w'_1|} \theta_{n-4+|w'_1|}$. On obtient

$$\begin{aligned} w' &= w''_1 \theta_{n-5+|w'_1|} \theta_{n-4+|w'_1|} \theta_{n-2+|w'_1|} w'_2 \theta_{n-1+|w'_1 w'_2|} w'_3, \\ w &= w''_1 \theta_{n-4+|w'_1|} \theta_{n-5+|w'_1|} \theta_{n-4+|w'_1|} w'_2 \theta_{n-1+|w'_1 w'_2|} w'_3 \\ &= w''_1 \theta_{n-2+|w'_1|} \theta_{n-5+|w'_1|} \theta_{n-4+|w'_1|} w'_2 \theta_{n-1+|w'_1 w'_2|} w'_3. \end{aligned}$$

De plus, on a $w''_1 \theta_{n-5+|w'_1|} \theta_{n-4+|w'_1|} w'_2 w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := w''_1$, $w_2 := \theta_{n-5+|w'_1|} \theta_{n-4+|w'_1|} w'_2$ et $w_3 := w'_3$.

Sous-cas 2.2 : θ_i est la dernière lettre de w'_1 , on a $i+1 = n-2+|w'_1|$, et θ_{i+3} est la première lettre de w'_2 , soit

$$(v', v) = (\theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n+|w'_1|}, \theta_{n-2+|w'_1|} \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|}).$$

Ce cas n'est pas possible car $\lceil w' \rceil = 3n-7$, alors que $\theta_{n+|w'_1|}$ contribuerait pour $n+|w'_1|-1+|w'_2|+1+|w'_3| = n+2n-6 = 3n-6$.

Sous-cas 2.3 : On a $i = n-2+|w'_1|$, et θ_{i+1} et θ_{i+3} sont les premières lettres de w'_2 , soit

$$(v', v) = (\theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|} \theta_{n+1+|w'_1|}, \theta_{n-1+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|}).$$

Ce cas est impossible comme 2.2.

Sous-cas 2.4 : θ_{i+1} et θ_i sont les dernières lettres de w'_1 et on a $i+1 = n-2+|w'_1|$, soit

$$(v', v) = (\theta_{n-2+|w'_1|} \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|}, \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n+|w'_1|})$$

avec $w'_1 = w''_1 \theta_{n-2+|w'_1|} \theta_{n-3+|w'_1|}$. Ce cas n'est pas possible car $\lceil w \rceil$ est $3n-7$, alors que $\theta_{n+|w'_1|}$ contribuerait pour

$$n+|w'_1|+|w'_2|+1+|w'_3| = n+2n-5 = 3n-5.$$

Sous-cas 2.5 : θ_{i+1} est la dernière lettre de w'_1 , on a $i = n-2+|w'_1|$, et θ_{i+1} est la première lettre de w'_2 , soit

$$(v', v) = (\theta_{n-1+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|}, \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|} \theta_{n+1+|w'_1|})$$

Ce cas est impossible comme 2.4.

Sous-cas 2.6 : On a $i+1 = n-2+|w'_1|$, et θ_i et θ_{i+1} sont les premières lettres de w'_2 , soit

$$(v', v) = (\theta_{n-2+|w'_1|} \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|}, \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n+|w'_1|})$$

avec $w'_2 = \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} w''_2$. On obtient

$$\begin{aligned} w' &= w'_1 \theta_{n-2+|w'_1|} \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} w''_2 \theta_{n-1+|w'_1 w'_2|} w'_3, \\ w &= w'_1 \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n+|w'_1|} w''_2 \theta_{n-1+|w'_1 w'_2|} w'_3. \end{aligned}$$

De plus, on a $w'_1 \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|} w''_2 w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := w'_1 \theta_{n-3+|w'_1|} \theta_{n-2+|w'_1|}$, $w_2 := w''_2$ et $w_3 := w'_3$.

(iii) On suppose maintenant que seule la lettre $\theta_{n-1+|w'_1 w'_2|}$ apparaît dans v' .

Cas 1 : (v', v) est une relation de type 2. Il y a encore quatre cas possibles.

Sous-cas 1.1 : θ_i est la dernière lettre de w'_2 et on a $j = n - 1 + |w'_1 w'_2| \geq i + 3$. On pose $w'_2 = w''_2 \theta_i$. On obtient

$$\begin{aligned} w' &= w'_1 \theta_{n-2+|w'_1|} w''_2 \theta_i \theta_{n-1+|w'_1 w'_2|} w'_3 \\ w &= w'_1 \theta_{n-2+|w'_1|} w''_2 \theta_{n-2+|w'_1 w'_2|} \theta_i w'_3. \end{aligned}$$

De plus, on a $w'_1 w''_2 \theta_i w'_3 = w'_1 w'_2 w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := w'_1$, $w_2 := w''_2$ et $w_3 := \theta_i w'_3$.

Sous-cas 1.2 : θ_i est la dernière lettre de w'_2 et on a $j = n - 1 + |w'_1 w'_2| \leq i - 2$. Ce cas n'est pas possible car $\lceil w' \rceil = 3n - 7$, alors que θ_i contribuerait au plafond pour $i + 1 + |w'_3| \geq n + 1 + |w'_1 w'_2| + 1 + |w'_3| = 3n - 4$.

Sous-cas 1.3 : θ_i est $\theta_{n-1+|w'_1 w'_2|}$ et θ_j est la première lettre de w'_3 et on a $j \geq i + 3$. Ce cas est impossible comme le sous-cas 1.2.

Sous-cas 1.4 : θ_i est $\theta_{n-1+|w'_1 w'_2|}$ et θ_j est la première lettre de w'_3 et on a $j \leq i + 2$. Ce cas est analogue au sous-cas 1.1.

Cas 2 : (v', v) est une relation de type 3. Il y a encore six cas possibles.

Sous-cas 2.1 : θ_i et θ_{i+1} sont les dernières lettres de w'_2 et on a $i + 3 = n - 1 + |w'_1 w'_2|$, soit

$$(v', v) = (\theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|}, \theta_{n-3+|w'_1 w'_2|} \theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|}).$$

On pose $w'_2 := w''_2 \theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|}$. On obtient

$$\begin{aligned} w' &= w'_1 \theta_{n-2+|w'_1|} w''_2 \theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} w'_3, \\ w &= w'_1 \theta_{n-2+|w'_1|} w''_2 \theta_{n-3+|w'_1 w'_2|} \theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|} w'_3, \end{aligned}$$

De plus, on a $w'_1 w''_2 \theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|} w'_3 \equiv \underline{\Delta}_{n-1,5}$, d'où (2.11) en posant $w_1 := w'_1$, $w_2 := w''_2$ et $w_3 := \theta_{n-4+|w'_1 w'_2|} \theta_{n-3+|w'_1 w'_2|} w'_3$.

Sous-cas 2.2 : θ_i est la dernière lettre de w'_2 , on a $i + 1 = n - 1 + |w'_1 w'_2|$, et θ_{i+3} est la première lettre de w'_3 , soit

$$(v', v) = (\theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} \theta_{n+1+|w'_1 w'_2|}, \theta_{n-1+|w'_1 w'_2|} \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|}).$$

Ce cas n'est pas possible car $\lceil w' \rceil = 3n - 7$ alors que $\theta_{n+1+|w'_1 w'_2|}$ contribuerait pour $n + 1 + |w'_1 w'_2| - 1 + |w'_3| = n + 2n - 6 = 3n - 6$.

Sous-cas 2.3 : On a $i = n - 1 + |w'_1 w'_2|$, et θ_{i+1} et θ_{i+3} sont les premières lettres de w'_3 , soit

$$(v', v) = (\theta_{n-1+|w'_1 w'_2|} \theta_{n+|w'_1 w'_2|} \theta_{n+2+|w'_1 w'_2|}, \theta_{n+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} \theta_{n+|w'_1 w'_2|}).$$

Ce cas est impossible comme 2.2.

Sous-cas 2.4 : θ_{i+1} et θ_i sont les dernières lettres de w'_2 et on a $i + 1 = n - 1 + |w'_1 w'_2|$, soit

$$(v', v) = (\theta_{n-1+|w'_1 w'_2|} \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|}, \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} \theta_{n+1+|w'_1 w'_2|}).$$

avec $w'_2 = w''_2 \theta_{n-1+|w'_1 w'_2|} \theta_{n-2+|w'_1 w'_2|}$. Ce cas n'est pas possible car $\lceil w \rceil = 3n - 7$ alors que $\theta_{n+1+|w'_1 w'_2|}$ contribuerait pour $n + 1 + |w'_1 w'_2| + |w'_3| = n + 2n - 5 = 3n - 5$.

Sous-cas 2.5 : θ_{i+1} est la dernière lettre de w'_2 , on a $i = n - 1 + |w'_1 w'_2|$, et θ_{i+1} est la première lettre de w'_3 , soit

$$(v', v) = (\theta_{n+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} \theta_{n+|w'_1 w'_2|}, \theta_{n-1+|w'_1 w'_2|} \theta_{n+|w'_1 w'_2|} \theta_{n+2+|w'_1 w'_2|}).$$

Ce cas est impossible comme 2.4.

Sous-cas 2.6 : On a $i+1 = n - 1 + |w'_1 w'_2|$, et θ_i et θ_{i+1} sont les premières lettres de w'_3 , soit

$$(v', v) = (\theta_{n-1+|w'_1 w'_2|} \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|}, \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} \theta_{n+1+|w'_1 w'_2|}).$$

avec $w'_3 = \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} w''_3$. On obtient

$$\begin{aligned} w' &= w'_1 \theta_{n-2+|w'_1|} w'_2 \theta_{n-1+|w'_1 w'_2|} \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} w''_3, \\ w &= w'_1 \theta_{n-2+|w'_1|} w'_2 \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} \theta_{n+1+|w'_1 w'_2|} w''_3. \end{aligned}$$

De plus, on a $w'_1 w'_2 \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|} w''_3 \equiv \Delta_{n-1,5}$, d'où (2.11) en posant $w_1 := w'_1$, $w_2 := w'_2 \theta_{n-2+|w'_1 w'_2|} \theta_{n-1+|w'_1 w'_2|}$ et $w_3 := w''_3$.

(iv) Pour finir, on suppose que les deux lettres $\theta_{n-2+|w'_1|}$ et $\theta_{n-1+|w'_1 w'_2|}$ apparaissent dans v' . *A priori*, cette situation est la plus compliquée, mais, en fait, il n'y a que peu de possibilités valides.

Cas 1 : (v', v) est une relation de type 2. Alors v' est un mot de longueur 2 et la seule possibilité est

$$|w'_2| = 0 \quad \text{et} \quad v' = \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1 w'_2|} = \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|}.$$

Or ceci est impossible car on a pas de relation $u = v$ avec u de la forme $\theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|}$ dans la présentation (\mathcal{P}) .

Cas 2 : (v', v) est une relation de type 3. Alors v' est un mot de longueur 3, soit du type $\theta_i \theta_{i+1} \theta_{i+3}$, soit du type $\theta_{i+1} \theta_i \theta_{i+1}$. Comme les deux lettres $\theta_{n-2+|w'_1|}$ et $\theta_{n-1+|w'_1 w'_2|}$ apparaissent dans v' , il y a seulement deux cas possibles.

Sous-cas 2.1 : $|w'_2| = 0$, $i = n - 2 + |w'_1|$, $i + 1 = n - 1 + |w'_1|$ et θ_{i+3} est la première lettre de w'_3 , soit

$$(v', v) = (\theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|} \theta_{n+1+|w'_1|}, \theta_{n-1+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|}).$$

Ce cas n'est pas possible, car on a $\lceil w' \rceil = 3n - 7$, alors que $\theta_{n+1+|w'_1|}$ contribuerait pour $n + 1 + |w'_1| + |w'_3| - 1 = 3n - 6$.

Sous-cas 2.2 : $|w'_2| = 0$, θ_{i+1} est la dernière lettre de w'_1 , $i = n - 2 + |w'_1|$ et $i + 1 = n - 1 + |w'_1|$, soit

$$(v', v) = (\theta_{n-1+|w'_1|} \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|}, \theta_{n-2+|w'_1|} \theta_{n-1+|w'_1|} \theta_{n+1+|w'_1|}).$$

Ce cas n'est pas possible, car on a $\lceil w \rceil = 3n - 7$ alors que $\theta_{n+1+|w'_1|}$ contribuerait pour $n + 1 + |w'_1| + |w'_3| = 3n - 5$.

Ceci complète l'induction : on a ainsi montré que tout représentant de $\Delta_{n-0,5}$ est de la forme (2.11) avec $w_1 w_2 w_3 \equiv \underline{\Delta}_{n-1,5}$, et il reste à montrer qu'on a alors

$$(2.12) \quad w_1 \theta_{n-2+|w_1|} w_2 w_3 \equiv \underline{\Delta}_{n-1}.$$

Montrons (2.12) par récurrence sur $|w_3|$. Pour $|w_3| = 0$, on a par hypothèse $w_1 w_2 \equiv \underline{\Delta}_{n-1,5}$, d'où $|w_1 w_2| = 2n - 6$, et on trouve

$$\begin{aligned} \underline{\Delta}_{n-0,5} &\equiv w_1 \theta_{n-2+|w_1|} w_2 \theta_{n-1+|w_1 w_2|} w_3 \\ &\equiv w_1 \theta_{n-2+|w_1|} w_2 \theta_{3n-7}, \end{aligned}$$

donc (2.12) en simplifiant θ_{3n-7} à droite.

Supposons maintenant $|w_3| \geq 1$. On pose $w_3 = \theta_i w'_3$. Par hypothèse, on a $w_1 w_2 \theta_i w'_3 \equiv \underline{\Delta}_{n-1,5}$. Donc le plafond de $w_1 w_2 \theta_i w'_3$ est $3n - 10$ et, par le lemme 1.26, on a

$$i \leq 3n - 10 - |w'_3| = 3n - 10 - (|w_3| - 1) = 3n - 9 - |w_3|.$$

Maintenant, par (2.11), on a

$$\begin{aligned} w_1 \theta_{n-2+|w_1|} w_2 \theta_{n-1+|w_1 w_2|} \theta_i w'_3 &= w_1 \theta_{n-2+|w_1|} w_2 \theta_{3n-7-|w_3|} \theta_i w'_3 \\ &\equiv w_1 \theta_{n-2+|w_1|} w_2 \theta_i \theta_{3n-6-|w_3|} w'_3 \\ &= w_1 \theta_{n-2+|w_1|} w_2 \theta_i \theta_{n-1+|w_1 w_2 \theta_i|} w'_3. \end{aligned}$$

On pose $w'_1 := w_1$ et $w'_2 := w_2 \theta_i$. On obtient alors

$$w'_1 \theta_{n-2+|w'_1|} w'_2 \theta_{n-1+|w'_1 w'_2|} w'_3 \equiv \underline{\Delta}_{n-0,5},$$

avec $w'_1 w'_2 w'_3 \equiv \underline{\Delta}_{n-1,5}$ et on a $|w'_3| < |w_3|$. Par hypothèse de récurrence, on trouve $\underline{\Delta}_{n-1} \equiv w'_1 \theta_{n-2+|w'_1|} w'_2 w'_3$, d'où $\underline{\Delta}_{n-1} \equiv w_1 \theta_{n-2+|w_1|} w_2 w_3$ puisque les mots $w'_1 \theta_{n-2+|w'_1|} w'_2 w'_3$ et $w_1 \theta_{n-2+|w_1|} w_2 w_3$ coïncident. \square

Le lemme 2.10 permet de répartir les diviseurs de $\Delta_{n-0,5}$ en deux sous-ensembles. Ce point sera crucial dans la dernière étape de la partition des diviseurs de Δ_n (sous-section 2.2).

LEMME 2.13. *Pour $n \geq 4$, les diviseurs à gauche de $\Delta_{n-0,5}$ soit sont des diviseurs à gauche de Δ_{n-1} , soit sont de la forme $\theta_{n-2} \theta_{n-1} a$ avec $a \preceq \underline{\Delta}_{n-1,5}$.*

DÉMONSTRATION. Supposons que $[w]$ divise à gauche $\Delta_{n-0,5}$. Il existe donc un Θ -mot w' tel que ww' représente $\Delta_{n-0,5}$. Par le lemme 2.10, le mot ww' est de la forme $w_1 \theta_{n-2+|w_1|} w_2 \theta_{n-1+|w_1 w_2|} w_3$ avec $w_1 w_2 w_3 \equiv \underline{\Delta}_{n-1,5}$. On a donc trois possibilités.

- Ou bien w est un préfixe de w_1 . On a donc $[w] \preceq \underline{\Delta}_{n-1,5}$ et, par transitivité de \preceq , $[w]$ est un diviseur à gauche de Δ_{n-1} .

- Ou bien w est de la forme $w_1 \theta_{n-2+|w_1|} w'_2$ avec w'_2 un préfixe de w_2 . Par le lemme 2.10, $[w]$ est un diviseur à gauche de Δ_{n-1} ,

- Ou bien w est de la forme $w_1 \theta_{n-2+|w_1|} w_2 \theta_{n-1+|w_1 w_2|} w'_3$, avec w'_3 préfixe de w_3 . En posant $w_3 = w'_3 w''_3$, on trouve alors

$$w_1 \theta_{n-2+|w_1|} w_2 \theta_{n-1+|w_1 w_2|} w'_3 w''_3 \equiv \underline{\Delta}_{n-0,5}$$

$$\begin{aligned}
&= \underline{\Delta}_{n-2}\theta_{3n-10}\theta_{3n-8}\theta_{3n-7} \\
&\equiv \theta_{n-2}\underline{\Delta}_{n-2}\theta_{3n-10}\theta_{3n-7} \\
&\equiv \theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-2}\theta_{3n-10} \\
&\equiv \theta_{n-2}\theta_{n-1}w_1w_2w'_3w''_3.
\end{aligned}$$

En simplifiant w''_3 à droite, on déduit $w \equiv \theta_{n-2}\theta_{n-1}w_1w_2w'_3$, avec w_1, w_2, w'_3 vérifiant $[w_1w_2w'_3] \preccurlyeq \underline{\Delta}_{n-1,5}$. \square

2.2. Le résultat de partition. En utilisant les lemmes préparatoires de la section 2.1, on va montrer que (i) les ensembles $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}$, et $\Sigma_{n,\ell}^{III}$ de la définition 2.2 sont inclus dans $\Sigma_{n,\ell}$, (ii) ils sont disjoints deux à deux, et (iii) ils recouvrent $\Sigma_{n,\ell}$.

Le point (i) est facile, puisqu'il s'agit simplement de trouver des décompositions de Δ_n commençant par des préfixes donnés.

LEMME 2.14. *Pour $n \geq 4$ et $2 \leq \ell \leq 2n-3$, les ensembles $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}$ et $\Sigma_{n,\ell}^{III}$ sont inclus dans $\Sigma_{n,\ell}$.*

DÉMONSTRATION. Tous les diviseurs à gauche de longueur ℓ de Δ_{n-1} sont des diviseurs à gauche de Δ_n par transitivité de \preccurlyeq , donc $\Sigma_{n,\ell}^0$ est inclus dans $\Sigma_{n,\ell}$.

Considérons maintenant un élément de $\Sigma_{n,\ell}^I$, soit $\theta_{n-1}a$ avec $a \preccurlyeq \Delta_{n-1}$. *A fortiori*, on a $\theta_{n-1}a \preccurlyeq \theta_{n-1}\Delta_{n-1}$. Par (1.17), on a $\Delta_n = \theta_{n-1}\Delta_{n-1}\theta_{3n-7}$, donc $\theta_{n-1}\Delta_{n-1} \preccurlyeq \Delta_n$. Par transitivité de \preccurlyeq , on déduit $\theta_{n-1}a \preccurlyeq \Delta_n$.

Ensuite, considérons un élément $\theta_{n-2}\theta_{n-1}a$ de $\Sigma_{n,\ell}^{II}$, avec $a \preccurlyeq \Delta_{n-1,5}$. Un calcul direct donne

$$\begin{aligned}
\Delta_n &= \Delta_{n-0,5}\theta_{3n-5} = \theta_{n-2}\underline{\Delta}_{n-1,5}\theta_{3n-7}\theta_{3n-5} \\
&= \theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-1,5}\theta_{3n-5},
\end{aligned}$$

donc $a \preccurlyeq \Delta_{n-1,5}$ implique $\theta_{n-2}\theta_{n-1}a \preccurlyeq \theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-1,5} \preccurlyeq \Delta_n$, et, de là, $\theta_{n-2}\theta_{n-1}a \preccurlyeq \Delta_n$ par transitivité de \preccurlyeq .

Enfin, considérons un élément $\theta_{n-1}\theta_{n-2}\theta_{n-1}a$ de $\Sigma_{n,\ell}^{III}$, avec $\theta_{n-2}a \preccurlyeq \Delta_{n-1}$. On trouve

$$\begin{aligned}
\Delta_n &= \underline{\Delta}_{n-1,5}\theta_{3n-8}\theta_{3n-7}\theta_{3n-5} = \underline{\Delta}_{n-1,5}\theta_{3n-7}\theta_{3n-8}\theta_{3n-7} \\
&= \theta_{n-1}\underline{\Delta}_{n-1,5}\theta_{3n-8}\theta_{3n-7} \\
&= \theta_{n-1}\theta_{n-2}\underline{\Delta}_{n-1,5}\theta_{3n-7} \\
&= \theta_{n-1}\theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-1,5}.
\end{aligned}$$

Or, par le lemme 2.9, on a $a \preccurlyeq \underline{\Delta}_{n-1,5}$, d'où

$$\theta_{n-1}\theta_{n-2}\theta_{n-1}a \preccurlyeq \theta_{n-1}\theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-1,5} = \Delta_n,$$

d'où $\theta_{n-1}\theta_{n-2}\theta_{n-1}a \preccurlyeq \Delta_n$. \square

La seconde étape, le caractère disjoint deux à deux des ensembles $\Sigma_{n,\ell}^0$ à $\Sigma_{n,\ell}^{III}$, exige plus de cas et est un peu moins facile, puisqu'il s'agit de montrer

des résultats de non-divisibilité, ce qui ne peut se faire qu'en utilisant le retournement à droite de représentants.

LEMME 2.15. *Pour $n \geq 4$ et $2 \leq \ell \leq 2n-3$, les ensembles $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}$ et $\Sigma_{n,\ell}^{III}$ sont deux à deux disjoints.*

DÉMONSTRATION. Pour prouver que $\Sigma_{n,\ell}^0$ est disjoint de $\Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}$ et $\Sigma_{n,\ell}^{III}$, on montre que les éléments de $\Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}$, et $\Sigma_{n,\ell}^{III}$ sont tous d'indice n , c'est-à-dire ne divisent pas Δ_{n-1} à gauche. Soit $\theta_{n-1}a$ un élément de $\Sigma_{n,\ell}^I$ et $\theta_{n-1}\theta_{n-2}\theta_{n-1}b$ un élément de $\Sigma_{n,\ell}^{III}$. La proposition 1.25 implique que θ_{n-1} ne divise pas Δ_{n-1} à gauche, donc $\theta_{n-1}a$ et $\theta_{n-1}\theta_{n-2}\theta_{n-1}b$ ne peuvent pas diviser Δ_{n-1} à gauche. Donc $\Sigma_{n,\ell}^0$ est disjoint de $\Sigma_{n,\ell}^I$ et de $\Sigma_{n,\ell}^{III}$.

Soit maintenant $\theta_{n-2}\theta_{n-1}a$ un élément de $\Sigma_{n,\ell}^{II}$. On va montrer, en utilisant le retournement à droite, la relation $\theta_{n-2}\theta_{n-1}a \not\leq \Delta_{n-1}$ à gauche, d'où, *a fortiori*, $\theta_{n-2}\theta_{n-1}a \not\leq \Delta_{n-1}$. On trouve

$$\begin{aligned} \overline{\theta_{n-1}\theta_{n-2}\Delta_{n-1}} &= \overline{\theta_{n-1}\theta_{n-2}\theta_1\theta_2 \cdots \theta_{3n-10}\theta_{3n-8}} \\ &\curvearrowright \overline{\theta_{n-1}\theta_1\theta_2 \cdots \theta_{3n-10}\theta_{3n-8}\theta_{3n-8}} \\ &\curvearrowright \overline{\theta_{n-1}\theta_1\theta_2 \cdots \theta_{3n-10}} \\ &\curvearrowright \theta_1\theta_2 \cdots \theta_{3n-10}\overline{\theta_{3n-7}} : \end{aligned}$$

le mot terminal n'est pas un mot positif, donc on a $\theta_{n-2}\theta_{n-1}a \not\leq \Delta_{n-1}$. Par conséquent, $\Sigma_{\ell,n}^0$ est disjoint de $\Sigma_{\ell,n}^{II}$.

Ensuite, supposons $a \in \Sigma_{n,\ell}^I \cap \Sigma_{n,\ell}^{II}$. Alors, on a à la fois $a = \theta_{n-1}b$ avec b dans $\Sigma_{n-1,\ell-1}$ et $a = \theta_{n-2}\theta_{n-1}c$ avec c dans $\Sigma_{n-1,\ell-2}$ vérifiant $c \leq \underline{\Delta}_{n-1,5}$. On a donc

$$(2.16) \quad \theta_{n-1} \leq \theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-1,5}.$$

Cependant, on trouve

$$\begin{aligned} \overline{\theta_{n-1}\theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-2}\theta_{3n-10}} &\curvearrowright \theta_{n-2}\theta_{n-1}\overline{\theta_{n+1}\theta_{n-1}\theta_{n-1}\underline{\Delta}_{n-2}\theta_{3n-10}} \\ &\curvearrowright \theta_{n-2}\theta_{n-1}\overline{\theta_{n+1}\underline{\Delta}_{n-2}\theta_{3n-10}} \\ &\curvearrowright \theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-2}\theta_{3n-10}\overline{\theta_{3n-5}}, \end{aligned}$$

d'où $\theta_{n-1} \not\leq \theta_{n-2}\theta_{n-1}\underline{\Delta}_{n-1,5}$, contredisant (2.16). Donc $\Sigma_{n,\ell}^I$ et $\Sigma_{n,\ell}^{II}$ sont disjoints.

Supposons ensuite $a \in \Sigma_{n,\ell}^I \cap \Sigma_{n,\ell}^{III}$. Alors, on a à la fois $a = \theta_{n-1}b$ avec $b \in \Sigma_{n-1,\ell-1}$ et $a = \theta_{n-1}\theta_{n-2}\theta_{n-1}c$ avec $\theta_{n-2}c \in \Sigma_{n-1,\ell-2}$. On déduit $b = \theta_{n-2}\theta_{n-1}c$ en simplifiant θ_{n-1} à gauche, donc $\theta_{n-2}\theta_{n-1}c \leq \Delta_{n-1}$ et, *a fortiori*, $\theta_{n-2}\theta_{n-1} \leq \Delta_{n-1}$. Or, on a vu ci-dessus que $\theta_{n-2}\theta_{n-1}$ ne divise pas Δ_{n-1} à gauche, contradiction. Par conséquent, $\Sigma_{n,\ell}^I$ et $\Sigma_{n,\ell}^{III}$ sont disjoints.

Supposons enfin $a \in \Sigma_{n,\ell}^{II} \cap \Sigma_{n,\ell}^{III}$. On a $a = \theta_{n-2}\theta_{n-1}b = \theta_{n-1}\theta_{n-2}\theta_{n-1}c$ avec b dans $\Sigma_{n-1,\ell-2}$ vérifiant $b \leq \underline{\Delta}_{n-1,5}$ et avec $\theta_{n-2}c$ dans $\Sigma_{n-1,\ell-2}$. On déduit $\theta_{n-2}\theta_{n-1}b = \theta_{n-1}\theta_{n-2}\theta_{n-1}c = \theta_{n-2}\theta_{n-1}\theta_{n+1}c$, d'où $b = \theta_{n+1}c$ en

simplifiant $\theta_{n-2}\theta_{n-1}$ à gauche. Or, par le lemme 1.25, on a $\theta_{n+1} \not\asymp \underline{\Delta}_{n-1,5}$, ce qui contredit $\theta_{n+1} \asymp b \asymp \underline{\Delta}_{n-1,5}$. Donc $\Sigma_{n,\ell}^{\text{II}}$ et $\Sigma_{n,\ell}^{\text{III}}$ sont disjoints. \square

On est maintenant prêt à conclure l'argument et établir le résultat de partition annoncé. Grâce à tous les lemmes préparatoires accumulés dans la sous-section 2.1, la démonstration est brève.

DÉMONSTRATION DE LA PROPOSITION 2.3. Au vu des lemmes 2.14 et 2.15, il ne reste plus qu'à montrer que tout élément de $\Sigma_{n,\ell}$ appartient à (au moins) un des quatre ensembles $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^{\text{I}}, \Sigma_{n,\ell}^{\text{II}}, \Sigma_{n,\ell}^{\text{III}}$.

Soit a un élément de $\Sigma_{n,\ell}$. Par le lemme 2.7, soit a est un diviseur à gauche de $\Delta_{n-0,5}$, soit a est de la forme $b\theta_{n+|b|-1}c$ avec $bc \asymp \Delta_{n-0,5}$.

Supposons d'abord $a \asymp \Delta_{n-0,5}$. Par le lemme 2.13, soit on a $a \asymp \Delta_{n-1}$, d'où $a \in \Sigma_{n,\ell}^0$, soit a est de la forme $\theta_{n-2}\theta_{n-1}d$ avec $d \asymp \Delta_{n-1,5}$, d'où $a \in \Sigma_{n,\ell}^{\text{II}}$.

Supposons maintenant a de la forme $b\theta_{n+|b|-1}c$ avec $bc \asymp \Delta_{n-0,5}$. Par le lemme 2.7, on a $a = \theta_{n-1}bc$ avec $bc \asymp \Delta_{n-0,5}$. Par le lemme 2.13, il y a à nouveau deux possibilités. Soit bc divisé à gauche Δ_{n-1} , et on trouve $a = \theta_{n-1}bc$ avec $bc \asymp \Delta_{n-1}$, d'où $a \in \Sigma_{n,\ell}^{\text{I}}$. Soit bc est de la forme $\theta_{n-2}\theta_{n-1}d$ avec $d \asymp \underline{\Delta}_{n-1,5}$. De là, on a $a = \theta_{n-1}\theta_{n-2}\theta_{n-1}d$ avec $d \asymp \Delta_{n-1,5}$. En outre, $d \asymp \Delta_{n-1,5}$ implique

$$\theta_{n-2}d \asymp \theta_{n-2}\Delta_{n-1,5} = \Delta_{n-1},$$

d'où $a \in \Sigma_{n,\ell}^{\text{III}}$. L'argument est donc complet. \square

2.3. Dénombrement des diviseurs de Δ_n . Grâce au résultat de partition démontré dans la sous-section 2.2, on va maintenant pouvoir dénombrer inductivement les diviseurs à gauche de Δ_n :

PROPOSITION 2.17 (dénombrement). *Pour $n \geq 2$, on a*

$$(2.18) \quad \#\Sigma_n = \#\{a \in H^+ \mid a \asymp \Delta_n\} = 2 \cdot 3^{n-2}.$$

Ainsi, le nombre de diviseurs à gauche de Δ_n dans H^+ est $2 \cdot 3^{n-2}$. Noter que, pour $n = 1$, on a $\Delta_1 = 1$, d'où $\Sigma_1 = \{1\}$, et $\#\Sigma_1 = 1$: la formule de la proposition 2.17 est donc en défaut (sauf à considérer 1 comme l'entier immédiatement supérieur à $2/3$).

En utilisant (1.23), on déduit immédiatement

COROLLAIRE 2.19 (dénombrement). *Pour $n \geq 3$, on a*

$$(2.20) \quad \#\{a \in H^+ \mid a \text{ simple et } \text{ind}(a) = n\} = 4 \cdot 3^{n-3}.$$

On rappelle que le cardinal de $\Sigma_{n,\ell}$, c'est-à-dire le nombre de diviseurs à gauche de Δ_n de longueur ℓ , est noté $N_{n,\ell}$. La démonstration de la proposition 2.17 repose sur la formule de récurrence suivante :

LEMME 2.21. *Pour $n \geq 3$ et $2 \leq \ell \leq 2n - 3$, on a*

$$(2.22) \quad N_{n,\ell} = N_{n-1,\ell} + N_{n-1,\ell-1} + N_{n-1,\ell-2}.$$

DÉMONSTRATION. On commence par le cas $n = 3$, auquel cas ℓ ne peut prendre que les valeurs 2 et 3. Les deux seules expressions de Δ_3 sont $\theta_1\theta_2\theta_4$ et $\theta_2\theta_1\theta_2$, d'où il résulte qu'on a $\Sigma_{3,2} = \{\theta_1\theta_2, \theta_2\theta_1\}$ et $\Sigma_{3,3} = \{\Delta_3\}$, et on trouve bien

$$\begin{aligned} N_{3,2} &= 2 = 0 + 1 + 1 = N_{2,2} + N_{2,1} + N_{2,0} \\ N_{3,3} &= 1 = 0 + 0 + 1 = N_{2,3} + N_{2,2} + N_{2,1}. \end{aligned}$$

Supposons maintenant $n \geq 4$ et $2 \leq \ell \leq 2n - 3$. Par la proposition 2.3, on a, en termes des ensembles $\Sigma_{n,\ell}^0, \dots, \Sigma_{n,\ell}^{\text{III}}$ de la définition 2.2,

$$N_{n,\ell} = \#\Sigma_{n,\ell}^0 + \#\Sigma_{n,\ell}^{\text{I}} + \#\Sigma_{n,\ell}^{\text{II}} + \#\Sigma_{n,\ell}^{\text{III}}.$$

Par définition, on a $\Sigma_{n,\ell}^0 = \Sigma_{n-1,\ell}$, d'où

$$\#\Sigma_{n,\ell}^0 = \#\Sigma_{n-1,\ell} = N_{n-1,\ell}.$$

Ensuite, on a

$$\Sigma_{n,\ell}^{\text{I}} = \{\theta_{n-1}a \mid a \preccurlyeq \Delta_{n-1} \text{ et } |a| = \ell - 1\},$$

d'où $\#\Sigma_{n,\ell}^{\text{I}} \leq N_{n-1,\ell-1}$. De plus, si a_1 et a_2 sont distincts dans $\Sigma_{n-1,\ell-1}$, alors, par simplifiabilité à gauche, $\theta_{n-1}a_1$ et $\theta_{n-1}a_2$ sont distincts dans $\Sigma_{n,\ell}^{\text{I}}$. On a donc $\#\Sigma_{n,\ell}^{\text{I}} = N_{n-1,\ell-1}$.

Enfin, par le lemme 2.8, on a

$$\{a \in \Sigma_{n-1,\ell-2} \text{ et } a \preccurlyeq \Delta_{n-1,5}\} \cup \{\theta_{n-2}b \in \Sigma_{n-1,\ell-2}\} = \Sigma_{n-1,\ell-2},$$

et, par le lemme 2.15, $\Sigma_{n,\ell}^{\text{II}}$ et $\Sigma_{n,\ell}^{\text{III}}$ sont disjoints. Ensuite, si a_1 et a_2 sont deux éléments distincts de $\Sigma_{n-1,\ell-2}$ vérifiant $a_1, a_2 \preccurlyeq \Delta_{n-1,5}$, on a $\theta_{n-2}\theta_{n-1}a_1 \neq \theta_{n-2}\theta_{n-1}a_2$, par simplifiabilité à gauche. De même, si $\theta_{n-2}b_1$ et $\theta_{n-2}b_2$ sont deux éléments distincts de $\Sigma_{n-1,\ell-2}$, alors on a $b_1 \neq b_2$, par simplifiabilité à gauche, puis, de même, $\theta_{n-1}\theta_{n-2}\theta_{n-1}b_1 \neq \theta_{n-1}\theta_{n-2}\theta_{n-1}b_2$. Finalement, on déduit l'égalité $\#\Sigma_{n,\ell}^{\text{II}} + \#\Sigma_{n,\ell}^{\text{III}} = N_{n-1,\ell-2}$, d'où (2.22) en faisant la somme. \square

On peut maintenant compléter l'argument.

DÉMONSTRATION DE LA PROPOSITION 2.17. On montre le résultat par récurrence sur $n \geq 2$. Pour $n = 2$, l'élément Δ_2 a deux diviseurs à gauche, à savoir l'élément neutre 1 et θ_1 , donc le résultat est vrai.

Supposons $n \geq 3$. Pour les diviseurs de longueur 0 et 1, la proposition 1.25 implique $N_{n,0} = N_{n-1,0} = 1$ et $N_{n,1} = 1 + N_{n-1,1} = N_{n-1,0} + N_{n-1,1}$. Alors, le lemme 2.21 implique que le nombre de diviseurs à gauche de Δ_n est

$$\begin{aligned} \sum_{\ell=0}^{2n-3} N_{n,\ell} &= N_{n,0} + N_{n,1} + \sum_{\ell=2}^{2n-3} N_{n,\ell}, \\ &= N_{n-1,0} + N_{n-1,0} + N_{n-1,1} + S, \end{aligned}$$

en posant $S := \sum_{\ell=2}^{2n-3} (N_{n-1,\ell} + N_{n-1,\ell-1} + N_{n-1,\ell-2})$. La somme S contient un seul terme $N_{n-1,0}$, provenant de $\ell = 2$. Ensuite, S contient deux termes $N_{n-1,1}$, l'un provenant de $\ell = 2$ et l'autre de $\ell = 3$. Pour $2 \leq i \leq 2n-5$, la somme S contient trois termes $N_{n-1,i}$, un provenant de $\ell = i$, un de $\ell = i+1$ et un autre de $\ell = i+2$. À la fin, comme on a $\ell \leq 2n-3$, la somme S contient seulement deux termes $N_{n-1,2n-4}$, l'un provenant de $\ell = 2n-4$ et l'autre de $\ell = 2n-3$, et un seul terme $N_{n-1,2n-3}$ provenant de $\ell = 2n-3$. On trouve donc au total

$$\sum_{\ell=0}^{2n-3} N_{\ell,n} = 3 \sum_{\ell=0}^{2n-5} N_{\ell,n-1} + 2N_{n-1,2n-4} + N_{n-1,2n-3}.$$

Or, comme on a $|\Delta_{n-1}| = 2n-5$, on déduit $N_{2n-4,n-1} = N_{2n-3,n-1} = 0$ et, finalement,

$$\sum_{\ell=0}^{2n-3} N_{\ell,n} = 3 \cdot \sum_{\ell=0}^{2n-5} N_{\ell,n-1},$$

d'où le résultat par induction. \square

La table 1 montre les valeurs des nombres $N_{n,\ell}$ pour $n \leq 10$ et $\ell \leq 11$, telles que résultant des formules de récurrence (2.22). Ces valeurs apparaissent donc dans un triangle de Pascal généralisé où un nombre est la somme des trois nombres situés sur la ligne au-dessus, voir [49] et la figure 1. Signalons ici que les valeurs de la table 1 ont été confirmées — en fait prédites — par un calcul direct par ordinateur fondé sur la section VI.2.3 et écrit avant que la preuve ci-dessus soit établie.

3. Forme normale et décomposition

On poursuit maintenant l'étude des éléments simples du monoïde H^+ en caractérisant leurs formes normales telle que définies au chapitre II : le résultat principal (proposition 3.24) est que, tous comme les mots réduits, les mots réduits « simples » sont caractérisés par le fait d'éviter certains facteurs, ici de longueur 2 ou 3, ce qui implique en particulier que la propriété pour un Θ -mot de représenter un élément simple de H^+ est décidable de façon très simple. La démonstration est délicate et requiert plusieurs lemmes préparatoires.

La section est divisée en trois parties. Dans la section 3.1, on établit une borne explicite pour l'indice d'un élément simple en fonction de son plafond, ce qui suffit à assurer que la simplicité est une propriété décidable. Ensuite, dans la section 3.2, on établit le lemme-clé, qui relie explicitement la forme normale d'un élément simple à celle d'un de ses diviseurs à droite suivant la partition de la section 2.2, et on en déduit que les formes normales des éléments simples évitent un certain nombre de facteurs. Enfin, dans la section 3.3, on montre que, réciproquement, tous les mots évitant les facteurs obtenus ci-dessus sont des formes normales d'éléments simples.

$\ell \downarrow$	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6	Δ_7	Δ_8	Δ_9	Δ_{10}
0	1	1	1	1	1	1	1	1	1	1
1	0	1	2	3	4	5	6	7	8	9
2	0	0	2	5	9	14	20	27	35	44
3	0	0	1	5	13	26	45	71	105	148
4	0	0	0	3	13	35	75	140	238	378
5	0	0	0	1	9	35	96	216	427	770
6	0	0	0	0	4	26	96	267	623	1288
7	0	0	0	0	1	14	75	267	750	1800
8	0	0	0	0	0	5	45	216	750	2123
9	0	0	0	0	0	1	20	140	623	2123
10	0	0	0	0	0	0	6	71	427	1800
11	0	0	0	0	0	0	1	27	238	1288
total	1	2	6	18	54	162	486	1458	4374	13122

TABLE 1. Dénombrément des diviseurs à gauche de Δ_n classés par longueur, telles que résultant des formules de cette section et d'un comptage direct par ordinateur des diviseurs de Δ_n .

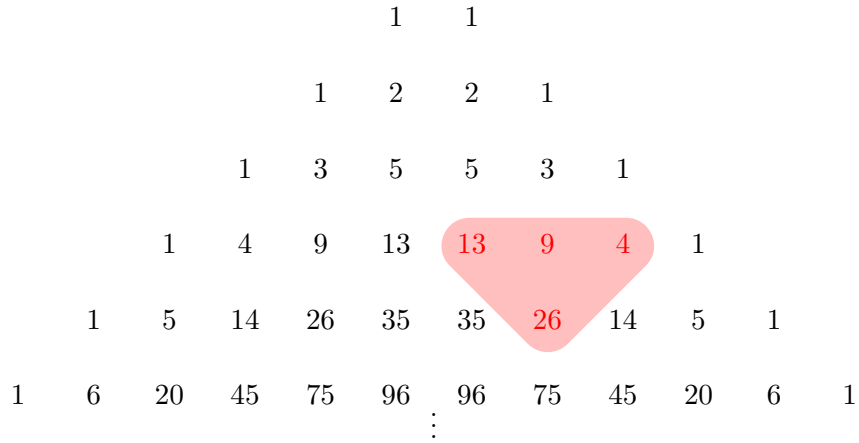


FIGURE 1. Triangle de Pascal généralisé engendrant les nombres $N_{n,\ell}$ à partir de la formule (2.22) : chaque nombre est la somme des *trois* nombres qui sont au-dessus de lui dans le triangle, par exemple 26 est la somme de 13, 9, et 4 ; à l'extérieur du triangle, les valeurs manquantes sont supposées être des 0.

3.1. Décidabilité de la simplicité. Après les résultats de dénombrement de la section 2.1, on continue avec une autre application importante des résultats fins de la section 2.3, à savoir la décidabilité de la propriété d'être un élément simple de H^+ .

Un élément a de H^+ est simple si, et seulement si, il existe un entier non nul n satisfaisant $a \preceq \Delta_n$. Pour une valeur de n donnée, on sait tester $a \preceq \Delta_n$, mais, pour tester $\exists n (a \preceq \Delta_n)$, il faut *a priori* une borne supérieure sur les indices n à considérer. Dans le cas présent, une telle borne peut être donnée à partir du plafond (définition I.3.11).

LEMME 3.1. *Pour tout élément simple a de H^+ , on a*

$$(3.2) \quad \text{ind}(a) \leq [a] + 1.$$

DÉMONSTRATION. Supposons que a est simple, posons $n := \text{ind}(a)$, et supposons qu'on a $[a] + 1 < n$. Il s'agit d'obtenir une contradiction.

Le lemme 2.7 implique qu'on a soit $a \preceq \Delta_{n-0,5}$, soit $a = b\theta_{n+|b|-1}c$ avec $bc \preceq \Delta_{n-0,5}$. Supposons d'abord $a \preceq \Delta_{n-0,5}$ à gauche. Par le lemme 2.13, on a soit $a \preceq \Delta_{n-1}$, ce qui contredit l'hypothèse que n est l'indice de a , soit $a = \theta_{n-2}\theta_{n-1}c$ avec $c \preceq \Delta_{n-1,5}$, ce qui implique $[a] \geq n - 1$ et contredit $[a] + 1 < n$. Supposons maintenant $a = b\theta_{n+|b|-1}c$ avec $bc \preceq \Delta_{n-0,5}$. Alors, par le lemme 2.7, on a $\theta_{n-1} \preceq a$, ce qui implique $[a] \geq n - 1$ et contredit $[a] + 1 < n$ à nouveau. \square

Une première application du lemme est une borne sur les indices des diviseurs simples d'un élément quelconque de H^+ :

COROLLAIRE 3.3 (**diviseurs simples**). *Pour tout a dans H^+ , tout élément simple s vérifiant $s \preceq a$ vérifie $s \preceq a \wedge \Delta_{[a]+1}$.*

DÉMONSTRATION. Supposons $s \preceq a$ avec s simple. Le lemme 3.1 implique $s \preceq \Delta_{[s]+1}$, et le corollaire I.3.22 implique $[s] \leq [a]$, d'où $s \preceq \Delta_{[a]+1}$. Alors la conjonction avec l'hypothèse $s \preceq a$ implique $s \preceq a \wedge \Delta_{[a]+1}$. \square

Une seconde application du lemme 3.1 est une caractérisation de la simplicité :

PROPOSITION 3.4 (**simplicité**). *Un élément a de H^+ est simple si, et seulement si, a vérifie*

$$(3.5) \quad a \preceq \Delta_{[a]+1}.$$

DÉMONSTRATION. Si a est simple, alors, par définition, on a $a \preceq \Delta_{\text{ind}(a)}$, qui entraîne $a \preceq \Delta_n$ pour tout $n \geq \text{ind}(a)$, donc (3.2) implique (3.5).

Inversement, si (3.5) est vérifié, il existe n tel que a divise à gauche Δ_n , et a est simple par définition. \square

Une conséquence importante au moins en théorie, de la proposition 3.4 est la décidabilité de la simplicité :

COROLLAIRE 3.6 (**décidabilité**). *La propriété pour un Θ -mot w de représenter un élément simple de H^+ est décidable.*

DÉMONSTRATION. Soit w un mot quelconque de Θ^* . Par la proposition 3.4, et puisqu'on a $[[w]] = [w]$, l'élément $[w]$ est simple si, et seulement si, $[w] \preceq \Delta_{[w]+1}$, donc si, et seulement si, le retournement à droite du

mot $\bar{w} \underline{\Delta}_{[w]_{+1}}$ se termine avec un mot positif : c'est une propriété décidable de w . \square

On donnera dans la section 3.2 une bien meilleure solution à la question précédente, puisqu'on montrera que la simplicité de $[w]$ se lit directement à partir de la \mathcal{E}_H -réduction du mot w .

3.2. Le lemme-clé. Notre but désormais est d'étudier les formes normales (au sens du chapitre II) des éléments simples de H^+ , le résultat final visé étant la proposition 3.24 qui caractérise celles-ci comme les mots réduits qui évitent un certain nombre de facteurs interdits explicites \mathcal{I}_Σ .

On commence par l'étude du support des formes normales d'éléments simples, c'est-à-dire la question de savoir quelles lettres peuvent apparaître dans la forme normale d'un élément simple, typiquement en position 1 ou 2. On va établir ici diverses contraintes, dont on montrera ensuite dans la section 3.2 qu'elles sont aussi suffisantes.

On rappelle qu'un mot w de Θ est dit réduit s'il n'est réductible à aucun mot autre que lui-même vis-à-vis du système \mathcal{E}_H de la définition II.3.1. On rappelle qu'un Θ -mot est réduit si, et seulement si, il évite l'ensemble de mots \mathcal{I} (proposition II.3.20). Pour tout a dans H^+ , on note $\text{NF}(a)$ l'unique mot réduit w représentant a , qu'on appelle la *forme normale* de a .

Le premier résultat concerne la première lettre de la forme normale d'un élément simple.

LEMME 3.7. *Si on a $a \preceq \Delta_{n+0,5}$, et donc en particulier si a est simple d'indice $\leq n$, alors la première lettre de $\text{NF}(a)$ est parmi $\theta_1, \dots, \theta_{n-1}$.*

DÉMONSTRATION. Si un Θ -mot w commence par la lettre θ_i , on a, par définition, $\theta_i \preceq [w]$ dans H^+ . Donc, si $\text{NF}(a)$ commence par θ_i , on a nécessairement $\theta_i \preceq a$, d'où $\theta_i \preceq \Delta_{n+0,5}$ puisqu'on suppose $a \preceq \Delta_{n+0,5}$. Or, par la proposition 1.25, on sait que les seuls atomes θ_i vérifiant $\theta_i \preceq \Delta_{n+0,5}$ sont $\theta_1, \dots, \theta_{n-1}$. Donc $\theta_i \preceq a$ implique $i \leq n-1$, et, de là, la première lettre de $\text{NF}(a)$ doit être parmi $\theta_1, \dots, \theta_{n-1}$. \square

Le résultat suivant est le point fondamental pour déterminer inductivement la forme normale d'un élément simple suivant sa classe dans la partition de la proposition 2.3.

PROPOSITION 3.8 (lemme-clé). *Pour a simple d'indice ≤ 3 , on a*

$$(3.9) \quad \text{NF}(a) \in \{\varepsilon, \theta_1, \theta_2, \theta_1\theta_2, \theta_2\theta_1, \theta_2\theta_1\theta_2\}.$$

Pour a simple d'indice $n \geq 4$, il existe b simple dans H^+ d'indice $< n$ et on a une, et une seule, des relations suivantes :

$$(3.10) \quad (\text{type I}) \quad b \preceq \Delta_{n-1} \quad \text{et} \quad \text{NF}(a) = \theta_{n-1}\text{NF}(b),$$

$$(3.11) \quad (\text{type II}) \quad b \preceq \Delta_{n-1,5} \quad \text{et} \quad \text{NF}(a) = \theta_{n-2}\theta_{n-1}\text{NF}(b),$$

$$(3.12) \quad (\text{type III}) \quad \theta_{n-2}b \preceq \Delta_{n-1} \quad \text{et} \quad \text{NF}(a) = \theta_{n-1}\theta_{n-2}\theta_{n-1}\text{NF}(b).$$

DÉMONSTRATION. Posons $n := \text{ind}(a)$. D'abord, les cas $n \leq 3$ sont faciles. Pour $n = 1$, la seule possibilité est $a = 1$, de forme normale le mot vide ε . Pour $n = 2$, l'hypothèse est $a \preceq \Delta_2$ avec $a \not\preceq \Delta_1$, et la seule possibilité est $a = \theta_1$, d'où $\text{NF}(a) = \theta_1$. Pour $n = 3$, l'hypothèse est $a \preceq \Delta_3$ avec $a \not\preceq \Delta_2$: les seules possibilités sont les quatre éléments $\theta_2, \theta_2\theta_1, \theta_1\theta_2$, et Δ_3 , dont les formes normales respectives sont $\theta_2, \theta_2\theta_1, \theta_1\theta_2$, et $\theta_2\theta_1\theta_2$. Donc (3.9) est établie.

Supposons maintenant $n = \text{ind}(a) \geq 4$, et posons $\ell := |a|$. Par hypothèse, puisque l'indice de a est n , l'élément a est dans $\Sigma_{n,\ell} \setminus \Sigma_{n-1,\ell}$. Le résultat de partition de la proposition 2.3 implique alors que a appartient à l'un exactement des trois ensembles $\Sigma_{n,\ell}^{\text{I}}, \Sigma_{n,\ell}^{\text{II}}$, ou $\Sigma_{n,\ell}^{\text{III}}$. Autrement dit, on est dans exactement un des trois cas suivants :

$$(3.13) \quad (\text{type I}) \quad b \preceq \Delta_{n-1} \quad \text{et} \quad a = \theta_{n-1} b,$$

$$(3.14) \quad (\text{type II}) \quad b \preceq \Delta_{n-1,5} \quad \text{et} \quad a = \theta_{n-2}\theta_{n-1} b,$$

$$(3.15) \quad (\text{type III}) \quad \theta_{n-2}b \preceq \Delta_{n-1} \quad \text{et} \quad a = \theta_{n-1}\theta_{n-2}\theta_{n-1} b.$$

Dans le cas de (3.13), on a $b \preceq \Delta_{n-1}$, donc b est simple et on a $\text{ind}(b) \leq n-1$. Dans le cas de (3.14), on a

$$b \preceq \Delta_{n-1,5} \preceq \Delta_{n-1,5}\theta_{3n-8} = \Delta_{n-1},$$

donc, à nouveau, b est simple et on a $\text{ind}(b) \leq n-1$. Enfin, dans le cas de (3.15), le lemme 2.9 implique $b \preceq \Delta_{n-1,5}$, donc $b \preceq \Delta_{n-1}$, et, de là, encore une fois, b est simple et on a $\text{ind}(b) \leq n-1$. Donc, dans tous les cas, b est simple et on a $\text{ind}(b) < n = \text{ind}(a)$. De là, la définition de NF et la proposition 1.25 impliquent que

$$(3.16) \quad \text{NF}(b) \text{ est un mot réduit et sa première lettre est parmi } \theta_1, \dots, \theta_{n-2}.$$

Dans le cas de (3.13), la relation (3.16) implique que le mot $\theta_{n-1}\text{NF}(b)$, et en particulier son facteur initial de longueur 2, évitent \mathcal{I} , et donc $\theta_{n-1}\text{NF}(b)$ est un mot réduit. Alors l'égalité $a = \theta_{n-1}b$ dans H^+ implique l'égalité $\text{NF}(a) = \theta_{n-1}\text{NF}(b)$ dans Θ^* , et (3.10) est satisfaite.

Dans le cas de (3.14), la relation (3.16) implique que le mot $\theta_{n-2}\theta_{n-1}\text{NF}(b)$, et en particulier ses facteurs initiaux de longueur 2 en position 1 et 2, évitent \mathcal{I} , et donc $\theta_{n-2}\theta_{n-1}\text{NF}(b)$ est un mot réduit. Alors l'égalité $a = \theta_{n-2}\theta_{n-1}b$ dans H^+ implique l'égalité $\text{NF}(a) = \theta_{n-2}\theta_{n-1}\text{NF}(b)$ dans Θ^* , et (3.11) est satisfaite.

Enfin, dans le cas de (3.15), la relation (3.16) implique que le mot $\theta_{n-1}\theta_{n-2}\theta_{n-1}\text{NF}(b)$, et en particulier ses facteurs initiaux de longueur 2 en position 1, 2, et 3, évitent \mathcal{I} , et donc $\theta_{n-1}\theta_{n-2}\theta_{n-1}\text{NF}(b)$ est un mot réduit. Alors l'égalité $a = \theta_{n-1}\theta_{n-2}\theta_{n-1}b$ dans H^+ implique l'égalité $\text{NF}(a) = \theta_{n-1}\theta_{n-2}\theta_{n-1}\text{NF}(b)$ dans Θ^* , et (3.12) est satisfaite. \square

Une première application directe du lemme-clé (proposition 3.8) est une borne supérieure pour la hauteur de la forme normale d'une élément simple.

On rappelle que la hauteur $\text{ht}(w)$ d'un mot de Θ^* est le maximum des indices i des lettres θ_i qui y figurent (définition I.3.8).

PROPOSITION 3.17 (**hauteur**). *Pour tout élément simple a de H^+ , on a*

$$(3.18) \quad \text{ht}(\text{NF}(a)) \leq \text{ind}(a) - 1.$$

DÉMONSTRATION. On raisonne par induction sur $n := \text{ind}(a)$. Pour $n \leq 3$, une inspection au cas par cas sur les 6 mots de (3.9) donne le résultat directement.

Supposons maintenant $n \geq 4$. Par le lemme-clé (proposition 3.8), il existe b simple d'indice $< n$ tel qu'on soit dans un (et un seul) des cas (3.10), (3.11), ou (3.12). Par hypothèse d'induction, on a

$$\text{ht}(\text{NF}(b)) \leq n - 2,$$

et les formes explicites de (3.10), (3.11), et (3.12) montrent que, dans tous les cas, on a

$$\text{ht}(\text{NF}(a)) \leq \max(\text{ht}(\text{NF}(b)), n - 1),$$

d'où (3.18). \square

Noter que l'inclusion (3.18) est optimale : pour $a = \Delta_n$, qui est simple d'indice n , on sait par la proposition 1.9 que $\text{NF}(a)$ est le mot

$$\theta_{n-1} \cdot \theta_{n-2} \theta_{n-1} \cdot \theta_{n-3} \theta_{n-2} \cdot \cdots \cdot \theta_2 \theta_3 \cdot \theta_1 \theta_2,$$

et (3.18) est une égalité. Noter aussi que (3.18) implique une borne inférieure sur l'indice d'un élément simple en fonction de son plafond :

COROLLAIRE 3.19 (**bornes indice**). *Pour tout a simple dans H^+ , on a*

$$(3.20) \quad [a] - |a| + 2 \leq \text{ind}(a) \leq [a] + 1.$$

DÉMONSTRATION. D'abord, (3.18) implique, pour a simple, l'inégalité $\text{ind}(a) \geq \text{ht}(\text{NF}(a)) + 1$. Ensuite, pour tout Θ -mot w , on a $\text{ht}(w) \geq [w] - |w| + 1$ par (I.3.18), d'où $\text{ht}(\text{NF}(a)) \geq [a] - |a| + 1$ pour tout a dans H^+ . On en déduit la première inégalité de (3.20). La seconde est (3.2), établie dans le lemme 3.1. \square

Une seconde application du lemme-clé (proposition 3.8) est que, outre les obstructions de \mathcal{I} , un certain nombre de facteurs supplémentaires sont interdits dans les formes normales des éléments simples de H^+ . On rappelle qu'on dit qu'un mot w évite un ensemble de mots X si aucun facteur de w n'appartient à X .

PROPOSITION 3.21 (**facteurs interdits**). *Posons*

$$(3.22) \quad \mathcal{I}_\Sigma := \{\theta_i^2 \mid i \geq 1\} \cup \{\theta_i \theta_{i+2} \mid i \geq 1\} \\ \cup \{\theta_i \theta_{i+1} \theta_i \mid i \geq 1\} \cup \{\theta_i \theta_{i+1} \theta_{i+2} \mid i \geq 1\}.$$

Alors, pour tout élément simple a de H^+ , le mot $\text{NF}(a)$ évite \mathcal{I} et \mathcal{I}_Σ .

DÉMONSTRATION. Par définition, tout mot $\text{NF}(a)$ est un mot réduit, donc, par la proposition II.3.20, il évite \mathcal{I} . Le point est de montrer que, si a est simple, alors $\text{NF}(a)$ évite aussi les quatre types additionnels de \mathcal{I}_Σ . Comme précédemment, on va montrer ce point par induction sur l'indice n de a . Pour $n \leq 3$, une inspection au cas par cas sur les 6 mots de (3.9) donne le résultat directement.

Supposons maintenant $n \geq 4$. Par le lemme-clé (proposition 3.8), il existe b simple d'indice $< n$ tel qu'on soit dans un (et un seul) des cas (3.10), (3.11), ou (3.12). Par hypothèse d'induction, le mot $\text{NF}(b)$ évite \mathcal{I}_Σ , et il ne reste qu'à montrer que l'adjonction des lettres initiales faisant passer de $\text{NF}(b)$ à $\text{NF}(a)$, qui crée de nouveaux facteurs, ne peut en créer aucun appartenant à \mathcal{I}_Σ . Le point important est que, par le lemme 3.7, on sait que la première lettre de $\text{NF}(b)$ est parmi $\theta_1, \dots, \theta_{n-2}$.

Dans le cas de (3.10), $\text{NF}(a)$ commence par $\theta_{n-1}\theta_j$ avec $1 \leq j \leq n-2$, et ce mot de longueur 2 n'est pas dans \mathcal{I}_Σ , ni n'est le début d'un mot de \mathcal{I}_Σ . De même, dans le cas de (3.11), $\text{NF}(a)$ commence par $\theta_{n-2}\theta_{n-1}\theta_j$ avec $1 \leq j \leq n-2$, et ce mot de longueur 3 n'inclut pas de mot de \mathcal{I}_Σ , ni ne peut contribuer à un facteur initial de longueur au moins 2 d'un tel mot. Enfin, dans le cas de (3.12), $\text{NF}(a)$ commence par $\theta_{n-1}\theta_{n-2}\theta_{n-1}\theta_j$ avec $1 \leq j \leq n-2$, et, à nouveau, ce mot de longueur 4 n'inclut pas de mot de \mathcal{I}_Σ , ni ne peut contribuer à un facteur initial de longueur au moins 2 d'un tel mot. Donc, dans tous les cas, le mot $\text{NF}(a)$ évite \mathcal{I}_Σ . \square

Une troisième application du lemme-clé (proposition 3.8) est une observation supplémentaire sur la première lettre des mots normaux.

LEMME 3.23. *Si on a $a \preceq \Delta_n$ et $\theta_{n-1} \preceq a$, alors la première lettre de $\text{NF}(a)$ est θ_{n-1} .*

DÉMONSTRATION. Supposons $a \preceq \Delta_n$ et $\theta_{n-1} \preceq a$. Puisqu'on a $a \preceq \Delta_n$, l'élément a est simple et on a $\text{ind}(a) \leq n$. Si on avait $\text{ind}(a) \leq n-1$, donc $a \preceq \Delta_{n-1}$, et puisque les atomes divisant à gauche a divisent à gauche Δ_{n-1} , ceux-ci seraient parmi $\theta_1, \dots, \theta_{n-2}$, et donc $\theta_{n-1} \preceq a$ serait impossible. On a donc $\text{ind}(a) = n$. On applique alors le lemme-clé (proposition 3.8). Pour $n \leq 3$, l'inspection des 6 éléments simples possibles suivant (3.9) montre que la propriété est vraie : l'unique élément d'indice 2 divisible par θ_1 a sa forme normale commençant par (en fait, égale à) θ_1 , et les 3 éléments d'indice 3 divisibles par θ_2 ont leur forme normale commençant par θ_2 . Supposons $n \geq 4$. On est alors dans un des trois cas (3.10), (3.11), (3.12). Dans les cas (3.10) et (3.12), le mot $\text{NF}(a)$ commence explicitement par θ_{n-1} . Reste le cas (3.11). Supposons $a = \theta_{n-2}\theta_{n-1}b$ avec $b \preceq \Delta_{n-1,5}$. En retournant le mot $\overline{\theta_{n-1}\theta_{n-2}\theta_{n-1}w}$, où w est un Θ -mot quelconque représentant b , on voit que $\theta_{n-1} \preceq a$ équivaut à $\theta_{n+1} \preceq b$, donc implique

$$\theta_{n+1} \preceq b \preceq \Delta_{n-1,5} \preceq \Delta_{n-1,5}\theta_{3n-8} = \Delta_{n-1},$$

contredisant la proposition 1.25 qui montre que les seuls atomes divisant à gauche Δ_{n-1} sont $\theta_1, \dots, \theta_{n-2}$. \square

3.3. Forme normale des éléments simples. On va maintenant montrer que le résultat de la proposition 3.21 est optimal en établissant qu'inversement tout mot réduit évitant \mathcal{I}_Σ est la forme normale d'un élément simple. On aura ainsi obtenu une caractérisation complète de la forme normale des éléments simples du monoïde H^+ . Le résultat visé est donc :

PROPOSITION 3.24 (forme normale). *Un Θ -mot est la forme normale d'un élément simple de H^+ si, et seulement si, il évite les ensembles \mathcal{I} et \mathcal{I}_Σ .*

Au vu de la proposition 3.21, il reste à montrer que tout Θ -mot réduit évitant \mathcal{I}_Σ est la forme normale d'un élément simple. On commence par une observation préliminaire.

LEMME 3.25. *Si $\theta_i v$ est un Θ -mot réduit évitant \mathcal{I}_Σ , on a*

$$(3.26) \quad \text{ht}(v) \leq i + 1.$$

DÉMONSTRATION. On montre le résultat par récurrence sur la longueur de v . Pour $|v| = 0$, (3.26) est trivialement vraie.

Supposons $|v| \geq 1$, et posons $v = \theta_j w$. Puisque $\theta_i v$, c'est-à-dire $\theta_i \theta_j w$, est réduit, il évite \mathcal{I} , donc $j \geq i + 3$ est exclu. Par ailleurs, puisque $\theta_i v$ évite \mathcal{I}_Σ , les valeurs $j = i$ et $j = i + 2$ sont exclues. Les valeurs possibles de j sont donc seulement $1, \dots, i - 1$, et $i + 1$.

Supposons d'abord $j \leq i - 1$. Comme tout facteur d'un mot réduit évitant \mathcal{I}_Σ est réduit et évite \mathcal{I}_Σ , le mot $\theta_j w$ est réduit et évite \mathcal{I}_Σ , et, puisqu'on a $|w| < |v|$, l'hypothèse de récurrence implique $\text{ht}(w) \leq j + 1$, d'où

$$\text{ht}(v) = \max(j, \text{ht}(w)) \leq j + 1 \leq i,$$

et (3.26) est vraie.

Supposons maintenant $j = i + 1$. Pour $|v| = 1$, (3.26) est vraie : le mot $\theta_i \theta_{i+1}$ n'a pas de facteur dans \mathcal{I}_Σ et sa hauteur est $i + 1$. Supposons maintenant $|v| \geq 2$, et posons $v = \theta_{i+1} \theta_k w$. Comme v évite \mathcal{I} , les valeurs $k \geq j + 3 = i + 4$ sont interdites, et, comme $\theta_i v$ évite \mathcal{I}_Σ , les valeurs $k = i$, $k = i + 1$, et $k = i + 2$ sont exclues également. Donc on a $k \leq i - 1$. Par construction, le mot $\theta_k w$ est réduit et évite \mathcal{I}_Σ , et on a $|w| < |v|$. L'hypothèse de récurrence implique donc $\text{ht}(w) \leq k + 1$, d'où

$$\text{ht}(v) = \max(i + 1, k, \text{ht}(w)) \leq \max(i + 1, k + 1) = i + 1. \quad \square$$

Une (longue) étude de cas va nous permettre d'établir maintenant la réciproque de la proposition 3.21 (avec, en plus, un contrôle de l'indice) :

LEMME 3.27. *Si u est un Θ -mot réduit évitant \mathcal{I}_Σ , alors u est la forme normale d'un élément simple d'indice au plus $\text{ht}(u) + 1$.*

DÉMONSTRATION. On va montrer par récurrence sur $m \geq 0$ que

$$(3.28) \quad \begin{aligned} &\text{si } u \text{ est un } \Theta\text{-mot réduit évitant } \mathcal{I}_\Sigma \\ &\text{et satisfaisant } \text{ht}(u) = m, \text{ alors on a } [u] \preceq \Delta_{m+1}, \end{aligned}$$

ce qui signifie que $[u]$ est simple d'indice au plus $\text{ht}(u) + 1$, et donne bien la conclusion annoncée quand m varie.

On suppose donc dans toute la suite que u est un Θ -mot réduit évitant \mathcal{I}_Σ et satisfaisant $\text{ht}(u) = m$, et le but est de montrer

$$(3.29) \quad [u] \preceq \Delta_{m+1}.$$

Supposons $m = 0$. Cela signifie que u est le mot vide. Alors on trouve $[u] = 1 \preceq \Delta_1 = \Delta_{m+1}$, et (3.29) est satisfaite.

Supposons $m = 1$. Cela signifie que la seule lettre apparaissant dans u est θ_1 , donc u est de la forme θ_1^ℓ avec $\ell \geq 1$. L'hypothèse que u évite \mathcal{I}_Σ impose $\ell = 1$, et u est la lettre θ_1 . On a donc $[u] = \theta_1 \preceq \theta_1 = \Delta_2 = \Delta_{m+1}$, et (3.29) est satisfaite.

Supposons maintenant $m \geq 2$. Le mot u ne peut être vide, et a donc une première lettre, soit θ_i . Par hypothèse, on a $m = \text{ht}(u)$, donc $i \leq m$. D'un autre côté, le lemme 3.25 implique $\text{ht}(u) \leq i + 1$, donc $m \leq i + 1$. Par conséquent, u ne peut commencer que par θ_m ou θ_{m-1} .

Cas 1 : On suppose que la première lettre de u est θ_{m-1} , soit $u = \theta_{m-1}v$.

Si le mot v était vide, u serait la lettre θ_{m-1} , et on aurait $\text{ht}(u) = m-1 \neq m$, contredisant l'hypothèse. Donc v est non vide. Soit θ_j sa première lettre. Par définition, on a $j \leq \text{ht}(u) = m$. De plus, u évite \mathcal{I}_Σ , donc la valeur $j = m-1$ est impossible car elle créerait dans u un facteur initial θ_{m-1}^2 , qui est dans \mathcal{I}_Σ . Par ailleurs, puisque v , en tant que facteur de u , est réduit et évite \mathcal{I}_Σ , le lemme 3.25 implique $\text{ht}(v) \leq j + 1$ et, par conséquent, $j \leq m-2$ impliquerait

$$\text{ht}(u) \leq \max(m-1, \text{ht}(v)) \leq m-1,$$

contredisant $m = \text{ht}(u)$. Donc, finalement, la seule possibilité est $j = m$, c'est-à-dire que u commence par $\theta_{m-1}\theta_m$, soit $u = \theta_{m-1}\theta_m w$.

Sous-cas 1.1 On suppose que w est le mot vide.

Alors u est le mot $\theta_{m-1}\theta_m$. Or, appliquer le lemme 1.16 donne

$$\begin{aligned} \Delta_{m+1} &= \Delta_m \theta_{3m-4} \theta_{3m-2} \\ &= \theta_{m-1} \Delta_{m-0.5} \theta_{3m-4} \theta_{3m-2} = \theta_{m-1} \theta_m \Delta_{m-0.5} \theta_{3m-2}, \end{aligned}$$

d'où on déduit $[u] \preceq \Delta_{m+1}$, et (3.29) est satisfaite.

Sous-cas 1.2 On suppose que le mot w est non vide.

Soit θ_k la première lettre de w . Comme w est facteur de u qui a pour hauteur m , on a $k \leq m$. Ensuite, comme u , et v en tant que facteur de u , évitent \mathcal{I}_Σ , les valeurs $k = m-1$ et $k = m$ sont impossibles car elles créeraient, respectivement, des facteurs $\theta_{m-1}\theta_m\theta_{m-1}$ et θ_m^2 , tous deux dans \mathcal{I}_Σ . On a donc nécessairement $k < m-1$. Comme w , en tant que facteur de u , est réduit et évite \mathcal{I}_Σ , le lemme 3.25 implique $\text{ht}(w) \leq k+1$, d'où $\text{ht}(w) \leq m-1$. Le mot w est réduit et évite \mathcal{I}_Σ , donc l'hypothèse de récurrence implique $[w] \preceq \Delta_{\text{ht}(w)+1}$, donc *a fortiori* $[w] \preceq \Delta_m$. De plus, on sait que la première lettre de w , qui est un mot réduit, n'est pas θ_{m-1} . Par le lemme 3.23, on déduit $\theta_{m-1} \not\preceq [w]$, puis, par le lemme 2.8, $[w] \preceq \Delta_{m-0.5}$. Par définition, cela signifie que $[u]$ appartient à l'ensemble $\Sigma_{m+1,|u|}^{\text{II}}$ et, donc, *a fortiori*, qu'on a $[u] \preceq \Delta_{m+1}$. Donc (3.29) est satisfaite, et l'étude du cas 1 est complète.

Cas 2. On suppose que la première lettre de u est θ_m , soit $u = \theta_m v$.

Sous-cas 2.1. On suppose que v est le mot vide.

Alors u est la lettre θ_m , de hauteur m , et on a $[u] = \theta_m \preceq \Delta_{m+1}$, donc (3.29) est satisfaite.

Sous-cas 2.2. On suppose que v n'est pas vide.

Soit θ_j la première lettre de v . Comme plus haut, l'hypothèse $\text{ht}(u) = m$ implique $j \leq m$. Ensuite u évite \mathcal{I}_Σ , donc la valeur $j = m$ est impossible car elle créerait dans u un facteur initial θ_m^2 , appartenant à \mathcal{I}_Σ . On a donc $j \leq m - 1$.

Sous-cas 2.2.1. On suppose $j \leq m - 2$.

Par le lemme 3.25, l'hypothèse que la première lettre de v est $\leq m - 2$ implique $\text{ht}(v) \leq m - 1$. De plus, comme facteur de u , le mot v est réduit et évite \mathcal{I}_Σ . L'hypothèse de récurrence implique alors $[v] \preceq \Delta_{\text{ht}(v)+1}$, donc *a fortiori* $[v] \preceq \Delta_m$. Par conséquent, on a $[u] = \theta_m[v]$ avec $[v] \preceq \Delta_m$. Par définition, cela signifie que $[u]$ appartient à l'ensemble $\Sigma_{m+1,|u|}^I$ et, de là, qu'on a $[u] \preceq \Delta_{m+1}$. Donc (3.29) est satisfaite.

Sous-cas 2.2.2. On suppose $j = m - 1$.

Posons $v = \theta_{m-1}w$. On a donc $u = \theta_m \theta_{m-1}w$.

Sous-cas 2.2.2.1. On suppose que w est le mot vide.

Alors u est $\theta_m \theta_{m-1}$. Appliquer le lemme 1.16 deux fois (une première fois à Δ_{m+1} puis une deuxième fois à Δ_m) donne

$$(3.30) \quad \Delta_{m+1} = \theta_m \Delta_m \theta_{3m-4} = \theta_m \theta_{m-1} \Delta_{m-1} \theta_{3n-7} \theta_{3m-4},$$

d'où on déduit $[u] \preceq \Delta_{m+1}$, et (3.29) est satisfaite.

Sous-cas 2.2.2.2. On suppose que w est non vide.

Soit θ_k la première lettre de w . L'hypothèse $\text{ht}(u) = m$ implique $k \leq m$. De plus, u , évite \mathcal{I}_Σ , donc la valeur $k = m - 1$ est impossible, puisqu'elle créerait dans u (en position 2) un facteur θ_{m-1}^2 appartenant à \mathcal{I}_Σ .

Sous-cas 2.2.2.2.1. On suppose $k \leq m - 2$.

Comme w , en tant que facteur de u , est réduit et évite \mathcal{I}_Σ , le lemme 3.25 implique $\text{ht}(w) \leq m - 1$, d'où $\text{ht}(v) = m - 1$. De plus, comme facteur de u , le mot v est réduit et évite \mathcal{I}_Σ . L'hypothèse de récurrence implique alors $[v] \preceq \Delta_{\text{ht}(v)+1}$, donc *a fortiori* $[v] \preceq \Delta_m$. Comme ci-dessus, cela signifie que $[u]$ appartient à l'ensemble $\Sigma_{m+1,|u|}^I$ et, de là, qu'on a $[u] \preceq \Delta_{m+1}$. Donc (3.29) est satisfaite.

Sous-cas 2.2.2.2.2. On suppose $k = m$.

Posons $w = \theta_m u'$. On a alors $u = \theta_m \theta_{m-1} \theta_m u'$.

Sous-cas 2.2.2.2.2.1. On suppose que u' est le mot vide.

Alors (3.30) donne

$$\Delta_{m+1} = \theta_m \theta_{m-1} \Delta_{m-1} \theta_{3n-7} \theta_{3m-4} = \theta_m \theta_{m-1} \theta_m \Delta_{m-1} \theta_{3n-7}.$$

D'où $[u] \preceq \Delta_{m+1}$, et (3.29) est satisfaite.

Sous-cas 2.2.2.2.2.2. On suppose que u' n'est pas vide.

Soit θ_ℓ la première lettre de u' . L'hypothèse $\text{ht}(u) = m$ implique $\ell \leq m$. L'hypothèse que u évite \mathcal{I}_Σ exclut les valeurs $\ell = m - 1$ et $\ell = m$, car elles créeraient dans u des facteurs interdits, respectivement $\theta_{m-1}\theta_m\theta_{m-1}$ et θ_m^2 , tous deux dans \mathcal{I}_Σ . On a donc $\ell \leq m - 2$. Alors le lemme 3.25 implique $\text{ht}(u') \leq m - 1$. De plus, en tant que facteur de u , le mot u' est réduit et évite \mathcal{I}_Σ . L'hypothèse de récurrence implique alors $[u'] \preceq \Delta_m$. De là, par le lemme 3.23, si on avait $\theta_{m-1} \preceq [u']$, la première lettre de u' devrait être θ_{m-1} , ce qui contredit $\ell \leq m - 2$. Donc on a $\theta_{m-1} \not\preceq [u']$ et, de là, $[u'] \preceq \Delta_{m-0,5}$ par le lemme 2.8. On a alors $\theta_{m-1}[u'] \preceq \theta_{m-1}\Delta_{m-0,5} = \Delta_m$. Par conséquent, $[u]$ est de la forme $\theta_m\theta_{m-1}\theta_m[u']$ avec $\theta_{m-1}[u'] \preceq \Delta_m$. Cela signifie que $[u]$ appartient à l'ensemble $\Sigma_{m+1,|u|}^{\text{III}}$ et, de là, qu'on a $[u] \preceq \Delta_{m+1}$. Donc (3.29) est satisfaite. L'étude du cas 2 est complète. \square

On peut désormais compléter la démonstration de la proposition 3.24 :

DÉMONSTRATION DE LA PROPOSITION 3.24. La proposition 3.21 montre que les formes normales d'éléments simples évitent \mathcal{I} et \mathcal{I}_Σ . Le lemme 3.27 montre que, réciproquement, tout Θ -mot évitant \mathcal{I} et \mathcal{I}_Σ est la forme normale d'un élément simple de H^+ . \square

EXEMPLE 3.31. Le mot $\theta_2\theta_4$ appartient à \mathcal{I}_Σ : il n'est donc pas la forme normale d'un élément simple. Cet exemple est important : on a $\Delta_3 = \theta_1 \cdot \theta_2\theta_4$, et ceci montre qu'un diviseur à droite d'un élément simple n'est pas nécessairement simple : la famille Σ des éléments simples, qui, par construction, est close par diviseur à gauche, n'est *pas close* par diviseur à droite. On verra dans la section 4 que ce défaut de clôture empêche les décompositions Σ -gloutonnes sur le monoïde H^+ de partager toutes les propriétés des décompositions gloutonnes associées à une structure de Garside.

Avec la proposition 3.24, il est très facile de reconnaître si un mot réduit représente un élément simple, et on obtient une nouvelle version du résultat de décidabilité de la simplicité (corollaire 3.6) avec une bien meilleure complexité algorithmique. Si on se limite à des Θ -mots de hauteur bornée, alors l'ensemble des formes normales d'éléments simples de H^+ est un langage régulier, donc reconnaissable par automate fini déterministe. Pour le cas général, et en se ramenant à un alphabet fini comme dans la section II.3.2, on obtient, par un argument exactement similaire à celui du corollaire II.3.25 :

COROLLAIRE 3.32 (**complexité**). *L'ensemble des codes des mots \mathcal{E}_H -réduits de Θ^* représentant un élément simple du monoïde H^+ est décidable de complexité $O(\|w\|)$.*

REMARQUE 3.33. Puisqu'il existe une bijection entre les éléments simples de H^+ et les mots de Θ^* évitant \mathcal{I} et \mathcal{I}_Σ , le dénombrement de la section 2 donne un dénombrement des mots réduits de longueur donnée. Inversement, on pourrait (peut-être) partir de la définition explicite de \mathcal{I} et \mathcal{I}_Σ pour retrouver le résultat de la proposition 2.17. On peut noter que la démonstration du lemme 3.27 reconstruit essentiellement la partition de la proposition 2.3.

4. La structure « presque-Garside » de H^+

On établit maintenant l'existence d'une nouvelle forme normale pour les éléments du monoïde H^+ . À la différence de la forme normale du chapitre II, il ne s'agit pas d'une décomposition en atomes (éléments θ_i), mais d'une décomposition en éléments simples. Cette décomposition est directement réminiscente de la forme normale gloutonne des monoïdes de Garside [28, chapitre III], mais on verra qu'elle ne satisfait pas toutes les propriétés de ces dernières à cause du manque de symétrie gauche-droite de la famille des éléments simples de H^+ .

Cette section assez brève est divisée en deux sous-sections. Dans la sous-section 4.1, on étudie les décompositions gloutonnes dans le cas général d'un monoïde noethérien à droite, sous des hypothèses légèrement différentes de celles de la théorie de Garside. Dans la sous-section 4.2, on vérifie que le monoïde H^+ satisfait les hypothèses précédentes, et on étudie les décompositions ainsi associées à la famille de ses éléments simples.

4.1. Décompositions gloutonnes. On part de la notion classique de suite gloutonne (« greedy sequence ») introduite au moins dans un article de S. Adjan [1] en 1984 et retrouvée par M. El Rifai et H. Morton [35] et W. Thurston [54] à la fin des années 1980, qui est à la base de tout le développement ultérieur de la théorie de Garside [28] :

DÉFINITION 4.1 (suite gloutonne). Si Σ est une partie d'un monoïde M , une suite finie (a_1, \dots, a_p) d'éléments de M est dite Σ -gloutonne si, pour chaque $i \leq p$, l'élément a_i appartient à Σ et, pour tout $i \leq p - 1$, on a

$$(4.2) \quad \forall s \in \Sigma (s \preceq a_i \cdots a_p \Leftrightarrow s \preceq a_i).$$

On convient que la suite vide est Σ -gloutonne. Une suite Σ -gloutonne est dite *stricte* si elle est vide ou si son dernier terme n'est pas 1.

On comprend l'utilisation du mot « glouton » : ce qu'exprime (4.2) est que chaque terme de la suite est « le plus gros élément possible de Σ » divisant tout ce qui est à sa droite. On voit facilement qu'une suite (a_1, \dots, a_p) est Σ -gloutonne si, et seulement si, la suite $(a_1, \dots, a_p, 1)$ l'est : ajouter des termes triviaux à droite ne change rien à la gloutonnerie, d'où l'introduction du qualificatif « strict » si on veut éviter ces termes finaux « stupides ».

On dit qu'une suite d'éléments (a_1, \dots, a_p) d'un monoïde M est une *décomposition* d'un élément a si, dans M , on a l'égalité $a = a_1 \cdots a_p$. On va montrer le résultat suivant, dont la conclusion est exactement l'existence et l'unicité de la « greedy normal form » de la théorie de Garside :

PROPOSITION 4.3 (décomposition gloutonne). *Si M est un monoïde simplifiable, sans élément inversible non trivial, noethérien à droite, et admettant des ppcm conditionnels à droite, et si Σ est une famille d'éléments de M close par ppcm à droite et engendrant M , alors tout élément non trivial de M admet une unique décomposition Σ -gloutonne stricte.*

EXEMPLE 4.4. Un cas classique auquel la proposition 4.3 s'applique, et qui a mené par extensions successives à la théorie dite de Garside [28], est celui du monoïde de tresses B_n^+ , et de la famille des diviseurs (à gauche et à droite) de l'élément Δ_n , qu'on appelle éléments simples de B_n^+ . Ceux-ci correspondent à des diagrammes positifs, eux aussi dits simples, définis par la propriété que deux brins quelconques se croisent au plus une fois. L'idée géométrique de la décomposition gloutonne telle qu'introduite dans [35] est de décomposer une tresse initiale en fragments simples quelconques, puis de remonter autant que faire se peut les croisements vers le début de la tresse tant qu'on ne crée pas de fragment non simple, voire la figure 2. Le passage à B_∞^+ est trivial : les éléments simples sont ceux qui divisent au moins un élément Δ_n , et ils sont caractérisés par la même propriété de croisement des brins dans les diagrammes. La proposition 4.3 s'applique, car le monoïde B_∞^+ a toutes les propriétés, et, par construction, le ppcm de deux tresses simples est simple.

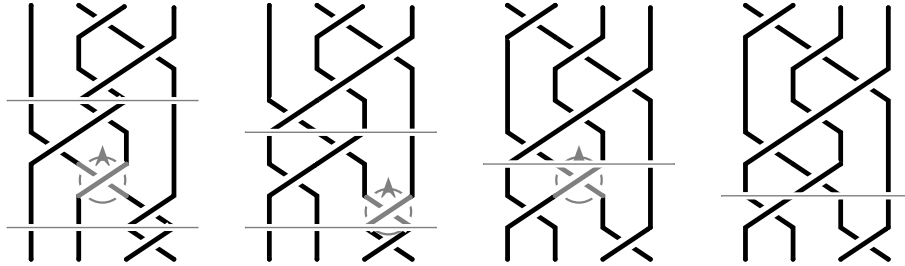


FIGURE 2. Décomposition gloutonne de la tresse $\sigma_2\sigma_3\sigma_2\sigma_2\sigma_1\sigma_2\sigma_3\sigma_3$ dans B_4^+ . On découpe d'abord en fragments simples maximaux, soit $\sigma_2\sigma_3\sigma_2|\sigma_2\sigma_1\sigma_2\sigma_3|\sigma_3$. Ensuite, on remonte les croisements tant que cela ne crée pas de fragment non simple, obtenant $\sigma_2\sigma_3\sigma_2\sigma_1|\sigma_2\sigma_1\sigma_3|\sigma_3$, $\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1|\sigma_2\sigma_1\sigma_3$, et enfin $\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_2|\sigma_1\sigma_3$ (qui n'a que deux fragments simples).

Comme expliqué dans la remarque 4.7 plus loin, les hypothèses de la proposition 4.3 ne sont pas exactement celles de la théorie de Garside classique, et nous devons faire une démonstration adaptée. On commence par un lemme de base (existence de la « tête ») :

LEMME 4.5. *Sous les hypothèses de la proposition 4.3, pour tout élément non trivial a de M , il existe un unique élément $a_1 \neq 1$ dans Σ vérifiant*

$$(4.6) \quad a_1 \preceq a \quad \text{et} \quad \forall s \in \Sigma (s \preceq a \Leftrightarrow s \preceq a_1).$$

DÉMONSTRATION. Soit a un élément non trivial de M . Posons

$$X := \{x \in M \mid \exists s \in \Sigma (s \neq 1 \text{ et } sx = a)\}.$$

L'hypothèse que Σ engendre M implique que a s'exprime comme produit non vide d'éléments de Σ distincts de 1, donc il existe au moins un élément s de Σ vérifiant $s \neq 1$ et $s \preceq a$, et, de là, l'ensemble X n'est pas vide. Alors, puisque M est noethérien à droite, il existe un élément \preceq -minimal a' dans X . Par définition, il existe alors (au moins) un élément a_1 de Σ vérifiant $a_1 a' = a$. On va montrer que a_1 vérifie (4.6).

D'abord, $a_1 \preceq a$ est vrai par construction, et, de là, $s \preceq a_1$ implique $s \preceq a$. Le problème est de montrer que, si s est dans Σ et vérifie $s \preceq a$, alors on a $s \preceq a_1$. Or soit s un tel élément. Par hypothèse, a est un multiple à droite commun pour a_1 et pour s , donc, puisque M admet des ppcm à droite conditionnels, $a_1 \vee s$ existe et, puisque Σ est clos par ppcm à droite, $a_1 \vee s$ appartient à Σ . Par ailleurs, puisque a_1 et s divisent à gauche a , il en est de même de $a_1 \vee s$. Il existe donc b vérifiant $a = (a_1 \vee s)b$, et b appartient à X . Utilisant $a_1 \setminus s$ pour le complément à droite de a_1 dans s , c'est-à-dire l'unique élément vérifiant $a_1 \vee s = a_1(a_1 \setminus s)$, on obtient

$$a_1 a' = a = (a_1 \vee s)b = a_1(a_1 \setminus s)b,$$

d'où $a' = (a_1 \setminus s)b$ en simplifiant a_1 à gauche. Ceci montre qu'on a $a' \approx b$. Or, le choix de a' interdit $a' \succ b$, et donc la seule possibilité est qu'on ait $a' = b$, donc, en simplifiant b à droite, $a_1 \setminus s = 1$, soit $s \preceq a_1$.

L'existence est donc établie. L'unicité est facile. Supposons que b_1 vérifie (4.6). Puisque b_1 est dans Σ et que a_1 satisfait (4.6), on déduit $b_1 \preceq a_1$. Symétriquement, puisque a_1 est dans Σ et que b_1 satisfait (4.6), on déduit $a_1 \preceq b_1$, d'où, finalement, $b_1 = a_1$. \square

REMARQUE 4.7. La démonstration ci-dessus est différente de la démonstration « standard » dont les hypothèses sont légèrement différentes. Pour le cas noethérien à droite, dans [28, section IV.2.2], par exemple, on n'a pas besoin de la simplifiabilité à droite, mais on considère des familles Σ closes par diviseur à droite. Ici, la simplifiabilité à droite est nécessaire pour conclure $s \preceq a_1$. Sans celle-ci, on pourrait simplement déduire $s \setminus a \approx a_1 \setminus a$. Le choix des hypothèses de la proposition (4.3) est dicté par les propriétés du monoïde H^+ auquel on va l'appliquer dans la section 4.2.

Une fois le lemme 4.5 établi, il est facile de compléter la construction de la décomposition gloutonne.

DÉMONSTRATION DE LA PROPOSITION 4.3. Soit a un élément quelconque de H^+ . Si a est trivial, la suite vide en est une décomposition Σ -gloutonne stricte. Supposons maintenant $a \neq 1$. Par le lemme 4.5, il existe $a_1 \neq 1$ et a' vérifiant $a = a_1 a'$ et

$$(4.8) \quad a_1 \in \Sigma \quad \text{et} \quad \forall s \in \Sigma (s \preceq a_1 a' \Leftrightarrow s \preceq a_1).$$

Si on a $a' = 1$, la suite (a_1) est une décomposition de a du type cherché. Sinon, on applique à a' la même construction : par le lemme 4.5, il existe $a_2 \neq 1$ et a'' vérifiant $a' = a_2 a''$, donc $a = a_1 a_2 a''$, et

$$(4.9) \quad a_2 \in \Sigma \quad \text{et} \quad \forall s \in \Sigma (s \preceq a_2 a'' \Leftrightarrow s \preceq a_2).$$

Si on a $a'' = 1$, la suite (a_1, a_2) est une décomposition de a du type cherché. Sinon, on recommence, construisant de proche en proche des éléments $a_i \neq 1$ et $a^{(i)}$ vérifiant $a = a_1 \cdots a_i a^{(i)}$ et

$$(4.10) \quad a_i \in \Sigma \quad \text{et} \quad \forall s \in \Sigma (s \preceq a_i a^{(i)} \Leftrightarrow s \preceq a_i).$$

Par construction, on a $a \succsim a' \succsim a'' \succsim \cdots \succsim a^{(i)}$ pour tout i tel que a_i est défini. L'hypothèse que M est noethérien à droite implique qu'il existe un entier p tel que la construction s'arrête après p étapes, c'est-à-dire qu'on a $a^{(p+1)} = 1$. Alors la suite (a_1, \dots, a_p) est, par construction, une décomposition de a qui est Σ -gloutonne stricte.

L'existence est donc démontrée. Pour l'unicité, supposons que (b_1, \dots, b_q) est une (autre) décomposition avec les mêmes propriétés. Quitte à ajouter des 1 additionnels à la plus courte (qui, du coup, n'est plus stricte), on peut supposer $p = q$. Par hypothèse, b_1 est dans Σ et on a $b_1 \preceq a$. Comme (a_1, \dots, a_p) satisfait (4.2), on a $b_1 \preceq a_1$. Par un argument symétrique, comme (b_1, \dots, b_p) satisfait (4.2), on a $a_1 \preceq b_1$, d'im finalement $a_1 = b_1$. Par simplifiabilité à gauche, on déduit, avec des notations évidentes, que (a_2, \dots, a_p) et (b_2, \dots, b_p) sont deux décompositions gloutonnes de $a' = b'$, et on recommence : formellement, on montre $\forall i \leq p (a_i = b_i)$ par induction sur p . \square

4.2. Le cas du monoïde H^+ . On va maintenant montrer que la construction de la section 4.1 s'applique au monoïde H^+ et à la famille Σ de ses éléments simples, et établir quelques propriétés des décompositions gloutonnes associées.

LEMME 4.11. *Le monoïde H^+ satisfait aux hypothèses de la proposition 4.3.*

DÉMONSTRATION. On a noté dès le chapitre I que H^+ est noethérien (à gauche et à droite), et ne possède pas d'élément inversible non trivial. Ensuite, on a montré au chapitre IV qu'il est simplifiable, à gauche et à droite (propositions IV.2.4 et IV.2.5), et qu'il admet des ppcm conditionnels à droite (proposition IV.2.6), ce qui complète la vérification. \square

LEMME 4.12. *La famille Σ des éléments simples du monoïde H^+ satisfait aux hypothèses de la proposition 4.3.*

DÉMONSTRATION. On sait que tous les atomes θ_i sont simples, donc la famille des éléments simples engendre le monoïde H^+ . Il reste à voir que Σ est close par ppcm à droite. Soient donc a et b deux éléments simples : par définition, il existe p et q vérifiant $a \preceq \Delta_p$ et $b \preceq \Delta_q$. Soit $n = \max(p, q)$. Alors Δ_n est un multiple à droite commun de Δ_p et Δ_q , donc de a et de b . Puisque H^+ admet des ppcm à droite conditionnels, il en résulte que $a \vee b$ existe, et qu'il divise Δ_n . Donc deux éléments simples ont toujours un ppcm à droite, et celui-ci est simple. \square

De ce qui précède et de la proposition 4.3, on déduit immédiatement :

PROPOSITION 4.13 (**décomposition gloutonne**). *Tout élément de H^+ admet une unique décomposition Σ -gloutonne stricte, c'est-à-dire une unique décomposition (a_1, \dots, a_p) avec a_1, \dots, a_p dans Σ satisfaisant $a_p \neq 1$ (dans le cas $a \neq 1$) et pour tout $1 \leq i \leq p-1$*

$$(4.14) \quad \forall s \in \Sigma (s \preceq a_i \cdots a_p \Leftrightarrow s \preceq a_i).$$

Détermination pratique. Comme dans le cas « Garside », l'intérêt des décompositions gloutonnes (comme de tout autre type de forme normale) dépend beaucoup de la possibilité de contrôler leurs propriétés et, en particulier, de les déterminer algorithmiquement. Pour ce dernier point, la question est de savoir déterminer à partir de a l'élément a_1 du lemme 4.5, auquel il est utile de donner un nom :

DÉFINITION 4.15 (**tête**). Sous les hypothèses du lemme 4.5, l'unique élément a_1 dont l'existence est affirmé est appelé la *tête* de a relativement à Σ , et notée $\mathbf{t}_\Sigma(a)$.

La démonstration de la proposition 4.3 montre que la détermination de la décomposition gloutonne est facile à partir de celle de la tête.

Sous les hypothèses de la proposition 4.3, le monoïde M admet des pgcd à gauche. De là, si la famille Σ considérée est la famille des diviseurs à gauche d'un élément Δ , on obtient immédiatement l'égalité

$$(4.16) \quad \mathbf{t}_\Sigma(a) = a \wedge \Delta,$$

(où on rappelle que \wedge dénote le pgcd à gauche), et tout dépend alors de la possibilité de calculer efficacement l'opération \wedge .

EXEMPLE 4.17. Dans le cas du monoïde de tresses B_n^+ et de l'élément Δ_n , un tel algorithme efficace existe [36, chapitre IX]. Plus généralement, dans le cas d'une présentation complétée à gauche et à droite pour laquelle les deux retournements sont complets, le calcul du pgcd est facile par un triple retournement [20].

Dans le cas du monoïde B_∞^+ , la famille Σ des éléments simples considérée dans l'exemple 4.4 n'est pas la famille des diviseurs d'un unique élément Δ , mais on a toujours une relation simple avec les éléments Δ_n : une tresse est simple si, et seulement si, elle divise à gauche la tresse Δ_n où n est le plus petit indice tel que a appartienne à B_n^+ . La formule (4.16) n'est plus valide, mais on a une formule semblable

$$(4.18) \quad \mathbf{t}_\Sigma(a) = a \wedge \Delta_{\mathbf{ht}(a)+1},$$

en notant, sur le modèle de ce qui a été fait pour H^+ au chapitre I, $\mathbf{ht}(a)$ le maximum des indices des lettres σ_i figurant dans une expression de a .

Dans le cas du monoïde H^+ , qui admet lui aussi des pgcd à gauche, le résultat est analogue au cas de B_∞^+ , à condition d'utiliser cette fois le plafond :

LEMME 4.19. *Pour tout élément a de H^+ , on a*

$$(4.20) \quad \mathfrak{t}_\Sigma(a) = a \wedge \Delta_{[a]+1},$$

DÉMONSTRATION. Soit a quelconque dans H^+ , et soit $a_1 := \mathfrak{t}_\Sigma(a)$. Par construction, on a $a_1 \preceq a$, donc $[a_1] \leq [a]$ par le corollaire I.3.22. D'autre part, puisque a_1 est simple, le lemme 3.1 implique $a_1 \preceq \Delta_{[a_1]+1}$, donc, *a fortiori*, $a_1 \preceq \Delta_{[a]+1}$, et, de là, $a_1 \preceq a \wedge \Delta_{[a]+1}$. Inversement, $a \wedge \Delta_{[a]+1}$ est simple et, par construction, il divise a , donc on a $a \wedge \Delta_{[a]+1} \preceq a_1$, d'où (4.20). \square

Il en résulte que la fonction « tête » est calculable dans le cas de H^+ et Σ . Par contre, comme le retournement à gauche n'est pas complet, il n'existe pas d'algorithme très efficace pour calculer un pgcd à gauche dans H^+ . Une méthode pour déterminer un pgcd $a \wedge b$ dans H^+ consiste à tester (par retournement à droite) chacune des relations $\theta_i \preceq a$ et $\theta_i \preceq b$ pour $i \leq \max([a], [b])$: si $a \wedge b$ n'est pas 1, il est divisible par au moins un tel atome θ_i , puisque $\theta_i \preceq a$ implique $i = [\theta_i] \leq [a]$. Si on trouve un tel θ_i divisant à la fois a et b , on pose $a' := \theta_i \setminus a$ et $b' := \theta_i \setminus b$, et on recommence avec a' et b' . Au bout d'au plus $\max(|a|, |b|)$ itérations, le pgcd de a et b est identifié. (Au moins théoriquement, cette méthode est plus efficace qu'une énumération exhaustive de tous les diviseurs de a et b .)

EXEMPLE 4.21. Soit $a := \theta_3\theta_2\theta_4\theta_6$. Pour déterminer la décomposition gloutonne de a , on cherche la tête $a_1 := \mathfrak{t}_\Sigma(a)$. Le plafond de a est 6, et on a donc $a_1 = a \wedge \Delta_7$. Il est évident que θ_3 divise a , et Δ_7 . On recommence avec les quotients, et finalement on trouve

$$a_1 = \theta_3\theta_2, \quad \text{d'où} \quad a' = \theta_4\theta_6.$$

On cherche donc la nouvelle tête $a_2 := \mathfrak{t}_\Sigma(a')$. Le plafond de a' est 6 à nouveau, et on a donc $a_2 = a' \wedge \Delta_7$. Ici on obtient l'égalité $a' \wedge \Delta_7 = \theta_4$, d'où

$$a_2 = \theta_4, \quad \text{d'où} \quad a'' = \theta_6.$$

Comme a'' est simple, on a terminé, et la décomposition Σ -gloutonne de a est la suite $(\theta_3\theta_2, \theta_4, \theta_6)$, de longueur 3.

EXEMPLE 4.22. Considérons maintenant $a := \theta_7\theta_6\theta_3\theta_5\theta_1$. Le plafond de a est 12, et on a donc $a_1 = a \wedge \Delta_{12}$. On trouve cette fois

$$a_1 = \theta_7\theta_6\theta_3\theta_1, \quad \text{d'où} \quad a' = \theta_6.$$

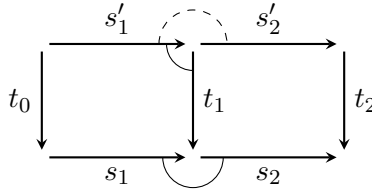
Comme a' est un atome, on a terminé, et la décomposition Σ -gloutonne de a est la suite $(\theta_7\theta_6\theta_3\theta_1, \theta_6)$, de longueur 2.

La règle du domino. Ce qui explique en grande partie l'efficacité (à la fois théorique et pratique) des décompositions gloutonnes dans le cas des monoïdes de tresses et, plus généralement, des familles de Garside est l'existence d'une procédure très simple déterminant, quand s est un élément de la famille Σ considérée, la décomposition Σ -gloutonne de sa à partir de celle

de a . La validité de la procédure repose sur ce qui a été appelé la *règle du domino* pour Σ [28, proposition III.1.45], affirmant que, si deux suites d'éléments de Σ de longueur 2 sont normales, alors une troisième l'est aussi :

DÉFINITION 4.23 (règle du domino). Sous les hypothèses de la proposition 4.3, on dit que la *règle du domino* est valide pour Σ si, toutes les fois que $s_1, s_2, s'_1, s'_2, t_0, t_1$, et t_2 sont dans Σ , qu'on a $t_0s_1 = s'_1t_1$ et $t_1s_2 = s'_2t_2$, et que (s_1, s_2) et (s'_1, t_1) sont Σ -gloutonnes, il en est de même de (s'_1, s'_2) .

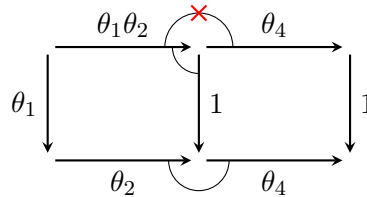
La règle du domino est satisfaite dans le contexte de toute famille de Garside, donc en particulier pour les décompositions gloutonnes dans B_∞^+ , et elle y joue un rôle fondamental. Il est commode de l'illustrer par un diagramme où on associe une flèche à chaque élément, où les diagrammes commutatifs indiquent des égalités de produits, et où on relie deux flèches par un arc quand elles sont associées à une suite gloutonne. Alors la règle du domino pour Σ correspond au diagramme



illustrant le fait que, si (s_1, s_2) et (s'_1, t_1) sont gloutonnes (deux petits arcs en trait plein), alors il en est de même de (s'_1, s'_2) (petit arc en pointillé).

FAIT 4.24. *La règle du domino n'est pas valide pour la famille des éléments simples de H^+ .*

DÉMONSTRATION. Dans H^+ , l'élément $\theta_1\theta_2$ est simple, de même que l'unité 1 et chacun des atomes. Or, on a $\theta_1 \cdot \theta_2 = \theta_1\theta_2 \cdot 1$ et $1 \cdot \theta_4 = \theta_4 \cdot 1$, et, d'autre part, les suites (θ_2, θ_4) et $(\theta_1\theta_2, 1)$ sont gloutonnes, et, pourtant, la suite $(\theta_1\theta_2, \theta_4)$ n'est pas gloutonne : $\theta_1\theta_2\theta_4$ est simple, sa tête est lui-même, et la décomposition gloutonne de $\theta_1\theta_2\theta_4$ étant (Δ_3) , donc $(\Delta_3, 1)$ est gloutonne au sens large.



Le diagramme ci-dessus illustre ce contre-exemple. □

Décomposition gloutonne et forme normale. Une question naturelle est de savoir si on peut lire la décomposition Σ -gloutonne sur la forme normale définie au chapitre II : la tête d'un élément a est une sorte de préfixe maximal de a qui soit simple, et il est naturel de se demander si $\text{NF}(t_\Sigma(a))$ peut se

lire comme le préfixe maximal de $\text{NF}(a)$ qui soit forme normale d'un élément simple, c'est-à-dire, par la proposition 3.24, qui évite \mathcal{I}_Σ .

Dans le même état d'esprit, on peut se demander si, supposant que la décomposition Σ -gloutonne de a est la suite (a_1, \dots, a_p) , le mot $\text{NF}(a)$ est la concaténation des mots $\text{NF}(a_1), \dots, \text{NF}(a_p)$.

Comme le montre le contre-exemple suivant, la réponse à ces deux questions est négative.

EXEMPLE 4.25. Reprenons $a = \theta_7\theta_6\theta_3\theta_5\theta_1$, comme dans l'exemple 4.22. Dans ce cas, on a $\text{NF}(a) = \theta_7\theta_6\theta_3\theta_5\theta_1 (= a)$, et le préfixe maximal évitant \mathcal{I}_Σ est $\theta_7\theta_6\theta_3$. D'un autre côté, on a vu que la décomposition Σ -gloutonne de a est $(\theta_7\theta_6\theta_3\theta_1, \theta_5)$, et on a $\text{NF}(\theta_7\theta_6\theta_3\theta_1) = \theta_7\theta_6\theta_3\theta_1 \neq \theta_7\theta_6\theta_3$. Donc la forme normale de la tête n'est pas nécessairement le plus grand préfixe de la forme normale qui soit une forme normale d'élément de Σ .

D'autre part, dans ce même cas, on a

$$\text{NF}(a) = \theta_7\theta_6\theta_3\theta_5\theta_1 \neq \text{NF}(a_1)\text{NF}(a_2) = \theta_7\theta_6\theta_3\theta_1\theta_5 :$$

la forme normale de a n'est pas nécessairement la concaténation des formes normales des éléments de sa décomposition Σ -gloutonne.

Conclusion. Les contre-exemples ci-dessus suggèrent que les décompositions Σ -gloutonnes ne sont guère compatibles avec la forme normale du chapitre II. Bien sûr, on pourrait contourner le problème en considérant une forme normale mixte définie, pour a dans H^+ de décomposition Σ -gloutonne (a_1, \dots, a_p) , par

$$(4.26) \quad \text{NF}_{\text{mix}}(a) := \text{NF}(a_1)\text{NF}(a_2) \cdots \text{NF}(a_p),$$

mais rien n'indique qu'une telle forme normale — certes calculable effectivement — ait de bonnes propriétés.

Au-delà, le défaut de la règle du domino est le signe que les décompositions Σ -gloutonnes de H^+ restent très en-deçà de celles du cas d'une famille de Garside : ce qui empêche les éléments simples de H^+ de former une famille de Garside est qu'ils ne sont pas clos par diviseur à droite : le diviseur à droite $\theta_2\theta_4$ de l'élément simple Δ_3 n'est *pas* simple — et cela suffit à faire toute la différence. À nouveau, on pourrait contourner l'obstacle en remplaçant la famille Σ par sa clôture $\widehat{\Sigma}$ par diviseur à droite et ppcm à droite, qui, elle, est une famille de Garside et donne donc lieu à des décompositions $\widehat{\Sigma}$ -gloutonnes ayant toutes les propriétés attendues. Mais, au moins pour le moment, on n'a aucune description effective ni aucun contrôle de cette clôture $\widehat{\Sigma}$, qui reste purement théorique : il se pourrait très bien que $\widehat{\Sigma}$ soit H^+ entier, auquel cas, la décomposition $\widehat{\Sigma}$ -gloutonne d'un élément a quelconque serait la suite (a) , évidemment sans aucun intérêt.

Suite et fin...

Toute une série de résultats algébriques sur le monoïde H^+ ont été démontrés dans les chapitres précédents à partir de l'étude directe de ses éléments via les mots qui les représentent, parfois au prix de démonstrations difficiles, comme dans le chapitre V. Dans ce dernier chapitre, on regroupe des observations supplémentaires, principalement sur les représentations du monoïde H^+ , et une liste de questions laissées ouvertes et appelant une suite à ce travail.

Le chapitre est organisé en deux sections. Dans la section 1, on étudie les représentations du monoïde H^+ . On montre l'existence d'une obstruction à une représentation géométrique par le biais des monoïdes \widehat{V}^+ ou \widehat{BV}^+ avec des classes d'isotopie de diagrammes comme pour B_∞^+ et F^+ . De ce fait, on explore les représentations fonctionnelles, en particulier linéaires, et on décrit plusieurs familles explicites. Certaines de ces représentations sont non fidèles, mais, pour l'une d'entre elles, les expériences systématiques par ordinateur n'ont pas trouvé de contre-exemple et on conjecture qu'elle est fidèle. Dans la section 2, on conclut en regroupant diverses questions ouvertes issues des approches développées dans les divers chapitres, et on mentionne quelques pistes de recherche. L'un des principaux problèmes ouverts est la question de savoir si le monoïde H^+ se plonge dans un groupe et, plus généralement, d'étudier le groupe H défini par la présentation (\mathcal{P}) de H^+ .

1. Les représentations du monoïde H^+

Une façon usuelle d'étudier un (semi)-groupe est de chercher ses représentations dans d'autres structures, typiquement des groupes linéaires. L'étude des représentations du monoïde H^+ est un problème naturel, dont on peut espérer qu'il éclaire certaines des questions laissées ouvertes, (voir la section 2). À ce jour, aucune représentation fidèle (c'est-à-dire injective) n'a été trouvée, mais on présente ci-dessous plusieurs observations, certaines un peu inattendues et exotiques, et on établit divers résultats partiels.

La section est divisée en trois parties. Dans la section 1.1, on fixe un cadre général pour une notion de représentation géométrique de H^+ , dont un exemple est la représentation Φ_F par la projection sur (la représentation géométrique) du monoïde F^+ , et de représentation fonctionnelle, c'est-à-dire à valeurs dans un espace de fonctions. Dans la section 1.2, on étudie une telle représentation fonctionnelle Φ_S , dont on montre qu'elle n'est pas fidèle, mais pas non plus factorisable par Φ_F , et on montre qu'il semble difficile d'en

donner une description géométrique. Dans la section 1.3, on décrit plusieurs familles de représentations linéaires explicites généralisant Φ_F et Φ_S , et on conjecture qu'au moins l'une d'entre elles, $\Phi_{1,t}$, est fidèle.

1.1. Représentations géométriques et fonctionnelles. On appellera ici *représentation* d'un monoïde M tout homomorphisme Φ de M dans un monoïde M' , et on la qualifiera de *fidèle* si Φ est injectif, auquel cas l'image de Φ est une *réalisation* de M . On va considérer ici deux types particuliers de représentations, dites géométriques et fonctionnelles.

On a vu dans la section I.2 comment associer des diagrammes de tresses, de permutations, et de forêts aux éléments des groupes B_∞ , \mathfrak{S}_∞ , et F , et aux monoïdes correspondants, de sorte que les diagrammes soient isotopes si, et seulement si, les mots qui les décrivent représentent le même élément du groupe ou du monoïde. Le cadre général de telles constructions peut être défini (informellement) comme suit :

DÉFINITION 1.1 (représentation géométrique). Une représentation d'un monoïde $\langle S \mid R \rangle^+$ est dite *géométrique (via S)* si elle est induite par une application Φ de S^* dans un ensemble de diagrammes telle que

$$(1.2) \quad w \equiv_R w' \quad \text{implique} \quad \Phi(w) \sim \Phi(w'),$$

où \sim est une notion d'isotopie adaptée à préciser.

Dans le contexte ci-dessus, la représentation de M obtenue est fidèle si, et seulement si, (1.2) est une équivalence.

De la sorte, la proposition I.2.1 et le fait que B_n^+ est le sous-monoïde de B_n engendré par les σ_i fournissent une représentation géométrique fidèle du monoïde de tresses B_n^+ par des diagrammes de tresses positives et, de la même façon, la proposition I.2.7 et le fait que F^+ est le sous-monoïde de F engendré par les a_i fournissent une représentation géométrique fidèle du monoïde F^+ par des diagrammes de forêts (familles d'arbres). Enfin, les résultats de [11] et [24] fournissent une représentation géométrique fidèle des monoïdes \widehat{BV}^+ et \widehat{V}^+ par des diagrammes « tresses plus bifurcations » et « transpositions plus bifurcations ».

Comme, par la proposition I.3.26, l'application $\pi : \theta_i \mapsto a_i$ définit un homomorphisme surjectif de H^+ sur F^+ , on en déduit immédiatement une représentation géométrique de H^+ :

PROPOSITION 1.3 (représentation Φ_F). *Soit $\Phi_F := \Phi_{\text{for}} \circ \pi$, où Φ_{for} est la réalisation de monoïde F^+ par diagramme de forêts. Alors Φ_F est une représentation géométrique de H^+ . Elle n'est pas fidèle.*

DÉMONSTRATION. Le fait que π soit un homomorphisme signifie que, pour tous Θ -mots w, w' , la relation $w \equiv w'$ entraîne $\pi(w) \equiv_F \pi(w')$, d'où $\Phi_{\text{for}}(\pi(w)) \sim \Phi_{\text{for}}(\pi(w')) : \Phi_F$ est une représentation de H^+ .

Mais cette représentation ne peut être fidèle puisque π n'est pas injective : on sait que, dans F^+ , on a $a_2 a_1 = a_1 a_3$, alors que, dans H^+ , on n'a pas

$\theta_2\theta_1 = \theta_1\theta_3$, et donc les diagrammes isotopes de la figure 1 sont associés à des éléments distincts de H^+ . \square



FIGURE 1. La représentation géométrique de H^+ par diagramme de forêts n'est pas fidèle : les diagrammes pour $\theta_2\theta_1$ et $\theta_1\theta_3$ sont isotopes en tout sens raisonnable, alors que les mots $\theta_2\theta_1$ et $\theta_1\theta_3$ ne représentent pas le même élément de H^+ .

À côté des représentations précédentes, on considérera aussi des représentations par des fonctions, suivant le cadre général suivant :

DÉFINITION 1.4 (représentations fonctionnelle et linéaire). Une représentation Φ d'un monoïde M est dite *fonctionnelle* s'il existe un ensemble \mathcal{X} tel que le but de Φ est le monoïde des fonctions de \mathcal{X} dans \mathcal{X} muni de la composition ; Φ est dite *linéaire* si, de plus, \mathcal{X} est un k -module et que le but de Φ est inclus dans les applications k -linéaires de \mathcal{X} .

En pratique, on considérera dans toute la suite des représentations fonctionnelles où le domaine \mathcal{X} est un ensemble de suites $X^{\mathbb{N}}$. Par défaut, on utilise x_i comme notation pour le i -ème terme d'une suite notée \vec{x} . D'autre part, pour obtenir une présentation par diagramme compatible avec celle des tresses et des forêts, il est commode de décrire l'action comme une action à droite, donc à utiliser la composition inversée, notée \bullet , et non la composition \circ . Pour un monoïde présenté $\langle S \mid R \rangle^+$, se donner une telle représentation Φ consiste, pour chaque élément s de S , à se donner une application $\Phi(s) : X^{\mathbb{N}} \rightarrow X^{\mathbb{N}}$, étendre Φ à S^* par $\Phi(s_1 \cdots s_\ell) := \Phi(s_1) \bullet \cdots \bullet \Phi(s_\ell)$, et vérifier que

$$(1.5) \quad w \equiv_R w' \quad \text{implique} \quad \forall \vec{x} \in X^{\mathbb{N}} (\Phi(w)(\vec{x}) = \Phi(w')(\vec{x})).$$

(On utilisera toujours ici la même notation pour l'application sur les mots et pour la représentation qu'elle induit éventuellement sur le monoïde associé.) Comme dans le cas géométrique, Φ est fidèle si, et seulement si, (1.5) est une équivalence.

En pratique, on ne considérera que des représentations locales, au sens où la valeur du i -ème terme $\Phi(s)(\vec{x})_i$ ne dépend que des valeurs de x_j pour j dans un (petit) voisinage de i . De plus, pour le cas du monoïde H^+ , qui possède une invariance par décalage à droite, il est raisonnable de considérer des représentations avec la même invariance :

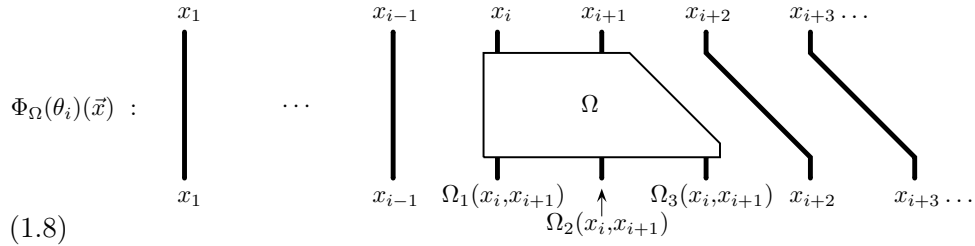
DÉFINITION 1.6 (représentation spéciale). Pour $\Omega = (\Omega_1, \Omega_2, \Omega_3) : X^2 \rightarrow X^3$, on dit qu'une représentation Φ de H^+ est *spéciale de graine Ω* si,

pour tout $i \geq 1$, on a

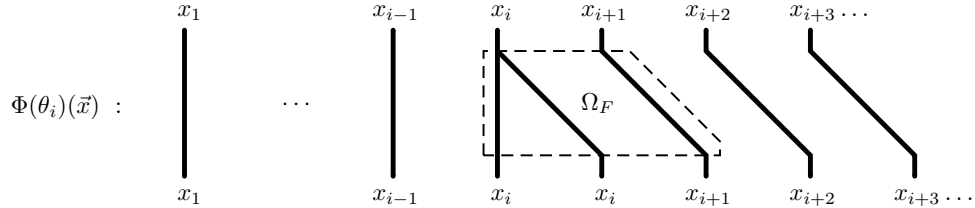
$$(1.7) \quad \Phi(\theta_i)(\vec{x})_k := \begin{cases} x_k & \text{pour } 1 \leq k < i, \\ \Omega_{k-i+1}(x_i, x_{i+1}) & \text{pour } k = i, i+1, i+2, \\ x_{k-1} & \text{pour } k \geq i+3. \end{cases}$$

La représentation spéciale associée à la graine Ω est notée Φ_Ω ; si Ω est linéaire de matrice A , on la note Φ_A .

Le principe est donc le suivant : l'image du générateur θ_i est l'application de $X^\mathbb{N}$ dans lui-même consistant à appliquer Ω aux positions initiales i et $i+1$, et à décaler les termes à partir de la position $i+2$ d'un cran vers la droite, suivant le schéma



EXEMPLE 1.9. La représentation Φ_F fournit une représentation spéciale évidente : si on voit les valeurs x_i comme des étiquettes attachées aux brins d'un diagramme, alors il est naturel de mettre dans la boîte Ω le diagramme de bifurcation associé à a_i , c'est-à-dire à considérer la définition



qui est la représentation spéciale de graine définie par $\Omega_F(x, y) := (x, x, y)$, laquelle est linéaire de matrice $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. La représentation $\Phi_{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}$ revient à indiquer, pour chaque position du bas du diagramme, son origine dans le haut du diagramme, exactement comme la permutation d'une tresse indique les origines des brins dans un diagramme. Noter que $\Phi_{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}$, qui donc est facteur de Φ_F , perd de l'information par rapport à Φ_F : par exemple, elle ne sépare pas θ_1^2 et $\theta_1\theta_2$, alors que Φ_F le fait.

L'intérêt de considérer les représentations spéciales de H^+ tient au fait suivant, qui rendra leur identification facile dans la suite :

LEMME 1.10. Une fonction $\Omega : X^2 \rightarrow X^3$ définit une représentation du monoïde H^+ si, et seulement si, on a

$$(1.11) \quad \Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_k = \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_k \quad \text{pour } 1 \leq k \leq 6.$$

DÉMONSTRATION. Le caractère local de Φ_Ω garantit les relations de type 2 : pour $j \geq i + 2$, on trouve

$$\Phi_\Omega(\theta_j\theta_i)(\vec{x})_k = \Phi_\Omega(\theta_i\theta_{j+1})(\vec{x})_k = \begin{cases} x_k & \text{pour } k < i, \\ \Omega_{k-i+1}(x_i, x_{i+1}) & \text{pour } i \leq k \leq i + 2, \\ x_{k-1} & \text{pour } i + 3 \leq k < j, \\ \Omega_{k-j}(x_j, x_{j+1}) & \text{pour } j + 1 \leq k \leq j + 3, \\ x_{k-2} & \text{pour } j + 4 \leq k. \end{cases}$$

Pour la relation $\theta_2\theta_1\theta_2 = \theta_1\theta_2\theta_4$, un dessin montre immédiatement qu'il suffit de vérifier l'égalité pour $k \leq 6$, puisque, pour $k \geq 7$, on a simplement

$$\Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_k = \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_k = x_{k-3}.$$

Enfin, l'invariance par décalage, c'est-à-dire par translation à droite, entraîne que, dès que $\Phi_\Omega(\theta_2\theta_1\theta_2) = \Phi_\Omega(\theta_1\theta_2\theta_4)$ est vraie, il en est de même de $\Phi_\Omega(\theta_{i+1}\theta_i\theta_{i+1}) = \Phi_\Omega(\theta_i\theta_{i+1}\theta_{i+3})$ pour tout i . \square

1.2. La représentation Φ_S . L'intérêt de l'approche ci-dessus est qu'il existe d'autres représentations spéciales de H^+ que celle de l'exemple 1.9.

PROPOSITION 1.12 (**représentation Φ_S**). *Posons $S := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.*

Alors Φ_S définit une représentation de H^+ , qui n'est pas fidèle, mais n'admet pas Φ_F comme facteur.

Avant de démontrer la proposition 1.12 (qui est facile), on observe que, dans des cas comme ceux de Φ_F ou de Φ_S , une représentation générale dans un espace de suites $X^{\mathbb{N}}$ ne donne pas plus d'information que sa spécialisation en la suite particulière $(1, 2, \dots)$, ce qui permettra d'alléger les notations.

LEMME 1.13. *Soit \mathcal{F}_∞ le monoïde des applications de $\mathbb{N}_{>0}$ dans $\mathbb{N}_{>0}$. Supposons que $\Omega : X^2 \rightarrow X^3$ vérifie $\Omega(x, y) \in \{x, y\}^3$. Alors il existe un morphisme ϕ_Ω de Θ^* dans \mathcal{F}_∞ tel que, pour tout mot w et pour tout k , on a*

$$(1.14) \quad \Phi_\Omega(w)(\vec{x})_k = x_{\phi_\Omega(w)(k)}.$$

De plus, on a $\phi_\Omega(w)(k) = k - |w|$ pour k assez grand. Enfin, Φ_Ω induit une représentation de H^+ si, et seulement si, ϕ_Ω le fait.

DÉMONSTRATION. On montre l'existence de ϕ_Ω par induction sur $|w|$. Pour $w = \varepsilon$, (1.14) est vérifiée en prenant pour $\phi_\Omega(w)$ la fonction identité de \mathbb{N} . Supposons $w = v\theta_i$. Par définition, on a $\Phi_\Omega(w) = \Phi_\Omega(v) \bullet \Phi_\Omega(\theta_i)$, donc $\Phi_\Omega(w)(\vec{x})$ s'obtient en appliquant $\Phi_\Omega(\theta_i)$ à la suite $\Phi_\Omega(v)(\vec{x})$. Par hypothèse de récurrence, celle-ci est $x_{g(1)}, x_{g(2)}, \dots$ où g est $\phi_\Omega(v)$. Appliquer $\Phi_\Omega(\theta_i)$ à une telle suite signifie garder les $i - 1$ premiers termes, puis appliquer Ω , donc remplacer deux termes de la forme x_p, x_q par trois termes de même forme, puis recopier les termes en décalant les indices d'une unité à gauche, donc $\Phi_\Omega(w)(\vec{x})$ a la forme annoncée avec $\phi_\Omega(w) := \phi_\Omega(v) \bullet \phi_\Omega(\theta_i)$.

D'autre part, par hypothèse d'induction, $\phi_\Omega(v)$ est ultimement un décalage de $|v|$ crans vers la gauche. Sa composée par $\phi_\Omega(\theta_i)$ est donc ultimement un décalage de $|v| + 1$, soit $|w|$, crans vers la gauche.

Enfin, il est clair que Φ_Ω est invariant par les relations de (\mathcal{P}) si, et seulement si, ϕ_Ω l'est, puisque, pour tout Θ -mot w , l'application $\phi_\Omega(w)$ détermine entièrement l'application $\Phi_\Omega(w)$. \square

Le lemme dit simplement que, quand Ω se borne à choisir comme valeurs de sortie une des deux valeurs d'entrée, alors, pour tout Θ -mot w , l'image par $\Phi_\Omega(w)$ d'une suite (x_1, x_2, \dots) est de la forme $(x_{\phi_\Omega(w)(1)}, x_{\phi_\Omega(w)(2)}, \dots)$, toute l'information étant dans la fonction $\phi_\Omega(w)$ qui décrit l'action sur les indices. De là, au lieu de considérer des suites (x_1, x_2, \dots) quelconques, il suffit de considérer les indices, ce qui revient à ne considérer que l'image de l'unique suite d'entiers $(1, 2, \dots)$.

EXEMPLE 1.15. Pour Ω_F , on a $\Omega_F(x, y) = (x, x, y)$, et la fonction $\phi_F(w)$ associée est celle qui décrit, pour chaque position k , l'origine du brin qui finit en position k dans le diagramme de bifurcation associé à w . La fonction $\phi_F(\theta_1)$ envoie 1 sur 1, puis k sur $k - 1$ pour $k \geq 2$ et, plus généralement, $\phi_F(\theta_i)$ est l'identité pour $k < i$, puis un décalage de -1 pour $k \geq i + 1$.

Il sera commode d'utiliser une notation compacte pour les fonctions f sur $\mathbb{N}_{>0}$ qui sont ultimement des décalages, c'est-à-dire telles qu'il existe deux entiers N, d pour lesquels on a $f(k) = k - d$ pour $k > N$.

NOTATION 1.16 (**fonction** $[i_1, \dots, i_N]_d$). Pour i_1, \dots, i_N et d dans \mathbb{N} , on note $[i_1, \dots, i_N]_d$ la fonction de $\mathbb{N}_{>0}$ dans lui-même définie par

$$f(k) := i_k \text{ pour } 1 \leq k \leq N, \quad \text{et } f(k) := k - d \text{ pour } k > N.$$

Par exemple, avec cette notation, on a $\phi_F(\theta_i) = [1, 2, \dots, i]_1$ pour la fonction de l'exemple 1.15. On revient maintenant à Φ_S .

DÉMONSTRATION DE LA PROPOSITION 1.12. On est dans le cadre du lemme 1.13, avec cette fois $\Omega(x, y) := (x, y, x)$. Avec la notation 1.16, on a $\phi_S(\theta_1) = [1, 2, 1]_1$. Suivant le lemme 1.10, pour établir que Φ_S est une représentation de H^+ , il suffit de comparer les six premières valeurs de $\Phi_S(\theta_2\theta_1\theta_2)$ et $\Phi_S(\theta_1\theta_2\theta_4)$, donc, par le lemme 1.13, de $\phi_S(\theta_2\theta_1\theta_2)$ et $\phi_S(\theta_1\theta_2\theta_4)$. Or, on obtient dans ce cas

$$(1.17) \quad \phi_S(\theta_2\theta_1\theta_2) = \phi_S(\theta_1\theta_2\theta_4) = [1, 2, 1, 2, 3, 2]_3.$$

Donc Φ_S est une représentation (spéciale) du monoïde H^+ .

Ensuite, Φ_S n'est pas fidèle. Par un calcul explicite direct, on peut établir, pour tout $i \geq 1$,

$$(1.18) \quad \Phi_S(\theta_i^2\theta_{i+1}) = \Phi_S(\theta_i\theta_{i+1}\theta_{i+2}).$$

En effet, on obtient

$$\phi_S(\theta_1^2\theta_2) = \phi_S(\theta_1\theta_2\theta_3) = [1, 2, 1, 2, 1]_3,$$

au regard de $\overline{\theta_2\theta_1}\overline{\theta_1\theta_1}\theta_2\theta_3 \curvearrowright \theta_4\theta_5\overline{\theta_2\theta_1} \neq \varepsilon$, qui établit $\theta_1^2\theta_2 \neq \theta_1\theta_2\theta_3$ dans H^+ . Les autres cas sont semblables.

Enfin, la représentation Φ_S ne se factorise pas par Φ_F : en effet, on obtient

$$\phi_S(\theta_2\theta_1) = [1, 2, 1, 3, 2]_2 \neq \phi_S(\theta_1\theta_3) = [1, 2, 1, 3, 1]_2 :$$

ϕ_S , donc aussi Φ_S , sépare des éléments que Φ_F ne sépare pas. □

Géométrisation de Φ_S . Par sa définition dans la proposition 1.12, la représentation Φ_S est fonctionnelle, mais n'est pas géométrique. Il est facile d'en donner une version diagrammatique. Pour cela, on peut associer à une application f de $\mathbb{N}_{>0}$ dans lui-même un diagramme en bâtons joignant chaque valeur k à la valeur $f(k)$, sur le modèle de

$$(1.19) \quad \theta_i : \begin{array}{ccccccc} & 1 & 2 & & i & i+1 & i+2 \\ & | & | & \cdots & | & \diagdown & \diagdown \\ & & & & & \diagup & \diagup \end{array} \cdots$$

Ce qui précède ne suffit pas à faire de Φ_S une représentation géométrique au sens de la définition 1.1 tant qu'on ne spécifie pas une notion d'isotopie pour les diagrammes. Or, on remarque que le diagramme ci-dessus peut être vu (de haut en bas) comme un diagramme de bifurcation, comme dans le cas de F^+ , suivi d'un diagramme de permutation, comme dans le cas de \mathfrak{S}_∞ :

$$\theta_i \left\{ \begin{array}{ccccccc} & 1 & 2 & & i & i+1 & i+2 \\ a_i & | & | & \cdots & | & \diagdown & \diagdown \\ s_{i+1} & | & | & \cdots & | & \diagup & \diagup \end{array} \right. \cdots$$

Il est donc naturel d'interpréter θ_i par un diagramme associant bifurcations et permutations, donc un diagramme pour un élément du groupe \widehat{V} défini par la présentation (I.2.18) dans la section I.2.3 et, de là, d'espérer obtenir une représentation (géométrique) via le monoïde \widehat{V}^+ . Malheureusement, cette approche qui semble séduisante *ne fonctionne pas* :

FAIT 1.20. *Le morphisme $\Phi_{\widehat{V}} : \Theta^* \rightarrow \widehat{V}^+$ défini par*

$$(1.21) \quad \Phi_{\widehat{V}}(\theta_i) := a_i s_{i+1}$$

n'induit pas de représentation de H^+ dans le monoïde \widehat{V}^+ , ni dans le groupe \widehat{V} .

DÉMONSTRATION. On compare les représentations des mots $\theta_2\theta_1\theta_2$ et de $\theta_1\theta_2\theta_4$ dans \widehat{V}^+ , à savoir les éléments $a_2s_3a_1s_2a_1s_2$ et $a_1s_2a_2s_3a_4s_5$. Étant donnée la structure de \widehat{V}^+ comme produit de Zappa-Szép de F^+ et \mathfrak{S}_∞ , les relations de la présentation doivent permettre de faire passer tous les générateurs s_i à droite. De fait, on vérifie facilement

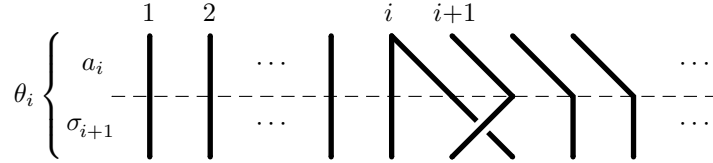
$$a_2s_3a_1s_2a_1s_2 \equiv_{\widehat{V}} a_2^2a_1s_3s_5 \quad \text{et} \quad a_1s_2a_2s_3a_4s_5 \equiv_{\widehat{V}} a_2a_3a_1s_3s_5.$$

Or, on n'a $a_2^2 a_1 = a_2 a_3 a_1$ ni dans le monoïde F^+ , ni donc dans le monoïde \widehat{V}^+ , la raison géométrique étant illustrée dans la figure 2. Les monoïdes considérés se plongeant dans les groupes correspondants, on a le même résultat négatif pour F ou \widehat{V} . \square



FIGURE 2. Dans les diagrammes pour a_2^2 et pour $a_2 a_3$, le brin 2 bifurque deux fois, mais avec des brins médians venant de la branche gauche dans a_2^2 (à gauche) et de la branche droite dans $a_2 a_3$ (à droite), donc non équivalents sauf à écraser l'ordre des bifurcations et obtenir une notion d'isotopie triviale.

Puisque le monoïde \widehat{V}^+ est une projection du monoïde \widehat{BV}^+ , le même résultat négatif vaut *a fortiori* quand on essaie de représenter H^+ dans \widehat{BV}^+ par la décomposition



FAIT 1.22. Le morphisme $\Phi_{\widehat{BV}} : \Theta^* \rightarrow \widehat{BV}^+$ défini par

$$(1.23) \quad \Phi_{\widehat{BV}}(\theta_i) := a_i \sigma_{i+1}$$

n'induit pas de représentation de H^+ dans le monoïde \widehat{BV}^+ , ni dans le groupe \widehat{BV} .

La question de donner un contenu géométrique à la représentation Φ_S (qui semble assez mystérieuse et artificielle) reste donc ouverte.

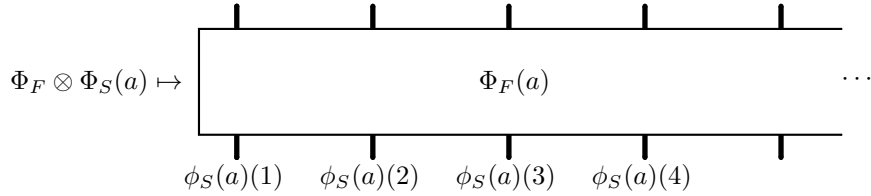
Le produit de Φ_F et Φ_S . Le fait que Φ_S ne se factorise pas par la représentation de Thompson Φ_F ouvre la perspective qu'en conjuguant les deux on s'approche davantage de la fidélité. Pour ce faire, il suffit de considérer le produit de Φ_F et Φ_S :

DÉFINITION 1.24 (**représentation $\Phi_F \otimes \Phi_S$**). On note $\Phi_F \otimes \Phi_S$ la représentation de H^+ définie pour a dans H^+ par

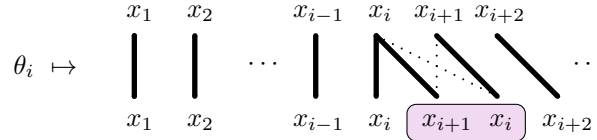
$$(1.25) \quad \Phi_F \otimes \Phi_S(a) := (\Phi_F(a), \Phi_S(a)).$$

La représentation $\Phi_F \otimes \Phi_S$ a une interprétation diagrammatique évidente : on garde la représentation par diagramme de forêts des éléments de F^+ , et on indique la valeur de l'entier $\phi_S(a)(k)$ en position k , ce qui revient à superposer le diagramme de (1.19) au diagramme de $\Phi_F(a)$ en ne

gardant que la valeur à l'extrémité basse des segments, mais pas les segments eux-mêmes, sur le modèle de



On voit facilement que, dans la représentation $\Phi_F \otimes \Phi_S$, le diagramme associé à un Θ -mot w s'obtient en partant de brins numérotés $1, 2, \dots$ en empilant les diagrammes des lettres successives θ_i de w suivant la règle d'actualisation des étiquettes



Noter le caractère « bizarre » de l'étiquetage en position $i + 1$ et $i + 2$: les étiquettes ne suivent pas les brins associés à Φ_F , mais elles correspondent à un diagramme virtuel associé à Φ_S (en traits pointillés), ce qui revient à insérer une transposition des noms entre les positions $i + 1$ et $i + 2$.

Du point de vue de la fidélité, la représentation $\Phi_F \otimes \Phi_S$ conjugue le pouvoir de séparation de Φ_F et de Φ_S , voir par exemple la figure 3.

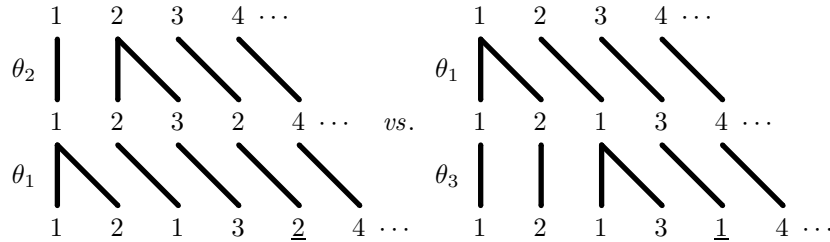


FIGURE 3. Contrairement à Φ_F , la représentation $\Phi_F \otimes \Phi_S$ sépare les éléments $\theta_2\theta_1$ et $\theta_1\theta_3$, grâce à l'ajout des étiquettes dans le diagramme de bifurcation : ici les étiquettes en position 5 (soulignées) diffèrent.

Pour autant, $\Phi_F \otimes \Phi_S$ n'est pas fidèle :

FAIT 1.26. *La représentation $\Phi_F \otimes \Phi_S$ ne sépare pas les éléments $\theta_1\theta_1\theta_3\theta_5$ et $\theta_1\theta_3\theta_1\theta_3$ de H^+ , qui sont pourtant distincts.*

DÉMONSTRATION. Les Θ -mots $\theta_1\theta_1\theta_3\theta_5$ et $\theta_1\theta_3\theta_1\theta_3$ sont réduits et distincts, donc ils représentent des éléments distincts de H^+ . Pourtant, leurs images par $\Phi_F \otimes \Phi_S$ coïncident, puisqu'on trouve à la fois

$$\Phi_F(\theta_1\theta_1\theta_3\theta_5) = \Phi_F(\theta_1\theta_3\theta_1\theta_3) = a_1^2 a_3 a_5,$$

$$\Phi_S(\theta_1\theta_1\theta_3\theta_5) = \Phi_F(\theta_1\theta_3\theta_1\theta_3) = [1, 2, 1, 1, 1, 3, 1]_4,$$

d'où $\Phi_F \otimes \Phi_S(\theta_1\theta_1\theta_3\theta_5) = \Phi_F \otimes \Phi_S(\theta_1\theta_3\theta_1\theta_3)$. \square

REMARQUE 1.27. La représentation $\Phi_F \otimes \Phi_S$ ne respecte pas la simplification à gauche : en contrepoint à l'égalité des images de $\theta_1|\theta_1\theta_3\theta_5$ et $\theta_1|\theta_3\theta_1\theta_3$, on peut vérifier que les images de $\theta_1\theta_3\theta_5$ et $\theta_3\theta_1\theta_3$, elles, diffèrent.

1.3. Les représentations $\Phi_{s,t}$. Comme ni la représentation Φ_S , ni la représentation produit $\Phi_F \otimes \Phi_S$ ne sont fidèles, on doit chercher d'autres représentations. Le choix de graines Ω vérifiant $\Omega(x, y) \in \{x, y\}^3$ semble trop restrictif : à part $\Omega(x, y) := (x, x, y)$, qui donne Φ_F , et $\Omega(x, y) := (x, y, x)$, qui donne Φ_S , on peut vérifier que seule $\Omega(x, y) := (x, y, y)$ donne une représentation de H^+ , laquelle est essentiellement Φ_F et ne sépare pas $\theta_1\theta_3$ et $\theta_2\theta_1$. On revient donc au cas général.

REMARQUE 1.28. Notons tout de suite qu'aucune graine Ω vérifiant $\Omega_3(x, y) = y$ ne peut séparer $\theta_1\theta_3$ et $\theta_2\theta_1$: en effet, dans ce cas, le trapèze de (1.8) se réduit à un carré : la valeur de sortie en $i + 2$ est simplement x_{i+1} et, de ce fait, $\Phi_\Omega(\theta_1\theta_3)$ et $\Phi_\Omega(\theta_2\theta_1)$ coïncident. Par exemple, on trouve

$$\Omega_1(x_1, x_2), \Omega_2(x_1, x_2), \Omega_1(x_2, x_3), \Omega_2(x_2, x_3), x_3, x_4, x_5, \text{ etc.}$$

comme valeur commune des suites $\Phi_\Omega(\theta_1\theta_3)(\vec{x})$ et $\Phi_\Omega(\theta_2\theta_1)(\vec{x})$.

Traduire les six égalités de (1.11) en un système de six équations fonctionnelles vérifiées par les trois composantes $\Omega_1, \Omega_2, \Omega_3$ de Ω est certainement faisable, mais compliqué. Sur le modèle de Φ_F et Φ_S , on se restreint ici au cas particulier

$$\Omega_1(x, y) = x :$$

autrement dit, dans le trapèze de la définition 1.6, on suppose que le brin de gauche garde son étiquette inchangée. Dès lors, il ne reste à chercher les contraintes que pour Ω_2 et Ω_3 , soit pour une fonction de X^2 dans lui-même.

LEMME 1.29. *Pour $f, g : X^2 \rightarrow X$, posons $\Omega(x, y) := (x, f(x, y), g(x, y))$.*

(i) *Le morphisme Φ_Ω induit une représentation du monoïde H^+ si, et seulement si, (f, g) est solution du système fonctionnel*

$$(1.30) \quad \begin{cases} f(g(f(x, y), g(x, y)), z) = f(y, z), \\ g(g(f(x, y), g(x, y)), z) = g(y, z). \end{cases}$$

En particulier, (1.30) est satisfaite si f et g sont solutions de

$$(1.31) \quad g(f(x, y), g(x, y)) = y.$$

(ii) *Dans le cas de (1.30), Φ_Ω sépare $\theta_1\theta_3$ et $\theta_2\theta_1$ que si, et seulement si, (f, g) n'est pas solution du système*

$$(1.32) \quad \begin{cases} f(g(x, y), z) = f(y, z), \\ g(g(x, y), z) = g(y, z); \end{cases}$$

ceci exclut en particulier toutes les solutions vérifiant $g(x, y) = y$.

DÉMONSTRATION. (i) Pour toute suite \vec{x} , les six premières valeurs de $\Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})$ et $\Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})$ sont :

$$\begin{aligned}\Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_1 &= \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_1 = x_1, \\ \Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_2 &= \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_2 = f(x_1, x_2), \\ \Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_3 &= \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_3 = f(f(x_1, x_2), g(x_1, x_2)), \\ \Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_4 &= \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_4 = g(f(x_1, x_2), g(x_1, x_2)), \\ \Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_5 &= f(x_2, x_3) \\ &\quad \text{à comparer avec } \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_5 = f(g(f(x_1, x_2), g(x_1, x_2)), x_3), \\ \Phi_\Omega(\theta_2\theta_1\theta_2)(\vec{x})_6 &= g(x_2, x_3) \\ &\quad \text{à comparer avec } \Phi_\Omega(\theta_1\theta_2\theta_4)(\vec{x})_6 = g(g(f(x_1, x_2), g(x_1, x_2)), x_3).\end{aligned}$$

La comparaison des valeurs en 5 et 6 donne (1.30) directement, et il est clair que (1.31) est une condition suffisante.

Le calcul pour (ii) est facile ; noter la cohérence avec la remarque 1.28. \square

REMARQUE 1.33. Sur le mode des biracks et des biquandles de la théorie des nœuds, voir par exemple [26, 43, 50], se donner deux fonctions de X^2 dans X équivaut à se donner deux opérations binaires, $*$ et $\bar{*}$, sur X . La condition (1.31) correspond alors à la loi algébrique $(x * y) \bar{*} (x \bar{*} y) = y$.

Il est naturel de chercher les solutions linéaires de l'équation fonctionnelle (1.30), et en particulier de (1.31).

LEMME 1.34. (i) *Pour a, b, c, d dans un anneau R , les fonctions f et g définies par $\begin{pmatrix} f(x, y) \\ g(x, y) \end{pmatrix} := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ sont solutions de (1.31) si, et seulement si, (a, b, c, d) est solution de*

$$(1.35) \quad \begin{cases} (a + d)c = 0 \\ bc + d^2 = 1. \end{cases}$$

(ii) *Si R est intègre de caractéristique différente de 2, les solutions de (1.35) sont les quadruplets (a, b, c, d) d'exactement un des trois types suivants :*

- *type I : $c = 0$ et $d = 1$,*
- *type II : $c = 0$ et $d = -1$,*
- *type III : $c \neq 0$ et $a + d = 0$ et $ad - bc = -1$.*

Dans le type I, (1.32) est toujours satisfait ; dans le type II, (1.32) est satisfait si, et seulement si, on a $a = 0$; dans le type III, (1.32) n'est jamais satisfait.

DÉMONSTRATION. (i) Porter la définition de f et g dans (1.30) donne

$$c(a + d)x + (bc + d^2 - 1)y = 0,$$

qui ne peut être identiquement satisfait que si on a

$$c(a + d) = 0 \quad \text{et} \quad bc + d^2 - 1 = 0,$$

soit (1.35).

(ii) Pour $c = 0$, il reste $d^2 = 1$, donc $d = \pm 1$. Dans ce cas, la seconde équation de (1.32) est toujours satisfaite, et la première est satisfaite si on a identiquement $2ay = 0$, donc si, et seulement si, $a = 0$.

Pour $c \neq 0$, la première équation de (1.35) devient $a+d = 0$, et la seconde équivaut alors à $ad - bc = -1$. Les deux équations de (1.32) deviennent

$$a(cx + (d - 1)y) = c(cx + (d - 1)y) = 0,$$

qui ne peut être identiquement nul puisque c est non nul. □

Dans les solutions de type I, on retrouve Φ_F pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, et on peut ignorer ces solutions puisqu'elles ne séparent pas $\theta_1\theta_3$ et $\theta_2\theta_1$. On n'a pas étudié les solutions de type II. Dans les solutions de type III, on retrouve Φ_S pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, et on retrouve le fait qu'elle sépare $\theta_1\theta_3$ et $\theta_2\theta_1$. Il est facile d'énumérer toutes les solutions de type III (en bijection avec les 2×2 -matrices de polynôme minimal $X^2 - 1$) sous la forme d'une famille à deux paramètres :

LEMME 1.36. *Les solutions de type III de (1.35) correspondent à la famille de matrices à deux paramètres s et t*

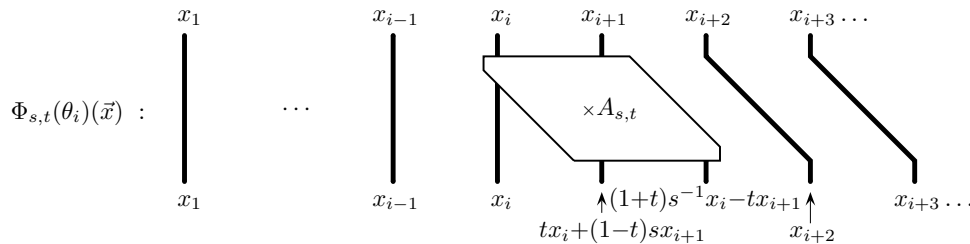
$$(1.37) \quad A_{s,t} := \begin{pmatrix} t & (1-t)s \\ (1+t)s^{-1} & -t \end{pmatrix} \quad \text{avec } s \neq 0.$$

DÉFINITION 1.38 (**représentation** $\Phi_{t,s}$). Pour $s \neq 0$, on note $\Phi_{s,t}$ la représentation de H^+ associée à la matrice $A_{s,t}$.

La représentation Φ_S est donc la spécialisation $\Phi_{1,0}$. La graine associée à la représentation $\Phi_{s,t}$ est la fonction

$$\Omega_{s,t} : (x, y) \mapsto (x, tx + (1-t)sy, (1+t)s^{-1}x - ty),$$

correspondant au diagramme



De façon équivalente, on peut voir $\Phi_{s,t}$ comme la représentation linéaire envoyant θ_i sur la matrice (infinie)

$$(1.39) \quad M_{s,t}(\theta_i) := \left(\begin{array}{c|cc|c} I_i & & 0 & \\ \hline & t & (1+t)s^{-1} & 0 \\ & (1-t)s & -t & \\ \hline 0 & & 0 & I_\infty \end{array} \right),$$

où I_n est la matrice carrée unité de taille n et où on a transposé la matrice $A_{s,t}$: dans la forme « matrice », on fait agir $M_{s,t}(\theta_i)$ à gauche sur \vec{x} écrit comme vecteur-colonne, et non à droite sur \vec{x} écrit comme vecteur-ligne dans le diagramme plus haut. Noter qu'il y a décalage d'indice : la matrice I_∞ de droite est décalée d'un cran à droite par rapport à la diagonale principale. En se restreignant à $s = 1$, on peut énoncer de façon plus précise :

PROPOSITION 1.40 (représentation $\Phi_{1,t}$). *Envoyer θ_i sur la matrice $M_{1,t}(\theta_i)$ définit une représentation linéaire de H^+ dans les matrices infinies à coefficients dans $\mathbb{Z}[t]$; pour tout a dans H^+ , si $P_{k,j}(a)$ est le coefficient de la k -ème ligne et de la j -ème colonne de $M_{1,t}(a)$, alors le degré de $P_{k,j}(a)$ est $\leq |a|$ et, de plus, on a $P_{k,j}(a) = 0$ pour $j > k$, et $P_{k,j}(a) = \delta_{k,j-|a|}$ pour $k \geq [a] + 3$.*

(On rappelle que $[a]$ est la valeur commune des paramètres $[w]$ pour w représentant a , voir définition I.3.11.)

DÉMONSTRATION. Par construction, les termes des suites $\Phi_{s,t}(a)(\vec{x})$ sont des combinaisons linéaires finies des x_i à coefficients dans $\mathbb{Z}[s, s^{-1}, t]$; de façon équivalente, les coefficients de la matrice correspondante $M_{s,t}(a)$ sont de tels polynômes, et il n'y en a qu'un nombre fini qui soient non nuls sur chaque ligne. Pour $s = 1$, les coefficients sont des polynômes de $\mathbb{Z}[t]$.

La borne sur le degré des polynômes $P_{k,j}(a)$ vient par une induction évidente : par définition, on a $M_{1,t}(a\theta_i) = M_{1,t}(a)M_{1,t}(\theta_i)$, et, dans $M_{1,t}(\theta_i)$, tous les degrés sont ≤ 1 .

Ensuite, appelons *seuil* (de décalage) pour a la plus petite valeur à partir de laquelle on a $P_{k,j}(a) = \delta_{k,j-|a|}$. Par exemple, le seuil pour θ_i est $i + 3$, soit $[\theta_i] + 3$. Alors, si le seuil pour a est k , le seuil pour $a\theta_i$ est $\leq i + 3$ si on a $k \leq i + 3$, et $\leq k + 1$ sinon, ce qui maintient l'hypothèse d'induction que le seuil pour a est au plus $[a] + 3$. \square

EXEMPLE 1.41. On pourra vérifier que la matrice $M_{1,t}(\theta_1\theta_2\theta_1)$ est

$$\begin{pmatrix} 1 & -t^2 + 2t & -t^2 + t + 1 \\ 0 & t^2 - 2t + 1 & t^2 - t \\ 0 & 0 & 0 \end{pmatrix},$$

bordée au-dessous par une matrice nulle $\infty \times 3$ et à droite par une matrice unité $\infty \times \infty$. Conformément à la proposition 1.40, les degrés des polynômes

sont au plus 3 (en fait, ici, au plus 2), et le seuil est au plus $\lceil \theta_1 \theta_2 \theta_1 \rceil + 3 = 6$ (en fait, ici, égal à 4).

On sait que la spécialisation $\Phi_{1,0}$, qui est Φ_S , n'est pas fidèle. Par contre, on propose

CONJECTURE 1.42 (fidélité). *La représentation générique $\Phi_{1,t}$ est fidèle, pour $t \neq 0$.*

La conjecture 1.42 est facile à tester par ordinateur — voir l'annexe informatique. Comme les éléments de H^+ sont exprimés de façon unique par les mots \mathcal{E}_H -réduits, il s'agit de vérifier que les suites $\Phi_{1,t}(u)(\vec{x})$ et $\Phi_{1,t}(v)(\vec{x})$ sont distinctes pour (u, v) couple de mots réduits distincts.

FAIT 1.43 (fidélité). *Il n'existe aucune paire de mots (u, v) de hauteur et de longueur ≤ 10 vérifiant $\Phi_{1,t}(u) \neq \Phi_{1,t}(v)$.*

REMARQUE 1.44. Telle qu'elles sont définies, les représentations fonctionnelles sont indépendantes de la représentation Φ_F . Comme on l'a vu pour Φ_S dans la définition 1.24, tensoriser par Φ_F est toujours possible et peut augmenter la fidélité. Une conjecture *a priori* plus facile que la conjecture 1.42 serait d'affirmer simplement que $\Phi_F \otimes \Phi_{1,t}$ est fidèle : le gain est qu'il suffit alors d'établir $\Phi_{1,t}(u) \neq \Phi_{1,t}(v)$ pour des paires de Θ -mots (u, v) vérifiant $\pi(u) \equiv_F \pi(v)$, puisque Φ_F sépare les autres paires. Comme les seuls mots \mathcal{E}_H -réduits que le morphisme π n'envoient pas sur des mots \mathcal{E}_F -réduits sont ceux qui ont un facteur $\theta_i \theta_{i+2}$, ce sont les paires $(w_1 \theta_i \theta_{i+2} w_2, w_1 \theta_{i+1} \theta_i w_2)$ qu'il faudrait étudier en premier. On a constaté dans la remarque 1.27 qu'une représentation peut très bien séparer deux mots u et v et néanmoins identifier des mots $\theta_i u$ et $\theta_i v$, donc le fait, garanti pour $\Phi_{1,t}$ par le lemme 1.34(ii), que $\Phi_{1,t}$ sépare $\theta_i \theta_{i+2}$ et $\theta_{i+1} \theta_i$ n'implique *a priori* rien pour $w_1 \theta_i \theta_{i+2} w_2$ et $w_1 \theta_{i+1} \theta_i w_2$.

2. Des questions ouvertes

Au terme de cette étude, de nombreuses questions sur le monoïde H^+ restent ouvertes, et on en regroupe quelques-unes ici. On évoquera successivement les relations de divisibilité (section 2.1), puis la question du plongement de H^+ dans un groupe et les propriétés du groupe H défini par la présentation (\mathcal{P}) (section 2.2), et enfin les représentations du monoïde H^+ et du groupe H (section 2.3).

2.1. Propriétés des relations de divisibilité. On a vu que le retournement à gauche n'est pas complet pour la présentation (\mathcal{P}) de H^+ , et, de là, on manque d'outil théorique et pratique pour étudier les questions relatives à la divisibilité à droite.

QUESTION 2.1. Le monoïde H^+ admet-il des pgcd à droite : étant donnés deux éléments a, b de H^+ , existe-t-il toujours un unique pgcd à droite de a et b ?

Comme on n'a pratiquement aucun contrôle de la relation de divisibilité à droite, il n'est pas du tout clair comment aborder ce type de question.

Comme chaque classe d'équivalence pour la congruence \equiv sur Θ^* associée à la présentation (\mathcal{P}) est finie, toutes les propriétés dérivées du problème de mots telles que « $[u]$ est-il diviseur à droite de $[v]$? » sont décidables. Par contre, si la réponse à la question 2.1 est négative, la question suivante est *a priori* ouverte :

QUESTION 2.2. Pour u, v dans Θ^* , la question « $[u]$ et $[v]$ ont-ils un multiple commun à gauche dans H^+ ? » est-elle décidable ?

Le problème est qu'on n'a pas de borne *a priori* sur la longueur d'un éventuel multiple commun, et donc qu'une recherche exhaustive est impossible.

D'autres questions portent sur la compatibilité de la forme normale du chapitre II et des relations de divisibilité du monoïde H^+ :

QUESTION 2.3. Pour a, b dans H^+ , peut-on reconnaître par inspection directe des mots $\text{NF}(a)$ et $\text{NF}(b)$ si a divise à gauche b ? si a divise à droite b ?

La réponse n'est pas claire. Une première étape serait de considérer le cas où a et b sont simples puisqu'alors, par les résultats du chapitre V, leur forme normale a un type très bien contrôlé.

Par ailleurs, on ne répète pas ici les questions posées à la fin du chapitre V par les décompositions Σ -gloutonnes, en particulier sur la possibilité de reconnaître la divisibilité à gauche sur la décomposition gloutonne des éléments.

2.2. Le groupe H . La présentation (\mathcal{P}) définit non seulement un monoïde, mais aussi un groupe :

DÉFINITION 2.4 (groupe H). On introduit le groupe H par

$$(2.5) \quad H := \left\langle \theta_1, \theta_2, \dots \left| \begin{array}{ll} \theta_j \theta_i = \theta_i \theta_{j+1} & \text{pour } j \geq i + 2 \\ \theta_j \theta_i \theta_j = \theta_i \theta_j \theta_{i+3} & \text{pour } j = i + 1 \end{array} \right. \right\rangle.$$

On note ι le morphisme canonique du monoïde H^+ dans le groupe H induit par l'identité sur Θ , et \equiv^\pm la congruence sur $(\Theta \cup \overline{\Theta})^*$ engendrée par les relations de (2.5) et les relations de groupe libre $\theta_i \overline{\theta_i} = \overline{\theta_i} \theta_i = 1$.

La principale question ouverte sur le lien entre le monoïde H^+ et le groupe H est celle du plongement :

QUESTION 2.6. Le monoïde H^+ se plonge-t-il dans le groupe H , c'est-à-dire, le morphisme ι de H^+ dans H est-il injectif ?

Soit, de façon équivalente :

QUESTION 2.7. Pour w, w' dans Θ^* , la relation $w \equiv^\pm w'$ implique-t-elle la relation $w \equiv w'$?

Dans le cas des monoïdes simplifiables admettant, au moins d'un côté, des multiples communs, on sait que le théorème de Ore [48] garantit le plongement du monoïde $\langle S | R \rangle^+$ dans le groupe $\langle S | R \rangle$, avec le résultat supplémentaire que le groupe est groupe de fractions du monoïde, c'est-à-dire que tout élément du groupe peut s'écrire (dans le cas où le monoïde admet des multiples communs à droite) sous la forme d'une fraction à droite $\iota(a)\iota(b)^{-1}$ avec a, b dans le monoïde. Comme on l'a rappelé, c'est le cas pour le monoïde de tresses B_∞^+ par rapport au groupe B_∞ , pour le monoïde de Thompson F^+ par rapport au groupe F , pour le monoïde de tresses parenthésées \widehat{BV}^+ par rapport au groupe \widehat{BV} . Mais on sait que cette propriété est en défaut dans H^+ : il existe des éléments sans multiple commun à droite, comme θ_2 et $\theta_1\theta_3$ (proposition IV.2.8), et des éléments sans multiple commun à gauche, comme θ_1 et θ_2 (proposition IV.2.13 ou II.3.30).

Les conditions de Malcev sont une liste explicite de conditions \mathcal{C} telles qu'un monoïde M se plonge dans un groupe si, et seulement si, il satisfait à \mathcal{C} [17]. Bien que ces conditions soient explicites, la première par exemple étant l'implication

$$(x_1y_1 = x_2y_2 \text{ et } x_1y'_1 = x_2y'_2 \text{ et } x'_1y_1 = x'_2y_2) \Rightarrow x'_1y'_1 = x'_2y'_2,$$

on ne voit pas comment les utiliser ici.

Dans [27], un critère de plongement mettant en jeu une condition plus faible que l'existence de multiples communs est établi :

DÉFINITION 2.8 (condition 3-Ore). On dit qu'un monoïde simplifiable M satisfait la *condition 3-Ore à droite* si trois éléments de M qui ont deux à deux un multiple commun à droite ont un multiple commun global. La *condition 3-Ore à gauche* est semblable, pour les multiples à gauche.

La condition 3-Ore est plus faible que l'existence de multiples communs : par exemple, un monoïde libre la satisfait (à gauche et à droite), car deux mots n'ont de multiple à droite commun que si l'un est préfixe de l'autre. Il est donc raisonnable de soulever :

QUESTION 2.9. Le monoïde H^+ satisfait-il la condition 3-Ore à droite ? À gauche ?

Grâce à la complétude du retournement à droite et au contrôle de sa terminaison à l'aide de la présentation dérivée de la section IV.3.2 décrit dans le lemme IV.3.6, il devrait être possible d'étudier assez facilement la condition 3-Ore à droite dans H^+ . Par contre, pour la condition à gauche, le piètre contrôle de la divisibilité à gauche rend pessimiste. Or, pour espérer appliquer le critère de plongement de [27], il faut absolument que les deux relations de divisibilité, à gauche et à droite, satisfassent les mêmes hypothèses.

À supposer que H^+ se plonge dans H mais que la condition 3-Ore soit en défaut, la question d'une décomposition distinguée des éléments du groupe en fonction de ceux du monoïde semble complètement ouverte.

Pour terminer, au-delà des questions sur le plongement de H^+ dans H , se posent immédiatement des questions sur le groupe H lui-même.

QUESTION 2.10. Le problème de mot du groupe H est-il décidable ?

QUESTION 2.11. Le groupe H a-t-il de la torsion ?

Faute d'un contrôle du lien avec le monoïde H^+ , il est douteux que l'étude de ce dernier puisse contribuer directement à des réponses. Par contre, la similarité de la présentation de H et de celle du groupe de Thompson F est peut-être la meilleure piste.

QUESTION 2.12. Existe-t-il pour le groupe H une réalisation semblable à celle de F par applications affines par morceaux de $[0, 1]$ dans lui-même ?

De nombreuses variations sur la construction de F à partir d'applications de $[0, 1]$ dans lui-même affines par morceaux sont apparues récemment [8, 44], et il serait intéressant de savoir si H peut être obtenu de la sorte.

Un résultat trivial, mais qui peut servir de point de départ, est que F est un quotient de H :

LEMME 2.13. *L'application $\pi : \theta_i \mapsto a_i$ définit un homomorphisme surjectif de H sur F .*

DÉMONSTRATION. La vérification est la même que pour la proposition I.3.26 : les éléments a_i du groupe F satisfont les relations de la présentation (\mathcal{P}) , donc le morphisme du groupe libre de base Θ vers F qui envoie θ_i sur a_i factorise par le groupe H . \square

QUESTION 2.14. Existe-t-il une description simple du noyau de la projection π de H sur F ?

Bien sûr, on sait que $\text{Ker}(\pi)$ est engendré par les éléments

$$(\theta_i \theta_{i+2})^{-1} (\theta_{i+1} \theta_i),$$

mais cela n'en donne pas une description explicite.

Contrairement à H^+ , le monoïde F^+ admet des multiples communs à droite, et F est groupe de fractions à droite pour F^+ . De ce fait, on peut utiliser les mots \mathcal{E}_F -réduits (section II.2.1) pour représenter les éléments de F .

QUESTION 2.15. Peut-on, à partir des mots \mathcal{E}_F - et \mathcal{E}_H -réduits, définir une section pour la projection de H sur F ? La suite exacte

$$1 \longrightarrow \text{Ker}(\pi) \longrightarrow H \longrightarrow F \longrightarrow 1$$

est-elle scindée ?

2.3. Représentations du monoïde H^+ (et du groupe H). Dans le cas de H^+ , plusieurs familles de représentations ont été décrites dans la section 1. Le problème est qu'on ne sait pas si ces représentations sont injectives, et, d'autre part, ce sont en général des représentations à valeurs dans un monoïde, pas un groupe : sauf dans le cas de Φ_F , qui va vers le monoïde F^+ , mais donc aussi vers le groupe F puisque F^+ se plonge dans F , la plupart des autres exemples ne semblent pas faciles à utiliser. En particulier,

la représentation $\Phi_{1,t}$ de la définition 1.38, conjecturée fidèle, correspond à une matrice (infinie) essentiellement non inversible : la matrice $A_{1,t}$ qui sert de graine est inversible (de déterminant -1), mais le décalage ultime des colonnes s'oppose à l'inversibilité.

QUESTION 2.16. Peut-on dériver de la représentation $\Phi_{s,t}$ une représentation au moins aussi fidèle et à valeurs dans un groupe linéaire ?

Si la réponse à la question 2.16 était positive, une preuve de la conjecture 1.42 suffirait à démontrer que le monoïde H^+ se plonge dans le groupe H . En effet, par la propriété universelle du groupe enveloppant d'un monoïde, donc ici du groupe H par rapport au monoïde H^+ , on sait qu'un monoïde M se plonge dans son groupe enveloppant $U(M)$ si, et seulement si, M se plonge dans un groupe G quelconque : en effet, dans ce cas, tout morphisme ϕ de M dans G factorise par le morphisme canonique ι de M dans $U(M)$ et, donc, si ϕ est injectif, alors ι est nécessairement injectif.

Une façon d'aborder la questions 2.16 — et, de là, la question 2.6 — est de se demander

QUESTION 2.17. Lesquelles des diverses représentations décrites dans la section 1 peut être définie sur le groupe H (ou étendue à H si on sait déjà que H^+ se plonge dans H) ?

D'autres questions portent sur les représentations de H^+ elles-mêmes. En particulier, certaines pistes n'ont pas encore été explorées.

QUESTION 2.18. Les représentations linéaires dites de type II suivant la classification du lemme 1.34 apportent-elles une information supplémentaire par rapport aux autres types ? Même question pour les représentations $\Phi_{s,t}$ avec $s \neq 1$?

D'autre part, on a vu dans le lemme 1.13 que, dans le cas particulier des représentations spéciales dont la graine satisfait la condition très particulière $\Omega(x, y) \in \{x, y\}^3$, alors on ne perd pas d'information si, au lieu d'évaluer la représentation Φ_Ω sur une suite \vec{x} générique, on l'évalue sur la suite particulière $(1, 2, 3, \dots)$. La représentation $\Phi_{1,t}$ est spéciale, mais associée à une graine qui n'est pas du type ci-dessus : les valeurs de sortie sont des combinaisons linéaires des x_i , mais pas des x_i eux-mêmes.

QUESTION 2.19. Perd-on de l'information — en l'occurrence, perd-on la fidélité conjecturée de $\Phi_{1,t}$ — en remplaçant l'évaluation de $\Phi_{1,t}$ en la suite générique \vec{x} par son évaluation en la suite particulière $(1, 2, \dots)$?

Comme les polynômes (à coefficients dans $\mathbb{Z}[t]$, ou dans $\mathbb{Z}[s, s^{-1}, t]$ dans le cas général de $\Phi_{s,t}$) qui sont les coefficients des combinaisons linéaires ne sont pas juste 0 ou 1 en général, on ne voit pas pourquoi la réponse à la question 2.19 devrait être positive, mais les expérimentations informatiques n'ont pas trouvé de contre-exemple.

Enfin, l'échec de la tentative de description du monoïde H^+ comme sous-monoïde de \widehat{V} ou de \widehat{BV} (Faits 1.20 et 1.22) en envoyant θ_i sur $a_i s_{i+1}$ ou $a_i \sigma_{i+1}$ mène aux deux questions jumelles sur les groupes ci-dessus :

QUESTION 2.20. Peut-on décrire explicitement le sous-monoïde de \widehat{V} (*resp.*, de \widehat{BV}) engendré par les éléments $a_i s_{i+1}$ (*resp.*, $a_i \sigma_{i+1}$) ?

Annexe informatique

Pour étudier le monoïde H^+ , diverses expérimentations par ordinateur ont été réalisées pour tester des possibilités, dénombrer des configurations, ou valider des conjectures. Dans cette annexe, on donne quelques précisions sur la représentation des données et les algorithmes utilisés.

1. Représentation des données

Tous les programmes ont été écrits en langage PYTHON et implémentés dans l'environnement de développement PYCHARM.

Les données ont été représentées principalement sous forme de listes. Les éléments du monoïde H^+ sont représentés par des mots positifs, eux-mêmes manipulés comme listes d'entiers naturels non nuls, dont le p -ème terme est l'entier i , si la p -ième lettre du mot est θ_i . Par exemple, le Θ -mot $\theta_3\theta_4\theta_1\theta_{10}$ est représenté par la liste $[3, 4, 1, 10]$.

Dans le cas de mots signés, si un mot possède une lettre négative, on rajoute simplement un $-$ devant l'entier correspondant à cette lettre dans la liste. Par exemple, le Θ -mot signé $\overline{\theta_3}\theta_4\theta_1\overline{\theta_{10}}$ est représenté par la liste $[-3, 4, 1, -10]$.

On a été amené également à manipuler des mots sur l'alphabet Θ' , dont les lettres sont elles-mêmes des mots sur l'alphabet Θ . On représente un Θ' -mot par une liste comprenant les différentes lettres de Θ' qui, en tant que Θ -mots, sont elles-mêmes des listes : on obtient une liste de listes. Pour distinguer une lettre positive d'une lettre négative dans un Θ' -mot signé, on rajoute un signe " + " si une lettre est positive et un " - " si une lettre est négative. Par exemple, le Θ' -mot signé $\overline{\theta_1} \cdot \theta_1\theta_2 \cdot \overline{\theta_1\theta_3\theta_4} \cdot \theta_4\theta_6$ est représenté par la liste de listes $[[" + ", 1], [" + ", 1, 2], [" - ", 1, 3, 4], [" + ", 4, 6]]$.

Enfin, pour étudier les représentations linéaires du monoïde H^+ , et en particulier la représentation $\Phi_{1,t}$, on a eu à manipuler des listes de polynômes à coefficients entiers. Comme il n'existe pas d'implémentation native des polynômes dans PYTHON, on a traité ceux-ci comme des listes de coefficients, puis les combinaisons linéaires à coefficients dans $\mathbb{Z}[t]$ comme listes de listes, et, finalement, les représentations $\Phi_{1,t}(w)$ comme des listes de listes — ce qui n'a pas posé pas de problème à l'exécution.

2. Principaux algorithmes

On donne maintenant quelques indications plus spécifiques sur les algorithmes utilisés. On passera en revue successivement la mise sous forme normale (section 2.1), le retournement de mot et les procédures dérivées (section 2.2), le comptage des éléments simples (section 2.3), et l'étude des représentations linéaires (section 2.4).

2.1. Mise sous forme normale. L'implémentation de la réécriture \mathcal{E}_H ne pose pas de problème, car les règles ne sont que de deux types et très simples. On manipule donc des listes d'entiers, qu'on réécrit comme dans le système \mathcal{E}_H . Le pseudocode correspondant est le suivant :

Algorithme 2.1 (réécriture \mathcal{E}_H).

Entrée: un Θ -mot u

Sortie: la forme réduite de u

- 1: **tant que** $(\exists i < |u| (u[i] < u[i + 1] - 2))$ ou $(\exists i < |u| - 1 (u[i] = u[i + 1] - 1$ et $u[i + 1] = u[i + 2] - 2))$ **faire**
- 2: **si** $u[i] < u[i + 1] - 2$ **alors**
- 3: $s := u[i]$
- 4: $t := u[i + 1]$
- 5: $u[i] := t - 1$
- 6: $u[i + 1] := s$
- 7: **sinon**
- 8: $s := u[i]$
- 9: $u[i] := s + 1$
- 10: $u[i + 1] := s$
- 11: $u[i + 2] := s + 1$
- 12: **retourner** u

Dans certains cas, en particulier lorsqu'on part d'un mot déjà réduit et qu'on ajoute des lettres à droite, la proposition II.3.28 donne une stratégie simple permettant de construire de façon inductive la forme réduite d'un mot : si u est un mot \mathcal{E}_H -réduit, on obtient la forme \mathcal{E}_H -réduite de $u\theta_i$ en poussant θ_i le plus possible vers la gauche. Ceci est facilement implémenté comme suit :

Algorithme 2.2 (forme réduite inductive).

Entrée: un Θ -mot réduit u et un atome θ_i

Sortie: la forme réduite de $u\theta_i$

- 1: $u' := u\theta_i$
- 2: $j := |u'|$
- 3: **tant que** $j \geq 3$ **faire**
- 4: **si** $u'[j] > u'[j - 1] + 2$ **alors**
- 5: $s := u'[j]$


```

6:      $t := u'[j - 1]$ 
7:      $u'[j] := t$ 
8:      $u'[j - 1] := s - 1$ 
9:      $j := j - 1$ 
10:  sinon
11:    si ( $u'[j] = u'[j - 1] + 2$  et  $u'[j - 1] = u'[j - 2] + 1$ ) alors
12:       $s := u'[j]$ 
13:       $u'[j] := s - 2$ 
14:       $u'[j - 1] := s - 3$ 
15:       $u'[j - 2] := s - 2$ 
16:       $j := j - 2$ 
17:    sinon
18:      retourner  $w'$ 
19:  si  $u'[2] > u'[1] + 2$  alors
20:     $s := u'[2]$ 
21:     $t := u'[1]$ 
22:     $u'[2] := t$ 
23:     $u'[1] := s - 1$ 
24:  retourner  $w'$ 

```

2.2. Retournement à droite et procédures dérivées. Le retournement de facteur à droite est utile pour plusieurs problèmes : comme solution au problème de mots, il est moins efficace que la mise sous forme normale, mais il est irremplaçable pour la détermination des multiples communs à droite et la divisibilité à gauche.

L'implémentation du retournement est facile : comme on utilise les entiers relatifs pour représenter les mots signés, le retournement est un système de réécriture déterministe sur de telles listes (une seule règle s'applique si on prend le premier motif $-+$ de la liste à retourner). Le retournement correspond alors au code suivant.

Algorithme 2.3 (R -retournement à droite).

Entrée: un Θ -mot signé w

Sortie: un Θ -mot positif-négatif ou pas de sortie

```

1: tant que  $\exists i < |w|$  ( $w[i] < 0$  et  $w[i + 1] > 0$ ) faire
2:    $j := \min\{i \mid w[i] < 0 \text{ et } w[i + 1] > 0\}$ 
3:   si  $|w[j]| = w[j + 1]$  alors
4:     supprimer  $w[j]$  et  $w[j + 1]$ 
5:   sinon
6:     si  $|w[j]| = w[j + 1] - 1$  alors
7:        $s := -w[j]$ 
8:        $t := -w[j + 1]$ 
9:        $w_1 := w[1 : j - 1]$ 
            $\triangleright w_1$  comprend les  $j - 1$ -ème premières lettres de  $w$ 
10:       $w_2 := w[j + 2 : |w|]$ 

```

$\triangleright w_2$ comprend les lettres de w de la $j + 2$ -ème à la $|w|$ -ème.

```

11:  $w := w_1 + [s + 1, s + 3, t, t + 1] + w_2$ 
12: sinon
13:   si  $|w[j]| = w[j + 1] + 1$  alors
14:      $s := -w[j]$ 
15:      $t := -w[j + 1]$ 
16:      $w_1 := w[1 : j - 1]$ 
17:      $w_2 := w[j + 2 : |w|]$ 
18:      $w := w_1 + [s - 1, s, t - 3, t - 1] + w_2$ 
19:   sinon
20:     si  $|w[j]| < w[j + 1] - 1$  alors
21:        $s := w[j]$ 
22:        $t := w[j + 1]$ 
23:        $w[j] := t + 1$ 
24:        $w[j + 1] := s$ 
25:     sinon
26:        $s := w[j]$ 
27:        $t := w[j + 1]$ 
28:        $w[j] := t$ 
29:        $w[j + 1] := s - 1$ 
30: retourner  $w$ 

```

Le problème (sérieux) avec le retournement est son éventuelle non-termination : on sait qu'il existe des couples de mots (u, v) pour lesquels le retournement de $\bar{u}v$, sans bloquer, ne termine pas.

Dans un premier temps, une solution heuristique (et peu efficace) a consisté, pour éviter que la boucle tourne indéfiniment, à mettre un compteur et une borne N (assez grande) qui arrête la procédure de retournement quand le compteur atteint la valeur fixée N . Cette solution est évidemment non satisfaisante, car les résultats négatifs sont alors entachés d'incertitude.

Heureusement, l'identification d'un ensemble de mots clos par complément à droite, comme expliqué dans la section III.3.1, a permis de régler ce problème, puisqu'en utilisant l'alphabet étendu Θ' et le R' -retournement correspondant, on sait d'avance que le retournement termine, en l'occurrence réussit ou bloque. Comme les éléments de Θ' sont eux-mêmes des mots sur l'alphabet Θ , ils sont implémentés naturellement comme listes de listes. Une étape de R' -retournement consiste à retourner un facteur $\bar{s} \cdot \underline{t}$ en $\underline{C_R(s, t)} \cdot \overline{C_R(t, s)}$ quand $C_R(s, t)$ est défini. Le point clé de l'algorithme 2.4 est l'implémentation du retournement à droite pour la nouvelle présentation (Θ', R') . En fait, on n'a pas besoin d'utiliser explicitement cette présentation (Θ', R') , mais simplement de savoir reconnaître, quand on a deux mots u, v dans Θ' , si le R -complément $C_R(u, v)$ existe, et à déterminer sa valeur s'il existe, donc à rester dans le cadre du R -retournement.

On rappelle qu'on a $\Theta' = \Theta_1 \cup \Theta_2 \cup \{\varepsilon\}$, avec

$$\Theta_1 = \{\theta_i \theta_{i+2} \theta_{i+4} \cdots \theta_{i+2k} \mid i \geq 1, k \geq 0\},$$

$$\Theta_2 = \{\theta_i \theta_{i+2} \theta_{i+4} \cdots \theta_{i+2k} \theta_{i+2k+1} \mid i \geq 1, k \geq 0\},$$

On dit que u est de *type 1* si u appartient à Θ_1 et de *type 2* si u appartient à Θ_2 . Il est facile de reconnaître si u est de type 1 ou de type 2 : Si $|u| = 1$, alors u est de type 1, et sinon, on regarde les deux dernières lettres de u . Le résultat important ici est le lemme IV.3.1, qui énumère tous les cas possibles de terminaison et de non-terminaison selon la forme de u et v . Le pseudo-code de l'implémentation correspondante est le suivant :

Algorithme 2.4 (*R'*-retournement à droite).

Entrée: un Θ' -mot signé w

Sortie: Un Θ' -mot positif-négatif ou BLOQUE

```

1: tant que  $\exists i < |w|$  ( $w[i][1] = \text{"-"}$  et  $w[i+1][1] = \text{"+"}$ ) faire
2:    $j := \min\{i \mid w[i][1] = \text{"-"} \text{ et } w[i+1][1] = \text{"+"}\}$ 
3:    $u := w[j][2 : |w[j]|]$ 
4:    $v := w[j+1][2 : |w[j+1]|]$ 
5:   si  $u = []$  alors
6:     supprimer  $w[j]$ 
7:   si  $v = []$  alors
8:     supprimer  $w[j+1]$ 
9:   si  $u$  et  $v$  sont de type 1 alors
10:    si  $u[1] < v[1] < u[1] + |u|$  ou  $v[1] < u[1] < v[1] + |v|$  alors
11:      retourner BLOQUE
12:    sinon
13:       $w_1 := [\text{"+"}] + \text{LISTE\_COMPLEMENT}(u, v)$ 
14:       $w_2 := [\text{"-"}] + \text{LISTE\_COMPLEMENT}(v, u)$ 
15:    si  $u$  est de type 1 et  $v$  sont de type 2 alors
16:      si  $u[1] < v[1] < u[1] + |u|$  ou  $v[1] < u[1] < v[1] + |v| - 1$  alors
17:        retourner BLOQUE
18:      sinon
19:         $w_1 := [\text{"+"}] + \text{LISTE\_COMPLEMENT}(u, v)$ 
20:         $w_2 := [\text{"-"}] + \text{LISTE\_COMPLEMENT}(v, u)$ 
21:    si  $u$  est de type 2 et  $v$  sont de type 1 alors
22:      si  $u[1] < v[1] < u[1] + |u| - 1$  ou  $v[1] < u[1] < v[1] + |v|$  alors
23:        retourner BLOQUE
24:      sinon
25:         $w_1 := [\text{"+"}] + \text{LISTE\_COMPLEMENT}(u, v)$ 
26:         $w_2 := [\text{"-"}] + \text{LISTE\_COMPLEMENT}(v, u)$ 
27:    si  $u$  et  $v$  sont de type 2 alors
28:      si  $u[1] < v[1] < u[1] + |u| - 1$  ou  $v[1] < u[1] < v[1] + |v| - 1$  alors
29:        retourner BLOQUE
30:      sinon

```

```

31:           $w_1 := [” + ”] + [LISTE\_COMPLEMENT(u, v)]$ 
32:           $w_2 := [” - ”] + [LISTE\_COMPLEMENT(v, u)]$ 
33:     $w[i] := w_1$ 
34:     $w[i + 1] := w_2$ 
35: retourner  $w$ 

```

La fonction LISTE_COMPLEMENT est une procédure qui a pour entrée deux Θ' -mots tels que le complément $C(u, v)$ existe et qui donne en sortie la liste $C(u, v)$. On ne l'écrit pas ici car elle énumère tous les cas possibles en suivant le lemme IV.3.1 selon la forme de u et v où $C(u, v)$ est défini et, de ce fait, elle est très longue (plus de 100 lignes de code).

Une fois le retournement implémenté, il est facile d'en déduire la solution au problème de mot par R' -retournement (tester si le mot final est vide), l'existence et la recherche de ppcm à droite ($[u]$ et $[v]$ ont un ppcm à droite si, et seulement si, le R' -retournement de $\bar{u} \cdot v$ ne bloque pas, et alors le ppcm est $[\text{dev}(\underline{u})\text{dev}(C(u, v))]$ — $\text{dev}(u)$ est le développement en Θ -mot d'un Θ' -mot — la divisibilité à gauche ($[u]$ divise à gauche $[v]$ si, et seulement si, le R' -retournement de $\bar{u} \cdot v$ ne bloque pas et termine avec un Θ' -mot positif), la simplicité (par la proposition V.3.4, $[u]$ est simple si, et seulement si, il divise à gauche Δ_n avec $n := [u] + 1$).

2.3. Comptage des éléments simples. En vue, dans un premier temps, d'orienter la recherche puis, dans un second temps, de confirmer les résultats démontrés, on a cherché à dénombrer systématiquement les éléments simples d'indice et de longueur fixés (les ensembles $\Sigma_{n,\ell}$ de la définition V.1.19). Le résultat est la table V.1, dont les valeurs des 10 premières lignes ont été confirmées par ordinateur.

À n fixé, on sait que le plafond de Δ_n est $3n - 5$. Ceci implique que si a est un diviseur à gauche de Δ_n , alors on a $[a] \leq 3n - 5$. Donc, si un Θ -mot w représente a , on doit avoir $\text{ht}(w) \leq 3n - 5$.

La structure générale du programme de comptage est la suivante : on énumère tous les mots réduits de longueur ℓ et de hauteur $\leq 3n - 5$, c'est-à-dire, tous les mots de longueur ℓ et de hauteur $\leq 3n - 5$ ne possédant aucun facteur de la forme $\theta_i \theta_j$ pour $j \geq i + 3$ ni de la forme $\theta_i \theta_{i+1} \theta_{i+3}$. La procédure pour énumérer ces mots est la suivante :

Algorithme 2.5 (mots réduits).

Entrée: deux entiers naturels non nuls ℓ et h

Sortie: la liste de tous les mots-réduits de longueur ℓ et de hauteur $\leq h$

```

1:  $L := []$ 
2: pour pour  $i$  allant de 1 à  $h$  faire
3:    $L := L + [[i]]$  ▷  $L$  contient tous les atomes  $\theta_1, \dots, \theta_h$ 
4:  $L' := []$ 
5: tant que  $L \neq L'$  faire
6:   pour  $j$  allant de 1 à  $h$  faire
7:     pour  $i$  allant de 1 à  $|L|$  faire
8:       si  $|L[i]| = 1$  alors

```

```

9:          si  $j \leq L[i][1] + 2$  alors
10:              $w := L[i] + [j]$ 
11:             si  $|w| \leq \ell$  et  $w$  n'appartient pas à  $L$  alors
12:                 $L := L + [w]$  ▷ on rajoute  $w$  à  $L$ 
13:          si  $|L[i]| \geq 2$  alors
14:             si  $j \leq L[i][|L[i]|] + 1$  alors
15:                 $w := L[i] + [j]$ 
16:                si  $|w| \leq \ell$  et  $w$  n'appartient pas à  $L$  alors
17:                    $L := L + [w]$ 
18:             si  $j = L[i][|L[i]|] + 2$  et  $L[i][|L[i]| - 1] \neq j - 3$  alors
19:                 $w := L[i] + [j]$ 
20:                si  $|w| \leq \ell$  et  $w$  n'appartient pas à  $L$  alors
21:                    $L := L + [w]$ 
▷ arrivé ici,  $L$  possède tous les mots réduits de longueur  $\leq \ell$ 
▷ et de hauteur  $\leq h$ , et il reste à trier ceux de longueur  $\ell$ 
22:  $M = []$ 
23: pour  $w$  dans  $L$  faire
24:     si  $|w| = \ell$  alors
25:          $M := M + [w]$ 
26: retourner  $M$ 

```

Ensuite, pour chacun de ces mots réduits de longueur ℓ et de hauteur $\leq 3n - 5$, disons u , on effectue le R' -retournement de $\bar{u} \cdot \underline{\Delta}_n$ et, si celui-ci termine par un Θ' -mot positif, on rajoute u à une liste (vide au départ). Le cardinal de cette liste est le nombre de diviseurs à gauche de Δ_n de longueur ℓ .

2.4. Représentations linéaires. On a implémenté la représentation $\Phi_{1,t}$ de la définition 1.38, et testé sa fidélité. En pratique, on a travaillé avec la version « suite de variables et combinaisons linéaires » plutôt qu'avec la version « matrice ». De ce fait, il s'agit de déterminer les (premières) valeurs de suites dont les termes sont des combinaisons linéaires à coefficients dans $\mathbb{Z}[t]$ de variables x_k .

Si w est un Θ -mot de hauteur h et de longueur ℓ , alors, par la proposition 1.40, le seuil de décalage de w est au plus $\lceil w \rceil + 3 \leq h + \ell + 2$. Donc, pour caractériser entièrement la suite $\Phi_{1,t}(w)(\vec{x})$, il suffit de donner les $h + \ell + 1$ premiers termes de la suite. Ensuite, ces $h + \ell + 1$ premiers termes sont des combinaisons dans $\mathbb{Z}[t]$ de variables x_1, \dots, x_{h+1} , c'est-à-dire de la forme $\sum_{j=1}^{h+1} P_{k,j}(t)x_j$ pour la valeur du k -ième terme. De plus, toujours par la proposition 1.40, le degré de chaque polynôme $P_{k,j}(t)$ est au plus ℓ . On peut donc implémenter un polynôme par une liste de longueur $\ell + 1$ et une valeur de la suite $\Phi_{1,t}(w)(\vec{x})$ par une liste de longueur $h + 1$ de listes de longueur $\ell + 1$. Par conséquent, on implémente $\Phi_{1,t}(w)(\vec{x})$ comme une liste de longueur $h + \ell + 1$ de listes de longueur $h + 1$ de listes de longueur $\ell + 1$.

À h fixé, on veut vérifier que les suites $\Phi_{1,t}(u)(\vec{x})$ et $\Phi_{1,t}(v)(\vec{x})$ sont distinctes pour (u, v) couple de mots réduits distincts de hauteur au plus h . Or, on sait que la suite $\Phi_{t,1}(u)(\vec{x})$ est ultimement un décalage de $|u|$ crans, donc il est inutile de tester les paires (u, v) avec $|u| \neq |v|$, qui n'ont pas le même décalage ultime.

Donc, à h et ℓ fixé, on veut vérifier que les suites $\Phi_{1,t}(u)(\vec{x})$ et $\Phi_{1,t}(v)(\vec{x})$ sont distinctes pour (u, v) couple de mots réduits de même longueur ℓ distincts d'hauteur au plus h . La structure générale du programme est la suivante. On énumère tous les mots réduits de longueur ℓ et de hauteur h dans une liste. Pour toute paire de mots distincts dans cette liste, on calcule chacune des deux suites $\Phi_{1,t}(u)(\vec{x})$ et $\Phi_{1,t}(v)(\vec{x})$, et on vérifie qu'elles sont distinctes. Le calcul d'une suite $\Phi_{1,t}(u)(\vec{x})$ se fait inductivement, en déterminant $\Phi_{1,t}(w\theta_i)(\vec{x})$ à partir de $\Phi_{1,t}(w)(\vec{x})$: on laisse inchangées les i premières valeurs et, à partir de $i + 3$ -ième, on effectue un décalage. L'algorithme 2.6 implémente l'actualisation des valeurs quand, partant des deux valeurs x et y supposées être les i -ème et $(i + 1)$ -ème termes d'une suite $\Phi_{1,t}(u)(\vec{x})$ avec u de longueur ℓ et de hauteur au plus h , on applique la fonction $f(x, y) := tx + (1 - t)y$. La procédure a pour entrée deux listes de listes (correspondant à x et y) et en sortie une liste de listes correspondant à $tx + (1 - t)y$.

Algorithme 2.6 (fonction f).

Entrée: deux combinaisons linéaires L et M de x_1, \dots, x_{h+1} à coefficients dans $\mathbb{Z}[t]$

Sortie: la combinaison linéaire $tL + (1 - t)M$

- 1: **pour** i de 1 à $h + 1$ **faire**
- 2: **pour** j décroissant de $\ell + 1$ à 2 **faire**
- 3: $L[i][j] := L[i][j - 1]$
- 4: $L[i][1] := 0$ ▷ chaque polynôme de L a été multiplié par t
- 5: $P := M$ ▷ on crée une copie de M destinée à être multipliés par $-t$
- 6: **pour** i de 1 à $h + 1$ **faire**
- 7: **pour** j décroissant de $\ell + 1$ à 2 **faire**
- 8: $P[i][j] := -P[i][j - 1]$
- 9: $P[i][1] := 0$
- 10: **pour** i de 1 à $h + 1$ **faire**
- 11: **pour** j de 1 à $\ell + 1$ **faire**
- 12: $M[i][j] := P[i][j] + M[i][j]$
 ▷ chaque polynôme de M a été multiplié par $1 - t$
- 13: **pour** i de 1 à $h + 1$ **faire**
- 14: **pour** j de 1 à $\ell + 1$ **faire**
- 15: $L[i][j] := L[i][j] + M[i][j]$
- 16: **retourner** L

La fonction $g(x, y) := (1 + t)x - ty$ s'implémente de manière similaire.

Bibliographie

- [1] S.I. Adyan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.
- [2] E. Artin, *Theorie des Zöpfe*, Abh. Math. Sem. Univ. Hamburg **4** (1925) 47–72.
- [3] E. Artin, *Theory of Braids*, Ann. of Math. **48** (1947) 101–126.
- [4] J.M. Autebert, *Langages algébriques*, Masson, Paris (1987).
- [5] F. Baader & T. Nipkow, *Term Rewriting and All That*, Cambridge University Press (1998).
- [6] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).
- [7] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Adv. Math. **139-2** (1998) 322–353.
- [8] C. Bleak, M.G. Brin, & J.T. Moore, *Complexity among the finitely generated subgroups of Thompson’s group*, arXiv :1711.10998.
- [9] L.A. Bokut, *Gröbner-Shirshov basis for the braid group in the Artin-Garside generators*, J. Symbolic Comput. **43** (2008) 397–405.
- [10] E. Brieskorn & K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972) 245–271.
- [11] M. Brin, *The algebra of strand splitting. I. A braided version of Thompson’s group V*, J. Group Th. ; 10; 2007; 757–788.
- [12] M. Brin, *The algebra of strand splitting. II. A presentation for the braid group on one strand*, Intern. J. of Algebra and Computation **16** (2006) 203–219.
- [13] M. Brin, *On the Zappa-Szép product*, Comm. in Algebra **33** (2005) 393–424.
- [14] O. Carton, *Langages formels, calculabilité et complexité*, Vuibert, Paris (2008).
- [15] J.W. Cannon, W.J. Floyd, & W.R. Parry, *Introductory notes on Richard Thompson’s groups*, Ens. Math. **42** (1996) 215–257.
- [16] J. Chamboredon, *Algorithmique des tresses et de l’autodistributivité*, Thèse de l’université de Caen (2011).
- [17] A.H. Clifford & G.B. Preston, *The Algebraic Theory of Semigroups, volume 1*, Math. surveys vol.7, Amer. Math. Soc., (1967).
- [18] P. Dehornoy, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997) 115–137.
- [19] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser (2000).
- [20] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002) 267–306.
- [21] P. Dehornoy, *Complete positive group presentations*, J. of Algebra **268** (2003) 156–197.
- [22] P. Dehornoy, *Geometric presentations of Thompson’s groups*, J. Pure Appl. Algebra **203** (2005) 1–44.

- [23] P. Dehornoy, *Mathématiques de l'informatique*, Dunod ; (2000)
- [24] P. Dehornoy, *The group of parenthesized braids*, Advances in Math. **205** (2006) 354–409.
- [25] P. Dehornoy, *The subword reversing method*, Internat. J. Algebra Comput. **21** (2011) 71–118.
- [26] P. Dehornoy, *Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs*, Adv. Math **282** (2015) 93-127.
- [27] P. Dehornoy, *Multifraction reduction I : The 3-Ore case and Artin-Tits groups of type FC*, J. Comb. Algebra **1** (2017) 185–228 arXiv :1606.08991.
- [28] P. Dehornoy, with F. Digne, E. Godelle, D. Krammer, J. Michel, *Foundations of Garside Theory*, EMS Tracts in Mathematics, vol. 22 (2015).
- [29] P. Dehornoy & B. Wiest, *On word reversing in braid groups*, Internat. J. Algebra Comput. **16-5** (2006) 941–957.
- [30] P. Dehornoy, with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Mathematical Surveys and Monographs vol. 148, Amer. Math. Soc. (2008).
- [31] P. Dehornoy & M. Autord, *On the distance between the expressions of a permutations*, Europ. J. Combin. **31** (2010) 1829–1846.
- [32] N. Dershowitz & J.P. Jouannaud, *Rewrite Systems, in Handbook of Theor. Comp. Sc.* vol. B, J. van Leeuwen ed., Elsevier (1994).
- [33] I. Dynnikov, *On a Yang-Baxter mapping and the Dehornoy ordering*, Uspekhi Mat. Nauk **57-3** (2002) 151-152 ; English translation : Russian Math. Surveys, 57-3 (2002) 592–594.
- [34] I. Dynnikov & B. Wiest, *On the complexity of braids*, J. Europ. Math. Soc. **9** (2007) 801–840.
- [35] E.A. El-Rifai & H.R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.
- [36] D. Epstein, with J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).
- [37] F.A. Garside, *The theory of knots and associated problems*, PhD thesis, Oxford (1965).
- [38] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.
- [39] D.F. Holt & S. Rees, *Groups, languages and automata*, London Math. Soc. Student Texts 88, Cambridge Univ. Press (2017)
- [40] G. Huet, *Confluent reductions : abstract properties and applications to term rewriting systems*, Journal of the ACM **27** (1980) 797-821.
- [41] D. Kapur & P. Narendran, *A finite Thue system with decidable word problem and without equivalent finite canonical system*, Theor. Comput. Sci. **35** (1985) 337-344.
- [42] D. Krammer, *An asymmetric generalisation of Artin monoids*, Groups Complexity Cryptology **5** (2013) 141-168.
- [43] V. Lebed & L. Vendramin, *On structure groups of set-theoretic solutions to the Yang-Baxter equation*, arXiv : 1707.00633.
- [44] Y. Lodha & J.T. Moore, *A finitely presented group of piecewise projective homeomorphisms*, Groups Geometry and Dynamics **10** (2016) 177–200.
- [45] R. McKenzie & R.J. Thompson, *An elementary construction of unsolvable word problems in group theory*, in : Word Problems, W.W. Boone and al. eds, Studies in Logic and Foundations of Mathematics, vol. 71, North Holland (1973), pp 457-478.

- [46] F. Müller-Hoissen et al., *Associahedra, Tamari lattices and related structures*, Prog. Math. Phys. vol. 299, Birkhäuser/Springer (2012).
- [47] M.H.A. Newman, *On theories with a combinatorial definition of "equivalence"*, Ann. Math. **43** (1942) 223–243.
- [48] Ø. Ore, *Linear equations in non-commutative fields*, Ann. Math. **34** (1933) 480–508.
- [49] N. Sloane, founder, *A169623*, The online encyclopedia of integer sequences; <https://oeis.org/>.
- [50] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation*, Adv. Math. **193** (2005) 40–55.
- [51] J. Szép, *On factorisable, not simple groups*, Acta Univ. Szeged. Sect. Sci. Math. **13** (1950) 239–241.
- [52] Terese, *Term Rewriting Systems*, Vol. 55 of Cambridge Tracts in Theoretical Computer Science, Cambridge University Press (2003).
- [53] R.J. Thompson, *Transformation structure of algebraic logic*, PhD Thesis Univ. of Berkeley; ProQuest LLC, Ann Arbor, MI (1979), 345 pages, MR2628711.
- [54] W. Thurston, *Finite state algorithms for the braid group*, Circulated notes (1988).
- [55] G. Zappa, *Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro*, Atti Secondo Congresso Un. Mat. Ital., Bologna, Edizioni Cremonense, Rome (1942) pp. 119D125.

Index

- aire, 20
- atome, 9
- bloquer, 53
- clos par complément, 57
- code, 35
- complément, 6, 56
- complémentée, 44
- complétude, 50
- complexité, 35
- concaténation, 1
- condition 3-Ore, 158
- condition du cube, 51
- confluence, 26
- confluence locale, 26
- convergence, 25
- décalage, 17
- diagramme maximal, 48
- diviseur
 - à droite, 5
 - à gauche, 4
- domaine, 70
- élément Δ_n , 104
- élément $\Delta_{n+0,5}$, 106
- éviter, 29
- facteur (mot), 29
- familles $\Sigma_{n,\ell}^0, \Sigma_{n,\ell}^I, \Sigma_{n,\ell}^{II}, \Sigma_{n,\ell}^{III}$, 110
- forme normale, 34
- groupe H , 157
- hauteur, 17
- indice, 107
- lettre, 1
- longueur, 1, 16
- monoïde H^+ , 16
- mot, 1
- mot Δ_n , 104
- mot $\Delta_{n+0,5}$, 106
- mot signé, 44
- noethérianité, 7, 27
- pgcd, 5
- plafond, 18, 19
- plancher, 20
- ppcm, 5
- ppcm à droite conditionnels, 6
- présentation, 2
- présentation récursive, 45
- réussir, 53
- réécriture associée, 24
- règle du domino, 141
- relations $\text{Rel}(S, R, S')$, 67
- représentation
 - $\Phi_{t,s}$, 154
 - $\Phi_F \otimes \Phi_S$, 150
 - fonctionnelle, 145
 - géométrique, 144
 - linéaire, 145
 - spéciale, 145
- retournement, 44
- retournement récursif, 45
- simple, 107
- simplifiable
 - à droite, 4
 - à gauche, 4
- suite de retournement, 45
- suite gloutonne, 135
- support, 17
- terminer, 53
- tête, 139

Un hybride du groupe de Thompson F et du groupe de tresses B_∞ .

Résumé : Nous étudions un monoïde H^+ défini par une présentation \mathcal{P} qui est un hybride de celles du monoïde de tresses infinies et du monoïde de Thompson. Pour cela, nous utilisons plusieurs approches. On décrit d'abord un système de réécriture convergent pour la présentation \mathcal{P} , ce qui fournit en particulier une solution au problème de mots de \mathcal{P} et rapproche H^+ du monoïde de Thompson. Puis, suivant le modèle du monoïde de tresses, on utilise la méthode du retournement de facteur pour analyser la relation de divisibilité à gauche de H^+ , et montrer en particulier que H^+ admet la simplification et des ppcm à droite conditionnels. Ensuite, on étudie la combinatoire de Garside sur H^+ : pour chaque entier n , on introduit un élément Δ_n de H^+ comme ppcm à droite des $n - 1$ premiers atomes, et on étudie les diviseurs à gauche des éléments Δ_n , appelés éléments simples. Les principaux résultats sont les dénombrement des diviseurs à gauche de Δ_n , qui sont $3 \cdot 2^{n-2}$, et la détermination effective des formes normales des éléments simples. On termine en construisant des représentations de H^+ dans divers monoïdes, en particulier une représentation dans des matrices à coefficients polynômes de Laurent dont on conjecture qu'elle est fidèle.

A hybrid of Thompson's group F and the braid group B_∞ .

Abstract : We study a monoid H^+ specified by a presentation \mathcal{P} that is a hybrid of the classical presentation of the infinite braid monoid and of the presentation of Thompson's monoid. To this end, we use several approaches. First, we describe a convergent rewrite system for \mathcal{P} , which provides in particular a solution to the word problem, and makes H^+ reminiscent of Thompson's monoid F^+ . Next, on the shape of the braid monoid, we use the factor reversing method to analyze the divisibility relation of H^+ , and show in particular that H^+ admits cancellation and conditional right lcms. Then, we study Garside combinatorics on H^+ : for every integer n , we introduce an element Δ_n of H^+ as the right lcm of the first $n - 1$ atoms, and one investigates the left divisors of the elements Δ_n , called simple elements. The main results are a counting of the left divisors of Δ_n , which are $2 \cdot 3^{n-2}$ in number, and a characterization of the normal forms of simple elements. We conclude with the construction of several representations of H^+ in various monoids, in particular a representation in a monoid of matrices whose entries are Laurent polynomials, which we conjecture could be faithful.

Mots-clés : monoïde présenté, représentation de monoïdes, retournement de facteur, système de réécriture, théorie de Garside, tresses.