

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

DES GROUPES AUTOMATIQUES
AUX SEMIGROUPES QUASI-AUTOMATIQUES

MÉMOIRE
PRÉSENTÉ COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES

PAR
BENJAMIN BLANCHETTE

OCTOBRE 2019

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

La diffusion de ce mémoire se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév.10-2015). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

TABLE DES MATIÈRES

RÉSUMÉ	iii
INTRODUCTION	1
CHAPITRE 1 NOTIONS PRÉLIMINAIRES	3
Algèbre générale	3
Systèmes d'écriture et dictionnaires	6
Normes et métriques	6
Groupe libre	9
Rationalité, reconnaissabilité et théorèmes classiques	10
Automates	15
Relations multiplicatives	19
Types de dictionnaires rationnels	20
CHAPITRE 2 DES GROUPES AUTOMATIQUES AUX SEMIGROUPES QUASI- AUTOMATIQUES	22
Inclusions générales	22
Dictionnaires Lipschitz	24
Groupes automatiques	26
Monoïdes automatiques	29
Semigroupes rationnels	32
Semigroupes quasi-automatiques	33
Dictionnaires faiblement Lipschitz	34
Groupes quasi-automatiques	36
Semigroupes gradués	39
CHAPITRE 3 ALGORITHMES ET COMPLEXITÉ	41
Décomposition d'une relation rationnelle	41
Problème du mot	43
Éléments inversibles d'un monoïde quasi-automatique	46
Inégalités isopérimétriques	47
CONCLUSION	51
BIBLIOGRAPHIE	52

RÉSUMÉ

Ce mémoire cherche à exposer les différentes classes de semigroupes, monoïdes et groupes définies en fonction de leur complexité de calcul. On y présente les relations connues entre ces classes ainsi que plusieurs résultats relatifs à des problèmes fondamentaux pour ces structures.

Dans le premier chapitre, on introduit les notions algébriques préalables à l'étude de ces objets. La notion classique de partie rationnelle d'un monoïde est critique. Nos travaux utilisent beaucoup les machines abstraites, avec comme prototype l'automate. On présente et utilise aussi les transducteurs, les automates miroir et les automates à deux bandes. Une notion fondamentale particulière à notre sujet est la notion de dictionnaire: un ensemble rationnel de représentants d'une structure algébrique. Les relations multiplicatives élémentaires d'un dictionnaire et leurs caractéristiques comme parties du monoïde produit $A^* \times A^*$ forment notre principal outil dans l'étude de la complexité calculatoire des structures.

Dans le deuxième chapitre, on établit les relations connues entre les diverses classes. Essentiellement, on démontre que les structures automatiques sont asynchrones, qui elles sont quasi-automatiques, et on caractérise géométriquement ces classes avec les propriétés Lipschitz. On démontre aussi que les notions de groupes et monoïdes automatiques ne dépendent pas du choix de système d'écriture. On introduit aussi notre nouvelle classe, les semigroupes quasi-automatiques, et on établit les relations avec les autres classes présentées précédemment. On montre aussi que cette notion ne dépend pas du choix de système d'écriture.

Dans le troisième et dernier chapitre, on présente des théorèmes assurant la décidabilité de plusieurs problèmes computationnels pour les semigroupes quasi-automatiques et automatiques. On montre que le problème du mot est résoluble en temps exponentiel pour les semigroupes quasi-automatiques et en temps quadratique pour les semigroupes automatiques. On montre qu'il est décidable de déterminer si un monoïde quasi-automatique est un groupe. Finalement, on montre qu'il existe une inégalité isopérimétrique exponentielle pour les groupes quasi-automatiques et quadratique pour les groupes automatiques.

Mots-clés: Groupes automatiques, semigroupes quasi-automatiques, complexité algorithmique, théorie des semigroupes, théorie des automates, théorie des langages formels, combinatoire, algèbre abstraite

INTRODUCTION

Les structures algébriques comme les groupes, les monoïdes et les semigroupes ont été étudiées en fonction de leur complexité de calcul par le passé, notamment en relation avec l'informatique théorique et les structures combinatoires comme les automates. Le but de ce mémoire est de dresser un portrait général des classes de semigroupes définies et étudiées dans cette perspective.

Le premier ouvrage notable sur le sujet est définitivement *Word processing in groups* (1992), de Epstein, Cannon, Holt, Levy, Paterson et Thurston, qui réunit dans un même livre la majorité des résultats connus à ce moment sur la classe des groupes automatiques et la classe des groupes asynchrones. Par la suite, plusieurs généralisations ont été réalisées. La définition originale de groupe automatique ne faisant appel qu'à la structure de semigroupe d'un groupe, l'application directe de cette définition aux semigroupes a été investiguée assez rapidement. Dans cette direction, on trouve d'abord les travaux de Duncan, Robertson et Ruskuc, avec leur article *Automatic monoids and change of generators* (1999), investiguant l'application de la définition originale sur les monoïdes. Peu après, Campbell, Robertson, Ruskuc et Thomas étudient le cas des semigroupes avec leur article *Automatic semigroups* (2001). Bien que la majorité des résultats sur les groupes tiennent aussi pour les semigroupes, la notion présente un problème fondamental: un semigroupe peut être automatique en fonction d'un ensemble générateur mais pas en fonction d'un autre.

Cette impasse marque la fin des généralisations qui tentent d'affaiblir le type de structures auxquels on applique les définitions et algorithmes. L'autre direction possible de généralisation, c'est-à-dire d'affaiblir les critères des définitions et donc potentiellement d'augmenter la complexité des algorithmes, est restée plutôt inexplorée jusqu'à tout récemment. Ceci est probablement dû au fait que pour la première généralisation, les structures asynchrones, les algorithmes sont déjà en temps exponentiel.

Dans la foulée des travaux entourant ce mémoire, mon directeur Christophe Reutenauer et moi avons introduit une nouvelle classe généralisant la notion d'asynchrone, qu'on appelle quasi-automatique. Ces travaux nous ont mené à l'écriture d'un article en collaboration

avec Christian Choffrut (IRIF, Paris). Notre article, *Quasi-automatic semigroups* (2019), est publié par Theoretical Computer Science¹ et est disponible en ligne. J'ai aussi un second article, accepté pour publication à la même revue, nommé *Quasi-automatic groups are asynchronously automatic*, présentant un nouveau résultat découvert lors de l'écriture du présent mémoire. Les semigroupes quasi-automatiques ont des propriétés utiles et intéressantes que les semigroupes automatiques n'ont pas, notamment l'indépendance du choix de système d'écriture. En comparaison avec les structures asynchrones, la définition est plus naturelle et praticable. Finalement, la complexité des algorithmes dans le cas quasi-automatique est généralement exponentielle, tout comme pour les structures asynchrones. On a donc une classe plus grande de structures auxquelles s'appliquent des algorithmes aussi efficaces, un gain net.

Notons que le présent mémoire met le focus sur les notions de relation et de dictionnaire. Par le passé, ces notions n'étaient pas nécessairement au centre du discours, les théorèmes portant par exemple sur les groupes munis d'une machine abstraite ayant certaines propriétés. En utilisant le vocabulaire issu de la théorie des langages formels et cette notion clef de dictionnaire, les énoncés sont clairs et concis et les preuves plus directes et élégantes. La majorité des propositions et théorèmes impliquant des structures comme les groupes automatiques sont en fait des résultats qu'on peut montrer directement au niveau des dictionnaires, ce qui nous permet de simplifier les énoncés, et par le fait même, faciliter leurs applications.

¹qualifié de "masterpiece" par l'évaluateur.

CHAPITRE 1

NOTIONS PRÉLIMINAIRES

Ce chapitre introduit les notions et définitions préalables à l'étude des objets qui nous intéressent. On établit les définitions de base pour fixer les notations qu'on utilisera tout au long du mémoire. On énonce quelques résultats classiques qui seront utilisés au cours des chapitres suivants. Les notions de rationalité et de reconnaissabilité sont particulièrement importantes. On introduit différents types de machines abstraites analogues aux automates. On introduit des notions propres à nos objets d'études, telles que les dictionnaires, les relations multiplicatives et les différents types de dictionnaires.

1.1 Algèbre générale

L'ensemble des parties d'un ensemble A est noté $2^A = \{P \subseteq A\}$. Le *produit cartésien* de deux ensembles A et B est noté $A \times B = \{(a, b) : a \in A \text{ et } b \in B\}$. Une partie $r \subseteq A \times B$ est appelée une *relation*. La relation $\{(a, b) : (b, a) \in r\}$ est appelée *relation inverse* de r et est notée r^{-1} . La relation $\{(a, a) : a \in A\}$ est appelée l'*identité* sur A et est notée 1_A . Pour $f \subseteq A \times B$ et $g \subseteq B \times C$, la *composition* de f et g est définie par

$$f \circ g = \{(a, c) : \exists b \in B; (a, b) \in f \text{ et } (b, c) \in g\}$$

Notons que cette définition suit les conventions de Eilenberg, avec les compositions écrites dans le sens de la lecture, de gauche à droite, voir par exemple [7].

On note $r(a)$ l'ensemble des $b \in B$ tel que $(a, b) \in r$. Une relation f telle que $|f(a)| \leq 1$ pour tout a est appelée une *fonction partielle*. Une relation f telle que $|f(a)| = 1$ pour tout a est appelée une *fonction*. Lorsque f est une fonction, on écrit $f : A \rightarrow B$ plutôt que $f \subseteq A \times B$. Pour chaque $a \in A$, l'unique $b \in B$ tel que $(a, b) \in f$ est appelé l'*image* de a sous f et on le note $b = f(a)$.

Si la relation inverse d'une fonction est elle-même une fonction, cette fonction est dite

bijective et sa relation inverse est appelée sa fonction *inverse*. Si la relation inverse d'une fonction f est contenue dans une fonction, f est dite *injective* et toute fonction contenant sa relation inverse est appelée une *post-inverse* de f . Si la relation inverse d'une fonction f contient une fonction, f est dite *surjective* et toute fonction contenue dans son inverse est appelée une *pré-inverse* de f .

Proposition 1.1.1. *Soient r une relation et f une fonction. On a*

$$i) (r^{-1})^{-1} = r.$$

$$ii) g \text{ est post-inverse de } f \text{ si et seulement si } f \circ g = 1_A.$$

$$iii) \text{ La fonction } g \text{ est pré-inverse de } f \text{ si et seulement si } g \circ f = 1_B.$$

$$iv) \text{ La fonction } f \text{ est bijective si et seulement si elle est injective et surjective.}$$

Une fonction $p : S \times S \rightarrow S$ est appelée une *opération binaire* sur l'ensemble S . Si pour tout $a, b, c \in S$ on a $p(p(a, b), c) = p(a, p(b, c))$, p est dite *associative* et (S, p) est appelé un *semigroupe*. On appelle p le *produit* de S et lorsqu'il n'y a pas d'ambiguïté sur l'opération, on note simplement $ab = p(a, b)$ pour tout $a, b \in S$. Si $ab = ba$ pour tout $a, b \in S$, S est dit *commutatif*. Si S et T sont deux semigroupes, $S \times T, ((a, b), (c, d)) \mapsto (ac, bd)$ est un semigroupe qu'on appelle le *produit direct* de S et T .

Un élément $1 \in S$ est appelé *neutre* si $1a = a1 = a$ pour tout a . Un semigroupe contenant un neutre est appelé un *monoïde*. Pour chaque $a \in S$, un élément $b \in S$ tel que $ab = 1$ (respectivement $ba = 1$) est appelé un *inverse à droite* (respectivement à gauche) de a . Un élément $b \in S$ tel que $ab = ba = 1$ est appelé un *inverse* de a . On le note $b = a^{-1}$. Un monoïde où chaque élément est inversible est appelé un *groupe*.

Un ensemble S muni de deux opérations $+$ et \times est appelé un *semi-anneau* si $(S, +)$ est un monoïde commutatif de neutre 0 , appelé *zéro*, (S, \times) est un monoïde de neutre 1 , appelée

unité, et si, pour chaque $a, b, c \in S$, on a

$$a0 = 0a = 0$$

$$a(b + c) = ab + ac$$

$$(a + b)c = ac + bc$$

Si de plus $(S, +)$ est un groupe, S est appelé un *anneau*.

Soit A un ensemble fini. L'ensemble des suites finies d'éléments de A , noté A^* , muni de l'opération

$$((a_1, \dots, a_n), (b_1, \dots, b_m)) \mapsto (a_1, \dots, a_n, b_1, \dots, b_m)$$

est un monoïde qu'on appelle le *monoïde libre* sur A . On identifie les singletons $\{a\}$ avec les éléments $a \in A$. On peut donc omettre les parenthèses sans ambiguïté. On appelle A un *alphabet*, ses éléments des *lettres* et les suites de lettres des *mots*. Si $w = pfs$ avec $p, f, s \in A^*$, on dit que p est *préfixe* de w , s est *suffixe* de w et f est *facteur* de w . Pour tout mot $w \in A^*$, $|w|$ désigne sa longueur, c'est-à-dire le nombre de lettres qui le composent. On appelle l'unique suite de longueur 0 le *mot vide*, qu'on note 1. Notons aussi que $A^+ = A^* - \{1\}$ est un semigroupe. On l'appelle le *semigroupe libre* sur A . Un ensemble de mot, c'est-à-dire une partie $L \subset A^*$, est appelé un *langage*.

Définition 1.1.2. Morphismes

Soient S et T deux semigroupes. Une fonction $f : S \rightarrow T$ est appelé un *morphisme de semigroupes* si, pour tout $a, b \in S$, on a $f(ab) = f(a)f(b)$. Si de plus S et T sont des monoïdes et $f(1_S) = 1_T$, f est appelé un *morphisme de monoïdes*. Si de plus S et T sont des groupes et $f(a^{-1}) = f(a)^{-1}$ pour tout $a \in S$, f est appelé un *morphisme de groupes*. Notons que les morphismes de semigroupes d'un groupe dans un autre sont tous des morphismes de groupes. Une fonction $f : R \rightarrow S$ entre semi-anneaux qui est un morphisme de monoïdes $(R, +) \rightarrow (S, +)$ et un morphisme de monoïdes $(R, \times) \rightarrow (S, \times)$ est appelé un *morphisme de semi-anneaux*. Si de plus R et S sont des anneaux et que $(R, +) \rightarrow (S, +)$ est un morphisme de groupes, f est appelé un *morphisme d'anneaux*. On utilise la flèche \hookrightarrow pour les morphismes injectifs, la flèche \twoheadrightarrow pour les morphismes surjectifs et la flèche \leftrightarrow

pour les morphismes bijectifs. Un morphisme bijectif est appelé un *isomorphisme*.

Les morphismes de monoïdes $f : A^* \rightarrow M$ sont entièrement définis par l'image des lettres $a \in A$. En effet, tout élément de A^* s'écrit $w = a_1 \dots a_{|w|}$ pour certains $a_i \in A$ et donc $f(w) = f(a_1) \dots f(a_{|w|})$ est déterminé entièrement par l'image des lettres.

1.2 Systèmes d'écriture et dictionnaires

Soient S un semigroupe et A un alphabet fini. Un morphisme $p : A^+ \rightarrow S$ est appelé un *système d'écriture* de S s'il est surjectif. S est dit *finiment engendré* s'il admet un système d'écriture. Un langage $L \subseteq A^+$ telle que $p(L) = S$ est appelée un *dictionnaire* de S utilisant le système d'écriture p et chaque mot $m \in L$ est appelée une *orthographe* de $p(m)$.

Donné un semigroupe et un système d'écriture $p : A^+ \rightarrow S$, on définit la relation d'équivalence \sim_p sur A^+ en posant $m \sim_p n \iff p(m) = p(n)$. S'il n'y a pas d'ambiguïté sur le système d'écriture, on omet la mention du p et on écrit simplement $m \sim n$.

1.3 Normes et métriques

Soit S un semigroupe. Une fonction $|\cdot| : S \rightarrow \mathbb{N}$ est appelée une *norme* sur S si $|xy| \leq |x| + |y|$ pour tout $x, y \in S$. La longueur d'un mot est une norme sur A^+ et A^* .

Donné un système d'écriture $p : A^+ \rightarrow S$, on définit sur S la *norme induite* par p en posant, pour tout $s \in S$,

$$|s| = \min\{|w| : p(w) = s\}$$

C'est bien une norme car si w_s, w_t sont des mots de longueur minimale représentant $s, t \in S$, alors $w_s w_t$ représente st et $|st| \leq |w_s| + |w_t| = |s| + |t|$. On utilise cette norme pour induire une norme sur A^+ en posant $|w|_S = |p(w)|$.

Une fonction $m : S \times S \rightarrow \mathbb{R}$ est appelée une *métrique* sur S si les quatres conditions

suivantes sont vérifiées.

$$m(x, x) = 0 \quad (1)$$

$$\text{si } y \neq x, m(x, y) > 0 \quad (2)$$

$$m(x, y) = m(y, x) \quad (3)$$

$$m(x, z) \leq m(x, y) + m(y, z) \quad (4)$$

pour tout $x, y, z \in S$. On définit une métrique sur A^+ en posant

$$d_{A^+}(u, v) = \min\{|s| + |s'| : s, s' \in A^*, \exists w \in A^*; u = ws \text{ et } v = ws'\}$$

Montrons que c'est bien une métrique. D'abord, $d_{A^+}(x, x) = 0$ car $x1 = x1$ et $|1| = 0$. Ensuite, supposons que $d_{A^+}(x, y) = 0$. Alors il existe $s, s', w \in A^*$ tels que $x = ws, y = ws'$ et $|s| + |s'| = 0$. Comme le seul mot de longueur 0 est le mot vide 1, il faut que $s = s' = 1$, et donc $x = w1 = y$. Par contraposée, si $x \neq y$, $d_{A^+}(x, y) > 0$. Ensuite, si $d_{A^+}(x, y) = c$, alors il existe $s, s', w \in A^*$ tels que $ws = x, ws' = y$ et $|s| + |s'| = c$ et $d_{A^+}(y, x) = c$. Finalement, si $d_{A^+}(x, y) = c, d_{A^+}(y, z) = c'$, il existe $w, s, s', u, t, t' \in A^*$ tels que $ws = x, ws' = y = ut, z = ut'$ avec $|s| + |s'| = c, |t| + |t'| = c'$. Alors soit w est préfixe de u ou u est préfixe de w . Supposons d'abord le premier. Alors $u = ww'$ pour un certain $w' \in A^+$. De plus, on a $y = ws' = ut = ww't$, ce qui assure que w' est de longueur au plus $|s'|$. On obtient alors $x = ws, z = ww't'$, si bien que

$$d_{A^+}(x, z) \leq |s| + |w'| + |t'| \leq |s| + |s'| + |t| + |t'| = c + c' = d_{A^+}(x, y) + d_{A^+}(y, z)$$

Pour le cas symétrique, $w = uu'$ avec $|u'| \leq |t|$ et on obtient

$$d_{A^+}(x, z) \leq |s| + |u'| + |t'| \leq |s| + |s'| + |t| + |t'| = c + c' = d_{A^+}(x, y) + d_{A^+}(y, z)$$

Similairement à la norme, un système d'écriture $p : A^+ \rightarrow S$ induit une métrique sur S , qu'on appelle la *métrique du mot*. Deux éléments du semigroupe à distance 1 l'un de l'autre s'ils admettent une écriture à distance 1 l'un de l'autre; explicitement

$$d_p(x, y) = 1 \iff \exists u_x, u_y \in A^+ \text{ tels que } d_{A^+}(u_x, u_y) = 1, p(u_x) = x, p(u_y) = y$$

On étend cette notion de distance en utilisant la notion de chemin minimal. Explicitement, pour tout $x, y \in S$ on pose

$$d_p(x, y) = \min\{n \in \mathbb{N} \mid \exists x_1, \dots, x_{n+1} \in S \text{ tels que } x_1 = x, x_{n+1} = y, d_p(x_i, x_{i+1}) = 1 \forall i \leq n\}$$

Montrons que c'est bien une métrique. D'abord, $d_p(x, y) = 0$ si et seulement s'il existe un x_1 tel que $x = x_1 = y$, ce qui montre les deux premières propriétés. Ensuite, notons d'abord que comme la distance est induite par d_{A^+} , $d_p(x, y) = 1$ si et seulement si $d_p(y, x) = 1$. Supposons qu'il existe $x = x_1, \dots, x_{n+1} = y$ tels que $d_p(x_i, x_{i+1}) = 1 \forall i$. On pose alors $y_i = x_{n+2-i}$, ce qui assure que $y_1 = x_{n+2-1} = x_{n+1} = y$ et $y_{n+1} = x_{n+2-(n+1)} = x_1 = x$ et que $d_p(y_i, y_{i+1}) = d_p(x_{n+2-i}, x_{n+1-i}) = d_p(x_{n+1-i}, x_{n+2-i}) = 1$. On a donc $d_p(y, x) \leq d_p(x, y)$ pour tout x, y . En répétant l'argument, on obtient $d_p(y, x) \leq d_p(x, y) \leq d_p(y, x)$, ce qui assure que $d_p(x, y) = d_p(y, x)$. Finalement, supposons que $d_p(x, y) = n$ et $d_p(y, z) = m$. Alors il existe $x_1, \dots, x_{n+1}, y_1, \dots, y_{m+1}$ tels que $x_1 = x, x_{n+1} = y = y_1, y_{m+1} = z$. On pose $x_{n+i} = y_i$ pour tout $n+2 \leq i \leq m+1$. On obtient alors $x_{n+m+1} = z$ et $d_p(x_i, x_{i+1}) = 1 \forall i \leq n+m$, ce qui assure que $d_p(x, z) \leq n+m = d_p(x, y) + d_p(y, z)$.

Pour alléger la notion, on pose, pour $w, w' \in A^+$,

$$d_p(w, w') = d_p(p(w), p(w'))$$

Notons que ce n'est pas forcément une métrique sur A^+ ; il peut très bien y avoir deux mots distincts représentant le même élément du semigroupe, une contradiction au premier axiome d'une métrique. Notons que $d_p(w, w') \leq d_{A^+}(w, w')$ pour tout mot w, w' .

Une métrique d sur un ensemble S induit une métrique sur 2^S . Pour $x \in S$ et $A \subseteq S$, on pose

$$d(x, A) = \inf\{d(x, a) \mid a \in A\}$$

et pour tout $A, B \subseteq S$,

$$d(A, B) = \sup\{\{d(a, B) \mid a \in A\} \cup \{d(A, b) \mid b \in B\}\}$$

Cette métrique est appelée la *métrique de Hausdorff* relative à d .

1.4 Groupe libre

Pour les systèmes d'écriture de groupes, on choisit un alphabet A possédant des propriétés particulières. On choisit d'abord un alphabet fini quelconque, disons B , puis on pose $A = B \cup \{a^{-1} | a \in B\}$. On définit une involution naturelle $^{-1} : A^* \rightarrow A^*$ en posant, pour tout $a, a_1, \dots, a_n \in A$,

$$(a^{-1})^{-1} = a \quad \text{et} \quad (a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$$

On note \sim_F la relation engendrée par l'ensemble des $aa^{-1} = 1$ et $a^{-1}a = 1$ pour tout $a \in A$. Le monoïde quotient $F(A) = A^* / \sim_F$ est un groupe qu'on appelle le *groupe libre* sur A . On note $F : A^* \rightarrow F(A)$ le morphisme surjectif canonique. Notons que c'est un système d'écriture de $F(A)$.

Pour un groupe quelconque G , on dit qu'un système d'écriture $p : A^+ \rightarrow G$ est un *système d'écriture de groupe* si A est tel que décrit ci-haut et si $p(w)^{-1} = p(w^{-1})$ pour tout $w \in A^+$. Dans ce cas, on a une autre expression pour la métrique du mot, comme le montre la proposition suivante.

Proposition 1.4.1. *Soit $p : A^+ \rightarrow G$ un système d'écriture de groupe. Alors pour tout $x, y \in G$,*

$$d_p(x, y) = \min\{d_{A^+}(u, v) | p(u) = x, p(v) = y\}$$

et

$$d_p(x, y) = |x^{-1}y|_G$$

D'abord, remarquons que si $d_p(x, y) = 1$, alors $xa = y$ ou $x = ya$ pour un certain $a \in A$, et comme on a un système d'écriture de groupe, on a alors $x = ya^{-1}$ ou $xa^{-1} = y$. Ainsi, l'équivalence entre la définition de d_p de la section 1.3 et celle de la présente proposition est évidente: si $d_p(x, y) = n$, il existe une suite de mots x_1, \dots, x_{n+1} tels que $x_1 x_2^{\pm 1} \dots x_n^{\pm 1} = x_{n+1}$ et $p(x_1) = x, p(x_{n+1}) = y$.

Comme A est stable sous inversion, $|x|_G = |x^{-1}|_G$ pour tout $x \in G$. Supposons que $d_p(x, y) = c$. Alors il existe $u \sim x, v \sim y, w, s, s' \in A^*$ tels que $u = ws, v = ws'$ et $|s| + |s'| = c$.

Alors $x^{-1}y \sim u^{-1}v = s^{-1}w^{-1}ws' \sim s^{-1}s'$, ce qui assure que

$$|x^{-1}y|_G \leq |s^{-1}| + |s'| = |s| + |s'| = c = d_p(x, y)$$

Réciproquement, supposons que $|x^{-1}y|_G = c'$. Soient $w \sim x$ et $s \sim x^{-1}y$ des mots de longueur minimale représentant respectivement x et $x^{-1}y$. Alors $ws \sim x(x^{-1}y) \sim y$ et $w(1) \sim x$, ce qui assure que

$$d_p(x, y) \leq |s| = c' = |x^{-1}y|_G$$

□

Tout système d'écriture de groupe $p : A^+ \rightarrow G$ peut se factoriser en morphismes de semi-groupes surjectifs successifs

$$A^+ \xrightarrow{F} F(A) \xrightarrow{q} G$$

Pour tout $w \in A^*$, on appelle $|w|_{F(A)}$ la *longueur réduite* d'un mot. Notons que donné un système d'écriture de groupe $p : A^+ \rightarrow G$, on obtient ainsi trois notions de norme sur A^+ ; la longueur $|\cdot|$, la longueur réduite $|\cdot|_{F(A)}$, et la norme $|\cdot|_G$. De plus, pour tout $w \in A^+$, on a

$$|w|_G \leq |w|_{F(A)} \leq |w|$$

1.5 Rationalité, reconnaissabilité et théorèmes classiques

Soit M un monoïde. Pour $A, B \subseteq M$ on définit le *produit* et l'*étoile* en posant

$$\begin{aligned} AB &= \{ab : a \in A, b \in B\} & A_n &= \bigcup_{k=0}^n A^k \\ A^0 &= \{1_M\} & A^* &= \bigcup_{k \geq 0} A^k \\ A^k &= AA^{k-1} \quad \forall k \geq 1 \end{aligned}$$

L'ensemble des parties d'un monoïde est un semi-anneau avec l'union ensembliste comme somme et $(A, B) \mapsto AB$ comme produit. De plus, l'ensemble vide \emptyset est le zéro de ce semi-anneau et $\{1_M\}$ est l'unité.

L'ensemble des *parties rationnelles* d'un monoïde est la plus petite famille de parties contenant les parties finies qui est stable sous l'union finie, le produit et l'étoile. On note cet ensemble $\text{Rat}(M)$. Un langage $L \subseteq A^*$ qui est une partie rationnelle du monoïde libre A^* est appelé un *langage rationnel*.

Proposition 1.5.1. *Soit $f : M \rightarrow N$ un morphisme de monoïdes. Alors*

$$P \in \text{Rat}(M) \implies f(P) \in \text{Rat}(N)$$

Soit \mathcal{F} la classe des sous-ensembles $P \subseteq M$ tels que $f(P) \in \text{Rat}(N)$. \mathcal{F} contient tous les ensembles finis car si P est fini, $f(P)$ l'est aussi et est donc rationnel. Montrons que \mathcal{F} est stable sous union finie, produit et étoile. Soient $P, Q \in \mathcal{F}$. Alors $f(P), f(Q) \in \text{Rat}(N)$. On obtient

$$f(P \cup Q) = f(P) \cup f(Q) \in \text{Rat}(N)$$

$$f(PQ) = f(P)f(Q) \in \text{Rat}(N)$$

$$f(P^*) = f(P)^* \in \text{Rat}(N)$$

Comme \mathcal{F} contient les ensembles finis et est stable sous les opérations rationnelles, il contient $\text{Rat}(M)$, si bien que $P \in \text{Rat}(M)$ implique $P \in \mathcal{F}$ qui implique $f(P) \in \text{Rat}(N)$. \square

Proposition 1.5.2. *Soit $f : M \rightarrow N$ un morphisme surjectif de monoïde. Alors pour toute partie rationnelle $Q \subseteq N$ il existe une partie rationnelle $P \subseteq M$ telle que $f(P) = Q$.*

Soit \mathcal{F} la classe de sous-ensembles $Q \subseteq N$ tels qu'il existe $P \in \text{Rat}(M)$ avec $f(P) = Q$. Comme f est surjective, pour tout $n \in N$ il existe $m \in M$ tel que $f(m) = n$. Le singleton $\{m\}$ est rationnel, ce qui assure que $\{n\} \in \mathcal{F}$ pour tout $n \in N$. Maintenant, soient $Q, Q' \in \mathcal{F}$. Alors il existe $P, P' \in \text{Rat}(M)$ tel que $f(P) = Q, f(P') = Q'$. On a donc $P \cup P' \in \text{Rat}(M)$ et $f(P \cup P') = f(P) \cup f(P') = Q \cup Q'$, ce qui assure que $Q \cup Q' \in \mathcal{F}$. Similairement, $PP' \in \text{Rat}(M), f(PP') = f(P)f(P') = QQ' \in \mathcal{F}, P^* \in \text{Rat}(M), f(P^*) = f(P)^* = Q^* \in \mathcal{F}$. Donc $\mathcal{F} \supseteq \text{Rat}(N)$.

$P \subseteq M$ est dite *reconnaissable* s'il existe un monoïde fini F , un morphisme de monoïdes $f : M \rightarrow F$ et $P' \subseteq F$ tel que $f^{-1}(P') = P$. On note $\text{Rec}(M)$ l'ensemble des parties reconnaissables de M .

Proposition 1.5.3. *$\text{Rec}(M)$ est stable sous union finie, intersection, complémentation et morphisme inverse.*

Soient M, N des monoïdes quelconques, F, G des monoïdes finis, $f : M \rightarrow F, g : M \rightarrow G, h : N \rightarrow M$ des morphismes de monoïde, $P, Q \subseteq M, P' \subseteq F, Q' \subseteq G$ tels que $f^{-1}(P') = P$ et $g^{-1}(Q') = Q$. On considère le morphisme produit $f \times g : M \rightarrow F \times G, m \mapsto (f(m), g(m))$. On a alors

$$\begin{aligned}
P \cap Q &= \{m \in M : f(m) \in P', g(m) \in Q'\} \\
&= \{m \in M : (f \times g)(m) \in P' \times Q'\} \\
&= (f \times g)^{-1}(P' \times Q') \\
P \cup Q &= \{m \in M : f(m) \in P'\} \cup \{m \in M : g(m) \in Q'\} \\
&= \{m \in M : (f \times g)(m) \in P' \times G\} \cup \{m \in M : (f \times g)(m) \in F \times Q'\} \\
&= (f \times g)(P' \times G) \cup (f \times g)(F \times Q') \\
&= (f \times g)(P' \times G \cup F \times Q') \\
M - P &= f^{-1}(F - P') \\
h^{-1}(P) &= h^{-1}(f^{-1}(P')) \\
&= (h \circ f)^{-1}(P')
\end{aligned}$$

ce qui montre la proposition. □

Théorème 1.5.4. *(Kleene, 1956) Une partie d'un monoïde libre est rationnelle si et seulement si elle est reconnaissable.*

Ce théorème est considéré par plusieurs comme le théorème fondamental en théorie des automates. On peut trouver une preuve dans la plupart des ouvrages généraux en théorie des automates, voir par exemple Eilenberg [7], Theorem VII.5.1.

Corollaire 1.5.5. *Soient $f : A^* \rightarrow B^*$ un morphisme, $L, K \in \text{Rat}(A^*), R \in \text{Rat}(B^*)$.*

Alors

$$L \cap K, L - K, f^{-1}(R) \in \text{Rat}(A^*)$$

On a montré que les parties reconnaissables sont stables sous intersection, complémentation et morphisme inverse, ce qui assure alors que les parties rationnelles de monoïdes libres, qui sont reconnaissables par le théorème de Kleene, le sont aussi. \square

Théorème 1.5.6. (Mc Knight, 1964) *Les parties reconnaissables d'un monoïde finiment engendré sont rationnelles.*

Soient M un monoïde finiment engendré, $p : A^* \rightarrow M$ un système d'écriture et $P \in \text{Rec}(M)$. Alors comme p^{-1} est un morphisme inverse, $p^{-1}(P) \in \text{Rec}(A^*)$. Par le théorème de Kleene, c'est alors une partie rationnelle de A^* . Comme p est surjective, $p^{-1} \circ p = 1_M$, et comme p est un morphisme de monoïdes, on a alors $P = (p^{-1} \circ p)(P) = p(p^{-1}(P)) \in \text{Rat}(M)$ par la Proposition 1.5.1. \square

Proposition 1.5.7. *Soient M un monoïde et $P, Q \subseteq M$ telles que P est rationnelle et Q est reconnaissable. Alors $P \cap Q$ est rationnelle.*

Comme P est rationnelle, on peut l'exprimer en fonction d'un nombre fini de singleton de M . On considère le sous monoïde de M engendré par ces singletons et stable sous étoile, disons $N \subseteq M$. Notons que P est une partie rationnelle de N et qu'en associant à chacun des singletons une lettre et en regroupant cet ensemble de lettre en un alphabet A , on obtient un système d'écriture $p : A^* \rightarrow N$. Comme il s'agit d'un morphisme surjectif de monoïde, on peut appliquer la Proposition 1.5.2; on obtient donc un langage rationnel $L_P \subseteq A^*$ tel que $p(L_P) = P$. Le théorème de Kleene assure que ce langage est aussi reconnaissable. Comme Q est reconnaissable, la Proposition 1.5.3 assure que $L_Q = p^{-1}(Q) \subseteq A^*$ est un langage reconnaissable. Alors $L_P \cap L_Q$ est reconnaissable par la Proposition 1.5.3. Le théorème de Kleene assure donc qu'il est rationnel, et la Proposition 1.5.1 assure que $p(L_P \cap L_Q)$ est aussi rationnelle. Mais

$$p(L_P \cap L_Q) = p(L_P \cap p^{-1}(Q)) = p(L_P) \cap Q = P \cap Q$$

\square

Soit A un alphabet fini. On pose $A_{gd} = A \times \{g, d\}$ et on définit les morphismes

$$\begin{array}{ll} \pi_g : A_{gd}^* \rightarrow A^* & \pi_d : A_{gd}^* \rightarrow A^* \\ \pi_g(a, g) = a & \pi_d(a, g) = 1 \\ \pi_g(a, d) = 1 & \pi_d(a, d) = a \end{array}$$

Ils sont respectivement appelés *projection à gauche* et *projection à droite*. On pose $\pi = \pi_g \times \pi_d$.

Théorème 1.5.8. (Nivat, 1968) *Une relation $R \subseteq A^* \times A^*$ est une partie rationnelle du monoïde $A^* \times A^*$ si et seulement s'il existe un langage rationnel $H \subseteq A_{gd}^*$ tel que*

$$R = \pi(H) = \{(\pi_g(w), \pi_d(w)) : w \in H\}$$

Soit $R \in \text{Rat}(A^* \times A^*)$. Le morphisme $\pi : A_{gd}^* \rightarrow A^* \times A^*$ est surjectif, ce qui nous permet d'appliquer la Proposition 1.5.2. Il existe donc $H \in \text{Rat}(A_{gd}^*)$ tel que $\pi(H) = R$. Réciproquement, soit $H \in \text{Rat}(A_{gd}^*)$. La Proposition 1.5.1 nous permet de conclure que $\pi(H) = R$ est rationnel. \square

Ce théorème est particulièrement important pour la suite. On utilise cette caractérisation des parties rationnelles de $A^* \times A^*$, qu'on appelle *relations rationnelles*, plutôt que la définition générale de partie rationnelle. On appelle un langage $H \subseteq A_{gd}^*$ tel que $\pi(H) = R$ un *langage de Nivat* pour la relation R . C'est le théorème qui nous permet, bien que partiellement, d'appliquer les outils de la théorie algébrique des automates.

Théorème 1.5.9. (Elgot et Mezei, 1965) *Si $R \subseteq A^* \times B^*$ et $T \subseteq B^* \times C^*$ sont rationnelles, $R \circ T \subseteq A^* \times C^*$ est rationnelle.*

Ce théorème classique est aussi utile dans notre contexte. Pour une preuve, voir par exemple Elgot et Mezei [9], ou Berstel [2], Theorem III.4.4.

1.6 Automates

Un *automate* sur un alphabet A est un quadruplet $W = (Q, T, I, F)$ où

Q est un ensemble fini d'*états*

$T \subseteq Q \times A \times Q$ est un ensemble fini de *transitions*

$I \subseteq Q$ est un ensemble d'états appelés *initiaux*

$F \subseteq Q$ est un ensemble d'états appelés *finaux*

On note les transitions $p \xrightarrow{a} q$ plutôt que (p, a, q) . Deux transitions $p \xrightarrow{a} q$ et $r \xrightarrow{b} s$ sont dites *compatibles* si $q = r$. Une suite de transitions compatibles est appelée un *chemin*. Un mot $a_1 \dots a_n \in A^*$ est dit *reconnu* par l'automate s'il existe un chemin $q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} q_n$ tel que $q_0 \in I$ et $q_n \in F$. On note $L(W)$ l'ensemble des mots reconnus par l'automate W .

Un automate est dit *déterministe* si $p \xrightarrow{a} q, p \xrightarrow{a} q' \in T \implies q = q'$ et $|I| = 1$. Dans ce cas, on peut noter un chemin $p \xrightarrow{a_1 \dots a_n} q$ sans ambiguïté car on peut itérativement déterminer les états visités. De plus, on peut considérer T comme une fonction partielle $Q \times A \rightarrow Q$. On note alors $pa = q$ pour toute flèche $p \xrightarrow{a} q$. On étend la fonction partielle T à une fonction partielle $Q \times A^* \rightarrow Q$ en posant $p(a_1 \dots a_n) = (((pa_1)a_2) \dots a_n)$.

On généralise la notion d'automate sur A à la notion d'automate sur un monoïde quelconque M . La notion est essentiellement la même; un quadruplet $W = (Q, T, I, F)$ où Q est un ensemble fini, T est une partie finie de $Q \times M \times Q$ et $I, F \subseteq Q$ sont les états initiaux et finaux. Un élément $m \in M$ est reconnu par l'automate si et seulement s'il existe des éléments $m_1, \dots, m_n \in M$ tels que $m = m_1 \dots m_n$ et qu'il existe un chemin

$$I \ni q_0 \xrightarrow{m_1} q_1 \rightarrow \dots \xrightarrow{m_n} q_n \in F$$

L'ensemble des éléments de M qui sont reconnus par l'automate est noté $L(W)$ comme pour les automates standards.

Un automate M sur le monoïde $A^* \times A^*$ est appelé un *transducteur*. La relation

$$R(M) = \{(u_1 \dots u_n, v_1 \dots v_n) \mid (u_1, v_1) \dots (u_n, v_n) \in L(M)\}$$

est appelée la *relation reconnue* par le transducteur. Un transducteur où $T \subseteq Q \times (A \times A^*) \times Q$ et où

$$p \xrightarrow{a,u} q, p \xrightarrow{a,u'} q' \implies u = u', q = q'$$

est appelé un transducteur *séquentiel*. Remarquons que dans ce cas, la relation reconnue est une fonction partielle. On appelle une fonction reconnue par un transducteur séquentielle une *fonction séquentielle*.

Plutôt que de noter les transitions d'un transducteur séquentiel sous la forme $p \xrightarrow{a,u} q$, on note $p \xrightarrow{a} q$ et séparément $(p, a) \mapsto u$. Ainsi, si pour tout $1 \leq i \leq n$ on a $(p_{i-1}, a_i) \mapsto u_i$ et

$$I \ni p_0 \xrightarrow{a_1} p_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} p_n \in F$$

l'image de $a_1 \dots a_n$ sous la fonction séquentielle associée au transducteur est $u_1 \dots u_n$.

On définit les automates *miroir* en effectuant la lecture de droite à gauche plutôt que de gauche à droite. Formellement, un automate miroir sur un monoïde M est un quadruplet (Q, T, I, F) où Q est un ensemble fini, T est une partie finie de $Q \times M \times Q$, $I, F \subseteq Q$ sont des états initiaux et finaux. Un élément $m \in M$ est reconnu par l'automate si et seulement s'il existe des éléments $m_1, \dots, m_n \in M$ tels que $m = m_1 \dots m_n$ et qu'il existe un chemin

$$I \ni q_0 \xrightarrow{m_n} q_1 \xrightarrow{m_{n-1}} \dots \xrightarrow{m_1} q_n \in F$$

Proposition 1.6.1. (*Rabin et Scott, 1959*) *Soit W un automate. Il existe W' un automate déterministe tel que $L(W) = L(W')$.*

Un algorithme simple permet de construire un automate déterministe à partir d'un automate quelconque. Pour un automate (Q, T, I, F) , on peut par exemple construire l'automate

$(2^Q, \tilde{T}, \{I\}, \tilde{F})$ où

$$\tilde{F} = \{P \in 2^Q \mid P \cap F \neq \emptyset\}$$

$$P \xrightarrow{a} P' \in \tilde{T} \iff P' = \bigcup_{p \in P} \{q \mid p \xrightarrow{a} q \in T\}$$

et vérifier qu'il reconnaît bien le même langage tout en étant déterministe. \square

Un état q est dit *accessible* s'il existe un chemin $p \xrightarrow{w} q$ avec $p \in I$ et *coaccessible* s'il existe un chemin $q \xrightarrow{w} r$ avec $r \in F$. Un état à la fois accessible et coaccessible est dit *actif* et un état qui n'est pas actif est dit *inactif*. On appelle *accessible* (respectivement *coaccessible*) un automate dont tous les automates sont accessibles (respectivement coaccessibles).

Proposition 1.6.2. Soient $W = (Q, T, I, F)$ un automate et $P \subseteq Q$ un sous ensemble d'états inactifs. On pose $Q' = Q - P$ et on considère l'automate $\tilde{W} = (Q', T \cap (Q' \times A \times Q'), I \cap Q', F \cap Q')$. Alors $L(W) = L(\tilde{W})$.

Les propositions précédentes nous assurent que lorsqu'on considère un automate quelconque, on peut supposer qu'il est déterministe, accessible ou coaccessible sans perdre de généralité.

Proposition 1.6.3. L'ensemble des langages de A^* qui sont reconnaissables par un automate est exactement $\text{Rec}(A^*)$ tel que défini à la section 1.5.

Pour montrer l'équivalence, on utilise le *monoïde de transition* d'un automate, une construction classique, voir par exemple Pin [11], Theorem IV.3.20.

Définition 1.6.4. Soient A un alphabet fini, $*$ $\notin A$ un symbole dit de remplissage et $R \subseteq A^* \times A^*$ une relation. On plonge R dans le monoïde libre sur $A_{(2)} = (A \cup \{*\}) \times (A \cup \{*\})$ avec une fonction $r : A^* \times A^* \rightarrow (A_{(2)})^*$ définie par

$$r(a_1 \dots a_{|a|}, b_1 \dots b_{|b|}) = \begin{cases} (a_1, b_1) \dots (a_{|a|}, b_{|b|}) & \text{si } |a| = |b| \\ (a_1, b_1) \dots (a_{|a|}, b_{|a|}) (*, b_{|a|+1}) \dots (*, b_{|b|}) & \text{si } |a| < |b| \\ (a_1, b_1) \dots (a_{|b|}, b_{|b|}) (a_{|b|+1}, *) \dots (a_{|a|}, *) & \text{si } |a| > |b| \end{cases}$$

pour tout $a = a_1 \dots a_{|a|}$ et $b = b_1 \dots b_{|b|} \in A^*$. r est appelée *fonction de remplissage*.

Proposition 1.6.5. (*Baumslag et al., 1991*) Soient $L, K \subseteq A^*$ deux langages reconnaissables. Alors $r(L \times K) \subseteq (A_{(2)})^*$ est reconnaissable.

Soient (Q, T, I, F) un automate reconnaissant L et (Q', T', I', F') un automate reconnaissant K . Soit $s \notin (Q \cup Q')$. On considère l'automate où l'ensemble d'états est $(Q \cup \{s\}) \times (Q' \cup \{s\})$, l'ensemble d'états initiaux est $I \times I'$, l'ensemble d'états finaux est $(F \cup \{s\}) \times (F' \cup \{s\}) - \{(s, s)\}$ et où les transitions sont données par

$$\begin{aligned} (p, q) &\xrightarrow{a,b} (pa, qb) && \forall a, b \in A, p \in Q, q \in Q' \\ (p, q) &\xrightarrow{a,*} (pa, s) && \forall b \in A, p \in Q, q \in F' \cup \{s\} \\ (p, q) &\xrightarrow{*,b} (s, qb) && \forall a \in A, p \in F \cup \{s\}, q \in Q' \end{aligned}$$

Cet automate reconnaît exactement $r(L \times K)$. Essentiellement, il lit les deux mots en parallèle et l'état supplémentaire s marque la fin de la lecture d'un mot, s'assurant qu'on ne recommence pas à lire des lettres du côté d'un mot qu'on a terminé de lire. \square

Proposition 1.6.6. (*Eilenberg*) Soit $R \subseteq A^* \times A^*$ une relation rationnelle telle que

$$(u, v) \in R \implies |u| = |v|$$

Alors $r(R)$ est une partie rationnelle de $(A \times A)^*$.

Pour une preuve, voir Eilenberg [7], Theorem IX.6.1.

Définition 1.6.7. On considère à nouveau un symbole $*$ $\notin A$, qui servira maintenant à marquer les fins de mots. Un *automate à deux bandes* sur A est un quintuplet $W = (Q, T, I, F, P)$ où (Q, T, I, F) est un automate déterministe sur $A \cup \{*\}$ et où $P \subseteq Q$ est une partie des états. Il reconnaît des relations $R \subseteq A^* \times A^*$ plutôt que des langages.

Pour chaque mot $w = a_1 \dots a_n$ reconnu par l'automate déterministe, on considère le chemin

$i \xrightarrow{w} f$. Comme il est déterministe, on peut déterminer la suite d'états visités et le réécrire

$$i \xrightarrow{a_1} p_1 \xrightarrow{a_2} \dots \xrightarrow{a_{n-1}} p_{n-1} \xrightarrow{a_n} f$$

On considère le mot suivant sur l'alphabet $Q \times A$:

$$m = (i, a_1)(p_1, a_2)\dots(p_{n-1}, a_n)$$

On y applique les morphismes $g, d : (Q \times A)^* \rightarrow (A \cup \{*\})^*$ donnés par

$$\begin{aligned} g(q, a) &= a \quad \forall q \in P & d(q, a) &= 1 \quad \forall q \in P \\ g(q, a) &= 1 \quad \forall q \notin P & d(q, a) &= a \quad \forall q \notin P \end{aligned}$$

Si $g(m) = w_1*$ et $d(m) = w_2*$ pour certains mots $w_1, w_2 \in A^*$, on dit que le couple (w_1, w_2) est reconnu par W . L'ensemble des couples reconnus par W est appelé la *relation reconnue par W* et est notée $R(W)$. Notons que cette définition implique que seuls les mots reconnus contenant exactement deux fois le caractère spécial $*$ contribuent à la relation reconnue. Par exemple, on peut très bien avoir un automate qui reconnaît un mot w tel que $g(w) = u*$ et $d(w) = v**$ pour certains mots $u, v \in A^*$, mais le couple (u, v) ne sera pas dans la relation reconnue.

1.7 Relations multiplicatives

Soient S un semigroupe, $p : A^+ \rightarrow S$ un système d'écriture et $L \subseteq A^+$ un dictionnaire. On définit les *relations multiplicatives* de L en posant, pour tout $w \in A^*$,

$$R_w^L = \{(u, v) \in L \times L \mid uw \sim v\}$$

R_w^L est une relation restreinte aux mots bien orthographiés (selon le dictionnaire L) analogue à la multiplication à droite par w dans S . Similairement, R_1^L est la relation analogue à l'identité dans S . Comme un élément de S peut admettre plusieurs orthographes, on peut, par exemple, avoir $v \neq v'$ et $(u, v), (u, v') \in R_a^L$, c'est-à-dire que ces relations peuvent ne pas être des fonctions. Les relations multiplicatives R_a^L et R_1^L , pour tout $a \in A$, sont appelées

relations multiplicatives *élémentaires*. S'il n'y a pas d'ambiguïté sur le dictionnaire dans un certain contexte, on omet l'écriture du L dans la notation, i.e. $R_a = R_a^L$.

Proposition 1.7.1. (Blanchette, Choffrut, Reutenauer, 2019) Soient $p : A^+ \rightarrow S$ un système d'écriture et $L \subseteq A^+$ un dictionnaire. Si $w = a_1 \dots a_n$, alors $R_w = R_{a_1} \circ \dots \circ R_{a_n}$.

Il suffit de considérer le cas $w = ab$, la proposition découle ensuite par récurrence. Soit $(u, v) \in R_{ab}$. Soit $x \in L$ tel que $x \sim ua$. Alors $(u, x) \in R_a$. De plus, comme $xb \sim uab \sim v$, $(x, v) \in R_b$. Alors $(u, v) \in R_a \circ R_b$ et $R_{ab} \subseteq R_a \circ R_b$.

Réciproquement, si $(u, v) \in R_a \circ R_b$, alors il existe $x \in L$ tel que $(u, x) \in R_a$ et $(x, v) \in R_b$, si bien que $uab \sim xb \sim v$, d'où $(u, v) \in R_{ab}$ et $R_a \circ R_b \subseteq R_{ab}$. \square

1.8 Types de dictionnaires rationnels

Un dictionnaire $L \subseteq A^+$ est dit rationnel s'il s'agit d'une partie rationnelle du semigroupe libre A^+ . Les dictionnaires qui nous intéressent sont tous rationnels. Pour cette raison, les dictionnaires seront dorénavant supposés rationnels. On introduit les différents types de dictionnaires qui seront étudiés au cours du prochain chapitre.

Un dictionnaire L est dit *automatique* si les images sous la fonction de remplissage de ses relations multiplicatives élémentaires sont rationnelles dans $(A_{(2)})^*$. Un dictionnaire L est dit *asynchrone* si ses relations multiplicatives élémentaires sont reconnaissables par un automate à deux bandes. Un dictionnaire L est dit *quasi-automatique* si ses relations multiplicatives élémentaires sont rationnelles comme parties du monoïde $A^* \times A^*$.

Soit $k \in \mathbb{N}$. Un dictionnaire $L \subseteq A^+$ est dit *k-Lipschitz* si pour tout $u, v \in L$ tel que $u = a_1 \dots a_n$, $v = b_1 \dots b_m$ et $n \leq m$ on a

$$d_p(u, v) \leq 1 \implies d_p(a_1 \dots a_i, b_1 \dots b_i) \leq k \quad \forall i \leq n$$

$$d_p(u, v) \leq 1 \implies d_p(a_1 \dots a_n, b_1 \dots b_i) \leq k \quad \forall n < i \leq m$$

Soit $k \in \mathbb{N}$. Un dictionnaire $L \subseteq A^+$ est dit *k-Lipschitz Hausdorff* si pour tout $u, v \in L$ l'ensemble des préfixes de u et l'ensemble des préfixes de v sont au plus à distance d'Hausdorff k l'un de l'autre. De façon équivalente, il faut que pour tout préfixe x de u , il existe un préfixe y de v tel que $d_p(x, y) \leq k$ et réciproquement, il faut que pour tout préfixe z de v , il existe un préfixe w de u tel que $d_p(z, w) \leq k$.

Soit $k \in \mathbb{N}$. Un dictionnaire $L \subseteq A^+$ est dit *faiblement k-Lipschitz* si pour tout $u, v \in L$ il existe $n \geq |u| + |v|$ et $a_1, \dots, a_n, b_1, \dots, b_n \in A \cup \{1\}$ tels que

$$\begin{aligned} u &= a_1 \dots a_n \in A^* \\ v &= b_1 \dots b_n \in A^* \\ d_p(u, v) \leq 1 &\implies d_p(a_1 \dots a_i, b_1 \dots b_i) \leq k \quad \forall i \end{aligned}$$

Un dictionnaire L est dit *Lipschitz*, *Lipschitz Hausdorff* ou *faiblement Lipschitz* s'il existe un entier k tel que L est *k-Lipschitz*, *k-Lipschitz Hausdorff* ou *faiblement k-Lipschitz*.

Proposition 1.8.1. *Les dictionnaires Lipschitz sont faiblement Lipschitz et les dictionnaires faiblement Lipschitz sont Lipschitz Hausdorff.*

Soient L Lipschitz, $u, v \in L$ tel que $u = a_1 \dots a_n$, $v = b_1 \dots b_m$ et $d_p(u, v) \leq 1$. Supposons sans perdre de généralité que $n \leq m$. On écrit simplement $u = a_1 \dots a_n 1^{|m|-|n|}$ et $v = b_1 \dots b_m$, et pour tout i , on a bien $d_p(a_1 \dots a_i, b_1 \dots b_i) \leq k$.

Soient L faiblement Lipschitz, $u, v \in L$ tel que $d_p(u, v) \leq 1$ et $a_i, b_i \in A \cup \{1\}$ tel que $u = a_1 \dots a_n, v = b_1 \dots b_n$ et $d_p(a_1 \dots a_i, b_1 \dots b_i) \leq k \forall i$. Alors pour tout préfixe de u il existe un i tel que ce préfixe est égal à $a_1 \dots a_i$, qui est au plus à distance k de $b_1 \dots b_i$, qui est bien un préfixe de v . □

CHAPITRE 2

DES GROUPES AUTOMATIQUES AUX SEMIGROUPES QUASI-AUTOMATIQUES

Ce chapitre expose les différents liens qui existent entre les différents types de dictionnaires. On montre que les dictionnaires automatiques sont asynchrones et Lipschitz, que les dictionnaires asynchrones sont quasi-automatiques, que les dictionnaires quasi-automatiques sont faiblement Lipschitz. On montre que les notions de groupe automatique, de monoïde automatique et de semigroupe quasi-automatique ne dépendent pas du choix de système d'écriture alors que celle de semigroupe automatique en dépend. On caractérise géométriquement les groupes automatiques et quasi-automatiques grâce aux propriétés Lipschitz et faiblement Lipschitz. On met en relation les semigroupes quasi-automatiques et les semigroupes rationnels. On montre que les groupes quasi-automatiques sont asynchrones et que les semigroupes quasi-automatiques gradués sont automatiques.

2.1 Inclusions générales

La première classe de structures algébriques définie et étudiée en fonction de la complexité de calcul est celle des groupes automatiques. Les notions subséquentes (asynchrones et quasi-automatiques) ont été définies comme généralisations de cette première classe. On montre que ce sont bien des généralisations et ce au niveau des types de relations directement.

Proposition 2.1.1. (*Epstein et al., 1992*) *Les dictionnaires automatiques sont asynchrones.*

Soit R une relation telle que $r(R)$ est rationnelle. Le théorème de Kleene nous assure qu'il existe un automate $W = (Q, T, I, F)$ sur $(A \cup \{*\}) \times (A \cup \{*\})$ qui reconnaît $r(R)$. On construit un automate à deux bandes $\widetilde{W} = (\widetilde{Q}, \widetilde{T}, \widetilde{I}, \widetilde{F}, P)$ sur A qui reconnaît R . Les états sont donnés par $\widetilde{Q} = Q \times \{g, d, g^*, d^*, f\}$, les états initiaux $\widetilde{I} = I \times \{g\}$, les états finaux $\widetilde{F} = Q \times \{f\}$ et la partie des états est $P = Q \times \{g, g^*\}$. On construit l'ensemble des

transitions \widetilde{T} avec T et F de la fa on suivante:

$$\begin{aligned}
p \xrightarrow{a,b} q \in T &\implies (p, g) \xrightarrow{a} (p, d) \xrightarrow{b} (q, g) \\
p \xrightarrow{a,*} q \in T &\implies (p, g) \xrightarrow{a} (p, d) \xrightarrow{*} (q, g^*) \\
&\quad (p, g^*) \xrightarrow{a} (q, g^*) \\
p \xrightarrow{*,b} q \in T &\implies (p, g) \xrightarrow{*} (p, d^*) \xrightarrow{b} (q, d^*) \\
&\quad (p, d^*) \xrightarrow{b} (q, d^*) \\
p \in F &\implies (p, g) \xrightarrow{*} (p, d^*) \xrightarrow{*} (p, f) \\
&\quad (p, g^*) \xrightarrow{*} (p, f) \\
&\quad (p, d^*) \xrightarrow{*} (p, f)
\end{aligned}$$

Montrons que cet automate   deux bandes reconna t exactement R . Ici, les fonctions g et d dictant la lecture   gauche ou   droite sont simples; lorsqu'on est dans un  tat (q, g) , on effectue la lecture de la prochaine lettre   gauche, et lorsqu'on est dans un  tat (q, d) , on effectue la lecture   droite. Notons que par construction, l'automate effectue forc ment la lecture d'une lettre   gauche puis d'une lettre   droite et continue d'alterner jusqu'  ce qu'un des deux mots soit termin , puis termine de lire celui qui n'est pas encore termin . Soit $(a_1 \dots a_n, b_1 \dots b_m)$ un couple de mots. Supposons sans perdre de g n ralit  que $n \leq m$. Alors $(a_1 \dots a_n, b_1 \dots b_m) \in R(\widetilde{W})$ si et seulement si le mot $a_1 b_1 a_2 b_2 \dots a_n b_n * b_{n+1} \dots b_m *$ est reconnu par l'automate simple $(\widetilde{Q}, \widetilde{T}, \widetilde{I}, \widetilde{F})$. On a alors un chemin

$$\begin{aligned}
I \times g \ni (i, g) &\xrightarrow{a_1} (i, d) \xrightarrow{b_1} (q_1, g) \xrightarrow{a_2} \dots \\
\dots &\xrightarrow{b_n} (q_n, g) \xrightarrow{*} (q_n, d^*) \xrightarrow{b_{n+1}} (q_{n+1}, d^*) \xrightarrow{b_{n+2}} \dots \\
\dots &\xrightarrow{b_m} (q_m, d^*) \xrightarrow{*} (q_m, f) \in F \times \{f\}
\end{aligned}$$

Mais par construction, ces transitions existent si et seulement s'il existe un chemin

$$I \ni i \xrightarrow{a_1, b_1} q_1 \xrightarrow{a_2, b_2} \dots \xrightarrow{a_n, b_n} q_n \xrightarrow{*, b_{n+1}} q_{n+1} \xrightarrow{*, b_{n+2}} \dots \xrightarrow{*, b_m} q_m \in F$$

Un tel chemin existe si et seulement si $(a_1, b_1)(a_2, b_2) \dots (a_n, b_n)(*, b_{n+1}) \dots (*, b_m) \in L(W) = r(R)$. Un tel mot est dans $r(R)$ si et seulement si le couple $(a_1 \dots a_n, b_1 \dots b_m)$ est  l ment de R .

Comme l'implication tient au niveau des relations, elle tient au niveau des dictionnaires. \square

Proposition 2.1.2. (Blanchette, Choffrut, Reutenauer, 2019) *Les dictionnaires asynchrones sont quasi-automatiques.*

Soit R une relation asynchrone reconnue par l'automate à deux bandes (Q, T, I, F, P) . Le théorème de Nivat nous assure que s'il existe un langage rationnel H sur A_{gd} tel que $\pi(H) = R$, R est rationnelle. Le théorème de Kleene nous assure qu'il suffit de montrer l'existence un tel langage reconnaissable. On construit l'automate à partir de l'automate à deux bandes. On garde les mêmes états ainsi que les mêmes états initiaux et finaux. On construit \tilde{T} à partir de T et P de la façon suivante:

$$\begin{aligned} p \xrightarrow{a} q \in T, p \in P &\implies p \xrightarrow{(a,g)} q \\ p \xrightarrow{a} q \in T, p \notin P &\implies p \xrightarrow{(a,d)} q \\ p \xrightarrow{*} q \in T &\implies p \xrightarrow{1} q \end{aligned}$$

Le langage reconnu par cet automate, disons H , est tel que $\pi(H) = R$. R est donc rationnelle. Comme l'implication tient au niveau des relations, elle tient au niveau des dictionnaires. \square

2.2 Dictionnaires Lipschitz

L'étude des groupes automatiques a d'abord émergé en théorie géométrique des groupes. C'est d'ailleurs la principale approche des différents auteurs de *Word processing in groups* [8]. Une caractérisation géométrique des groupes automatiques est le point de départ d'une telle approche. Les propositions suivantes établissent cette caractérisation.

Proposition 2.2.1. (Epstein et al., 1992) *Les dictionnaires automatiques sont Lipschitz.*

Soient $p : A^+ \rightarrow S$ un système d'écriture et $L \subseteq A^+$ un dictionnaire automatique. Alors pour chaque relation multiplicative élémentaire R il existe un automate W reconnaissant $r(L)$. Supposons sans perdre de généralité que tous les états de ces automates sont coaccessibles et soit m le nombre d'états du plus grand de ces automates.

Montrons que L est Lipschitz. Soient $u, v \in L$ tel que $d_p(u, v) \leq 1$. Alors (u, v) est élément d'une relation multiplicative élémentaire R . Soient p_u et p_v des préfixes de v de même longueur. On considère l'état $q_0(p_u, p_v)$ dans l'automate. Il existe un chemin de longueur au plus m entre $q_0(p_u, p_v)$ et un état final q_f . On a alors, pour certains $s_u, s_v \in A_m$ de même longueur, $q_0(p_u, p_v)(s_u, s_v) = q_0(p_u s_u, p_v s_v) \in F$. Donc $(p_u s_u, p_v s_v)$ est dans une relation multiplicative élémentaire de L . Donc $d_p(p_u s_u, p_v s_v) \leq 1$. D'où

$$d_p(p_u, p_v) \leq d_p(p_u, p_u s_u) + d_p(p_u s_u, p_v s_v) + d_p(p_v s_v, p_v) \leq m + 1 + m$$

□

Proposition 2.2.2. (Campbell et al., 2001) *Les dictionnaires Lipschitz ne sont pas tous automatiques.*

Supposons pour une contradiction que l'implication est vraie. Soient S un semigroupe, $p : A^+ \rightarrow S$ un système d'écriture et $L \subset A^+$ un dictionnaire qui n'est pas automatique. Le semigroupe $S' = S \cup \{0\}$ où $0 \notin S$ et $a0 = 0a = 0 \forall a \in S$ est engendré par $A \cup \{z\}$, $z \mapsto 0$ et admet $L \cup \{z\}$ comme dictionnaire. Ce dictionnaire est Lipschitz car pour tout u, v on a $d(u, v) \leq d(u, 0) + d(0, v) = 1 + 1$. On considère, pour chaque $a \in A \cup \{1\}$, R'_a la relation multiplicative de $L \cup \{z\}$. Comme z est la seule orthographe de 0 , on a

$$\begin{aligned} R'_1 &= R \cup \{(z, z)\} \implies R_1 = R'_1 - \{(z, z)\} \implies r(R_1) = r(R'_1) - \{(z, z)\} \\ R'_a &= R_a \cup \{(z, z)\} \implies R_a = R'_a - \{(z, z)\} \implies r(R_a) = r(R'_a) - \{(z, z)\} \end{aligned}$$

Comme $L \cup \{0\}$ est Lipschitz, il est automatique. Alors $r(R'_1)$ et $r(R'_a)$ sont rationnels. Alors $r(R_1) = r(R'_1) - \{(z, z)\}$ et $r(R_a) = r(R'_a) - \{(z, z)\}$ sont rationnels. Alors L est automatique, une contradiction. □

Proposition 2.2.3. (Epstein et al., 1992) *Les dictionnaires Lipschitz d'un groupe sont automatiques.*

Soient G un groupe, $p : A^+ \rightarrow G$ un système d'écriture, $L \subset A^+$ un dictionnaire Lipschitz. Comme L est rationnel, L^* est aussi rationnel. Le théorème de Kleene nous assure l'existence d'un automate déterministe $(Q, T, \{q_0\}, F)$ reconnaissant ce langage. On considère le quadruplet $W_a = (Q \times Q \times G, \tilde{T}, (q_0, q_0, 1_G), F \times F \times \{a\})$ pour chaque $a \in A \cup \{1\}$,

où \tilde{T} est l'ensemble des transitions suivantes, pour tout $p, q \in Q, g \in G, a, b \in A$

$$\begin{aligned} (p, q, g) &\xrightarrow{a,b} (pa, qb, a^{-1}gb) \\ (p, q, g) &\xrightarrow{a,*} (pa, q*, a^{-1}g) \\ (p, q, g) &\xrightarrow{*,b} (p*, qb, gb) \end{aligned}$$

Remarquons que si $|u| = |v| + i$

$$u, v \in L \text{ et } ua \sim v \iff q_0u, q_0v*^i \in F \text{ et } u^{-1}v = a$$

et si $|v| = |u| + j$

$$u, v \in L \text{ et } ua \sim v \iff q_0u*^j, q_0v \in F \text{ et } u^{-1}v = a$$

c'est-à-dire que $(u*^i, v*^j)$ est reconnu si et seulement s'il est dans $r(R_a)$. Comme L est Lipschitz, il existe un $k \in \mathbb{N}$ tel que pour tout w_u préfixe de u et w_v préfixe de v de même longueur, $d(w_u, w_v) = |w_u^{-1}w_v| \leq k$. Alors si $|g| > k$, (p, q, g) n'est pas coaccessible.

On restreint W_a aux états coaccessibles, ce qui ne change pas le langage reconnu. Comme $\{g \in G : |g| \leq k\}$ est fini, la restriction est bien un automate fini qui reconnaît $r(R_a)$. \square

2.3 Groupes automatiques

On montre que la notion de groupe automatique ne dépend pas du choix de système d'écriture; soit il admet un dictionnaire pour chaque choix de système d'écriture, soit il n'en admet aucun. On suit essentiellement la preuve de Epstein et al., utilisant la caractérisation géométrique. On commence par quelques lemmes.

Lemme 2.3.1. *S'il existe $L \subseteq A^+$ un dictionnaire Lipschitz d'un groupe G , alors il existe un dictionnaire Lipschitz $L' \subseteq (A \cup \{e\})^+$ où $e \mapsto 1_G$.*

On prend simplement $L' = L \subseteq A^+ \subseteq (A \cup \{e\})^+$. Comme les mots L' ne contiennent aucun e , la distance entre les préfixes pour la métrique induite par $A^+ \rightarrow G$ est exactement la même que celle induite par $(A \cup \{e\})^+ \rightarrow G$. \square

Lemme 2.3.2. *Soient G un groupe, $p : A^+ \rightarrow G$ un système d'écriture et $L \subseteq (A \cup \{e\})^+$*

un dictionnaire Lipschitz où $e \mapsto 1_G$. Alors il existe un dictionnaire Lipschitz $L' \subseteq A^+$.

Comme p est un système d'écriture, il existe un mot m non-vidé tel que $p(m) = 1_G$. Posons $|m| = n$. Chaque mot $w \in (A \cup \{e\})^+$ se factorise de façon unique sous la forme $w = u_1 \dots u_r v$ où

u_i termine par e et contient exactement n occurrences de e
 v contient entre 0 et $n - 1$ occurrences de e

On considère le morphisme $f : (A \cup \{e\})^* \rightarrow A^*$ défini par $f(a) = a \forall a \in A, f(e) = 1$ et la fonction $g : L \rightarrow A^+$ définie par

$$w \mapsto f(u_1)m f(u_2)m \dots f(u_r)m f(v)$$

Notons que pour tout i , on a

$$|f(u_i)m| = |u_i| \qquad f(u_i) \sim u_i \sim f(u_i)m$$

Comme on compense la disparition des e par l'introduction des m , chaque lettre est déplacée d'au plus n positions. Ainsi, tout préfixe de longueur k de w est à distance au plus n du préfixe de longueur k de $g(w)$.

Montrons que $L' = g(L)$ est Lipschitz. Soient $u', v' \in L'$. Alors il existe $u, v \in L$ tels que $u' = g(u), v' = g(v)$. Soient p_u, p'_u, p_v, p'_v les préfixes de longueur k de u, u', v, v' . Comme L est Lipschitz, il existe $j \in \mathbb{N}$ tel que $d_p(p_u, p_v) \leq j$. On a alors

$$d_p(p'_u, p'_v) \leq d_p(p'_u, p_u) + d_p(p_u, p_v) + d_p(p_v, p'_v) \leq n + j + n$$

□

Lemme 2.3.3. *Soit $L \subseteq A^+$ un dictionnaire k -Lipschitz. Alors pour tout p_u, p_v préfixes de u et v de même longueur,*

$$u, v \in L \text{ et } d_p(u, v) \leq n \implies d_p(p_u, p_v) \leq kn$$

Si u, v sont à distance au plus n , il existe $a_1 \dots a_m$ où $m \leq n$ tel que $ua_1 \dots a_m = v$. Il existe des mots $w_i \in L$ pour tout $0 \leq i < m$ tels que $ua_1 \dots a_i \sim w_i$. On a

$$d(u, w_1) = d(w_1, w_2) = \dots = d(w_{m-2}, w_{m-1}) = d(w_{m-1}, v) = 1$$

Soient $p_0, p_1, \dots, p_{m-1}, p_m$ les préfixes de longueur j de $u, w_1, \dots, w_{m-1}, v$. Comme L est k -Lipschitz, on a $d(p_i, p_{i+1}) \leq k$ pour tout i . Alors

$$d(u, v) \leq d(u, w_1) + d(w_1, w_2) + \dots + d(w_{m-1}, v) \leq km \leq kn$$

□

Théorème 2.3.4. (*Epstein et al., 1992*) Soient $p : A^+ \rightarrow G$ et $q : B^+ \rightarrow G$ deux systèmes d'écriture d'un groupe G . Il existe un dictionnaire Lipschitz $L_A \subseteq A^+$ si et seulement s'il existe un dictionnaire Lipschitz $L_B \subseteq B^+$.

Soit $e \notin A \cup B$. On étend p et q en posant $p(e) = q(e) = 1_G$. Pour chaque $a \in A$ et $b \in B$, on choisit un mot $m_a \in (B \cup \{e\})^+$ et $m_b \in (A \cup \{e\})^+$ tel que $m_a \sim a$ et $m_b \sim b$. Comme $e \mapsto 1_G$, on peut choisir des m_a et des m_b qui sont tous de même longueur, disons n . Il s'ensuit que pour tout $g, h \in G$, $d_p(g, h) \leq n d_q(g, h)$. On considère le morphisme $f : (A \cup \{e\})^+ \rightarrow (B \cup \{e\})^+$ donné par $f(a) = m_a \forall a \in A$.

S'il existe un dictionnaire Lipschitz dans A^+ , le Lemme 2.3.1 nous assure qu'il existe $L \subseteq (A \cup \{e\})^+$ un dictionnaire Lipschitz. Le Lemme 2.3.2 nous assure qu'il suffit maintenant de montrer que $L' = f(L) \subseteq (B \cup \{e\})^*$ est aussi Lipschitz pour montrer l'existence d'un dictionnaire Lipschitz dans B^+ .

Soient $u', v' \in L'$ tels que $u'b \sim v'$. Alors il existe $u, v \in L$ tels que $u' = f(u), v' = f(v)$. De plus, comme $um_b \sim u'b \sim v' \sim v$, on a

$$d_p(u, v) \leq d_p(u, um_b) + d_p(um_b, v) \leq |m_b| \leq n$$

Le Lemme 2.3.3 nous assure donc que tous les préfixes de même longueur de u et v est à distance au plus kn l'un de l'autre.

Soient p'_u, p'_v des préfixes de longueur k' de u' et v' . Posons $k = \lfloor \frac{k'}{n} \rfloor$ la partie entière inférieure de $\frac{k'}{n}$. Soient p_u, p_v les préfixes de longueur k de u et v . Par construction, $d_q(p_u, p'_u) \leq n$, $d_q(p_v, p'_v) \leq n$ et

$$\begin{aligned} d_q(p_u, p_v) &\leq d_q(p_u, p'_u) + d_q(p'_u, p'_v) + d_q(p'_v, p_v) \\ &\leq n + nd_p(p'_u, p'_v) + n \\ &\leq n + n(kn) + k \end{aligned}$$

□

Corollaire 2.3.5. (*Epstein et al., 1992*) Soient $p : A^+ \rightarrow G$ et $q : B^+ \rightarrow G$ deux systèmes d'écriture d'un groupe G . Il existe un dictionnaire automatique $L_A \subseteq A^+$ si et seulement s'il existe un dictionnaire automatique $L_B \subseteq B^+$.

Les Propositions 2.3 et 2.5 nous assure qu'un dictionnaire d'un groupe est automatique si et seulement s'il est Lipschitz. Le résultat découle donc directement du théorème précédent. □

Le corollaire précédent assure que la notion de groupe automatique est bien définie sans spécifier de système d'écriture. La notion de semigroupe automatique, quant à elle, n'est pas bien définie dans ce sens car elle dépend du choix de système d'écriture. Pour un exemple explicite de semigroupe qui admet un dictionnaire automatique pour un système d'écriture mais pas pour un autre, voir Campbell et al. [5], Exemple 4.5.

2.4 Monoïdes automatiques

Du côté des monoïdes, l'analogie du corollaire précédent tient. On ne peut par contre pas utiliser les arguments géométriques qu'apporte l'équivalence avec les dictionnaires Lipschitz. On suit essentiellement la preuve de Duncan et al. Comme pour les groupes, on commence avec des lemmes préliminaires qui nous permettent d'ajouter ou enlever des générateurs redondants envoyés sur l'identité.

Lemme 2.4.1. *S'il existe $L \subseteq A^+$ un dictionnaire automatique d'un monoïde M , alors il existe un dictionnaire automatique $L' \subseteq (A \cup \{e\})^+$ où $e \mapsto 1_M$.*

On prend à nouveau $L' = L$. La surjectivité de L comme partie de A^+ assure la surjectivité comme partie de $(A \cup \{e\})^*$. Les relations multiplicatives élémentaires sont les mêmes, et comme parties rationnelles de $(A_{(2)})^*$, elles sont aussi parties rationnelles de $((A \cup \{e\})_{(2)})^* \subseteq (A_{(2)})^*$. \square

Lemme 2.4.2. *Soient M un monoïde, $p : A^+ \twoheadrightarrow M$ un système d'écriture, $e \notin A$ avec $e \mapsto 1_M$, $L \subseteq (A \cup \{e\})^+$ un dictionnaire automatique, $m \in A^+$ tel que $m \mapsto 1_M$ et $g : L \rightarrow A^+$ la fonction définie plus tôt. Si $J \subseteq A_{(2)}^*$ est rationnel, alors $J_g = \{r(g(u), v) : r(u, v) \in J\} \subseteq A_{(2)}^*$ est aussi rationnel.*

Cette construction est due à Duncan et al, voir [6] Lemma 3.1. Soit $W = (Q, T, I, F)$ un automate sur $(A \cup \{e\})_2$ reconnaissant J . Posons $A_n = \bigcup_{k \leq n} A_{(2)}^k$, l'ensemble des mots sur $A_{(2)}$ de longueur au plus $n = |m|$. On définit un automate sur $A_{(2)} \cup \{1\}$ en posant $W' = (Q \times A_n, \tilde{T}, I \times \{1\}, F \times \{1\})$, où \tilde{T} est donné par les transitions suivantes, pour tout $q \in Q, u \in A^*, v \in (A \cup \{e\})^*$,

$$\begin{aligned}
(q, 1) &\xrightarrow{r(u,v)} (qr(u, v), 1) \\
(q, a_1 \dots a_k) &\xrightarrow{r(u,v)} (q(a_1, v), a_2 \dots a_k u) && \forall 1 \leq k \leq n-1, a_1, \dots, a_k \in A_{(2)} \\
(q, a_1 \dots a_k) &\xrightarrow{r(u,v)} (q(e, v), a_1 \dots a_k u) && \forall 0 \leq k \leq n-1, a_1, \dots, a_k \in A_{(2)} \\
(q, m) &\xrightarrow{1} (q, 1) \\
(q, a_1 \dots a_k) &\xrightarrow{1} (q(a_1, *), a_2 \dots a_k) && \forall 1 \leq k \leq n-1, a_1, \dots, a_k \in (A \cup \{e\})_2 \\
(q, a_1 \dots a_k) &\xrightarrow{1} (q(e, *), a_1 \dots a_k *) && \forall 1 \leq k \leq n-2, a_1, \dots, a_k \in (A \cup \{e\})_2
\end{aligned}$$

Cet automate reconnaît J_g , ce qui montre le lemme. \square

Lemme 2.4.3. *Sous les hypothèses du lemme précédent, il existe un dictionnaire automatique $L' \subseteq A^+$.*

Par une construction symétrique, on obtient que $J'_g = \{r(u, g(v)) : r(u, v) \in J\}$ est rationnel lorsque J est rationnel. Montrons que $L' = g(L)$ est un dictionnaire automatique. La surjectivité est vérifiée pour la même raison que pour les groupes, c'est-à-dire que $g(w) \sim w \forall w \in L$. Il suffit donc de montrer que les relations multiplicatives élémentaires

$R_a^{L'}$ sont telles que $r(R_a^{L'})$ sont rationnels. On a $r(R_a^L)$ rationnel pour tout a par hypothèse. En appliquant les deux constructions symétriques, on obtient $\{r(g(u), g(v)) : u, v \in L, ua \sim v\}$ rationnel sur $A_{(2)}^*$. Mais

$$\begin{aligned} \{r(g(u), g(v)) : u, v \in L, ua \in v\} &= \{r(u', v') : \exists u, v \in L, u' = g(u), v' = g(v), u'a \sim v'\} \\ &= \{r(u', v') : u', v' \in L', u'a \sim v'\} \\ &= r(R_a^{L'}) \end{aligned}$$

ce qui termine la preuve. □

Lemme 2.4.4. *Soient $p : A^+ \rightarrow S$ un système d'écriture et L un dictionnaire automatique. Alors pour chaque relation multiplicative R_w , $r(R_w)$ est rationnel.*

Montrons d'abord que si deux relations R, S sont telles que $r(R), r(S)$ sont rationnelles, alors $r(R \circ S)$ est aussi rationnel. Soient (Q, T, I, F) l'automate déterministe reconnaissant $r(R)$ et (Q', T', I', F') l'automate déterministe reconnaissant $r(S)$. On considère l'automate suivant sur $(A \cup \{*\})^3$: $W = (Q \times Q', \tilde{T}, I \times I', F \times F')$ où \tilde{T} est donné par

$$(p, q) \xrightarrow{a,b,c} (T(p, (a, b)), T'(q, (b, c)))$$

Un mot (u^{*i}, v^{*j}, w^{*k}) est reconnu si et seulement si $(u^{*i}, v^{*j}) \in r(R)$ et $(v^{*j}, w^{*k}) \in r(S)$. On définit un morphisme $f : ((A \cup \{*\})^3)^* \rightarrow ((A \cup \{*\})^2)^*$ en posant

$$f(*, b, *) = 1 \quad \forall b \quad \quad f(a, b, c) = (a, c) \quad \forall b, \forall (a, c) \neq (*, *)$$

$L(W)$ est reconnaissable donc rationnel, donc $f(L(W))$ est rationnel. Par construction, on a $f(L(W)) = r(R \circ S)$, qui est donc rationnel.

Si $w = a_1 \dots a_n$, alors $R_w = R_{a_1} \circ \dots \circ R_{a_n}$. On conclut donc que $r(R_w) = r(R_{a_1} \circ \dots \circ R_{a_n})$ est rationnel car L est automatique donc $r(R_{a_i})$ est rationnel pour tout i . □

Théorème 2.4.5. *(Duncan et al., 1999) Soient $p : A^+ \rightarrow M, q : B^+ \rightarrow M$ deux systèmes d'écriture d'un monoïde M . Il existe un dictionnaire automatique $L \subseteq A^+$ si et seulement*

s'il existe un dictionnaire automatique $L' \subseteq B^+$.

Comme pour les groupes, les lemmes précédents nous assurent qu'on peut supposer sans perdre de généralité qu'il existe $e \in M$ tel que $q(e) = 1_M$. On peut alors choisir, pour tout $a \in A$, des mots $m_a \in B^+$ de longueur exactement n tels que $m_a \sim a$. Soit $f : A^+ \rightarrow B^+$ le morphisme de semigroupes donné par $f(a) = m_a \forall a \in A$. On considère maintenant le morphisme $g : (A \cup \{*\} \times A \cup \{*\})^+ \rightarrow (B \cup \{*\} \times B \cup \{*\})^+$ donné par

$$g(a, b) = (f(a), f(b))$$

$$g(a, *) = (f(a), *)$$

$$g(*, b) = (*, f(b))$$

On choisit certains $w_b \in A^+$ tels que $p(w_b) = q(b)$. Alors $r(R_b) = g(r(R_{w_b}))$, qui est bien rationnel comme image sous morphisme d'un langage rationnel. \square

2.5 Semigroupes rationnels

La définition suivante est due à Jacques Sakarovitch, voir par exemple [12], où il introduit et étudie les monoïdes rationnels. On montre que les semigroupes quasi-automatiques forment une généralisation de ces objets.

Définition 2.5.1. (Sakarovitch, 1987) Soit $p : A^+ \rightarrow S$ un système d'écriture pour un semigroupe S . S est dit rationnel s'il admet un dictionnaire $L \subseteq A^+$ tel que $p|_L$ est une bijection entre L et S et si la fonction $\tau : w \mapsto L \cap (p \circ p^{-1})(w)$, est une partie rationnelle de $A^+ \times A^+$.

Proposition 2.5.2. (Blanchette, Choffrut, Reutenauer, 2019) Les semigroupes rationnels sont quasi-automatiques.

Soit $L \subseteq A^+$ un dictionnaire en bijection avec S tel que $\tau \subseteq A^+ \times A^+$ est rationnelle. Il suffit de montrer que les relations multiplicatives élémentaires sont rationnelles. Comme $p|_L$ est une bijection, il existe une unique orthographe de ua pour tout $u \in L, a \in A$, si bien que

$$R_a^L = \{(u, v) \in L \times L \mid ua \sim v\} = \{(u, \tau(ua)) \mid u \in L\} = \{(u, ua) \mid u \in L\} \circ \tau = \left(\bigcup_{u \in L} \{(u, ua)\} \right) \circ \tau$$

Le théorème de Elgot et Mezei nous assure qu'une composition de relations rationnelles est rationnelle, ce qui complète la preuve. \square

Notons que la réciproque est fautive. Les groupes rationnels sont tous finis, voir Sakarovitch [12], Exemple 4.2, mais \mathbb{Z} est par exemple un groupe quasi-automatique infini.

2.6 Semigroupes quasi-automatiques

La notion de semigroupe quasi-automatique ne dépend pas du choix de système d'écriture. On suit la preuve de l'article de Blanchette, Choffrut et Reutenauer introduisant la classe.

Théorème 2.6.1. *(Blanchette, Choffrut, Reutenauer, 2019) Soient $p : A^+ \twoheadrightarrow S$ et $q : B^+ \twoheadrightarrow S$ deux systèmes d'écriture d'un semigroupe S . Il existe un dictionnaire quasi-automatique $L \subseteq A^+$ si et seulement si il existe un dictionnaire quasi-automatique $L' \subseteq B^+$.*

Soient $L \subseteq A^+$ un dictionnaire quasi-automatique, $w_b \in A^+$ tel que $w_b \sim b \forall b \in B$ et $f : B^+ \rightarrow A^+$ défini par $b \mapsto w_b$. Montrons que $L' = f(L)$ est quasi-automatique.

On définit une fonction $g : B^+ \times B^+ \rightarrow A^+ \times A^+$ en posant $g(u, v) = (f(u), g(u))$. C'est un morphisme de semigroupes; en effet, pour tout $u, u', v, v' \in B^+$ on a

$$\begin{aligned} g(uu', vv') &= (f(uu'), g(vv')) \\ &= (f(u)f(u'), f(v)f(v')) \\ &= (f(u), f(v))(f(v), f(v')) \\ &= g(u, v)g(u', v') \end{aligned}$$

Montrons que pour tout b , $R'_b = g(R_{w_b})$. Soit $(u', v') \in R'_b$. Alors $u', v' \in L' = f(L)$. Alors il existe $u, v \in L$ tels que $u' = f(u)$ et $v' = f(v)$. De plus, $uw_b \sim u'b \sim v' \sim v$, d'où $(u, v) \in R_{w_b}$ et donc $(u', v') = g(u, v) \in g(R_{w_b})$. Réciproquement, soit $(u', v') \in g(R_{w_b})$. Alors il existe $(u, v) \in R_{w_b}$ tel que $g(u, v) = (u', v')$. Alors $uw_b \sim v$, $f(u) = u'$ et $f(v) = v'$. On a donc $u', v' \in L'$ ainsi que $u'b \sim uw_b \sim v \sim v'$, ce qui nous permet de conclure que $(u', v') \in R'_b$.

Posons $w_b = a_1 \dots a_n$. La Proposition 1.7.1 nous assure que $R_{w_b} = R_{a_1} \circ \dots \circ R_{a_n}$. Comme chacun des R_{a_i} est rationnel par hypothèse, le théorème de Elgot et Mezei nous assure que R_{w_b} est aussi rationnel. Comme g est un morphisme de semigroupes, $R'_b = g(R_{w_b})$ est aussi rationnel. \square

2.7 Dictionnaires faiblement Lipschitz

Les groupes quasi-automatiques sont caractérisés par la version faible de la propriété Lipschitz. De façon analogue à la relation entre les dictionnaires automatique et Lipschitz, on montre d'abord l'implication directe pour les semigroupes en général puis on montre que la réciproque tient, mais seulement pour les groupes.

Proposition 2.7.1. (*Blanchette, Choffrut, Reutenauer, 2019*) *Les dictionnaires quasi-automatiques sont faiblement Lipschitz.*

Soient $p : A^+ \rightarrow S$ un système d'écriture et $L \subset A^+$ un dictionnaire quasi-automatique. Le théorème de Nivat nous assure que pour chaque relation multiplicative élémentaire R_a , il existe un langage rationnel $L_a \subseteq (A \times \{g, d\})^*$ tel que $\pi_g \times \pi_d(L_a) = R_a$. Le théorème de Kleene nous assure qu'il existe un automate W_a reconnaissant L_a . On suppose ces automates coaccessibles. Soit c le nombre maximal d'état que contiennent les automates W_a .

Soient $u, v \in L$ tel que $d_p(u, v) \leq 1$. Alors $(u, v) \in R_a$ pour un certain $a \in A \cup \{1\}$. Alors il existe $w \in L_a$ tel que $\pi_g(w) = u$ et $\pi_d(w) = v$. Soient $c_1, \dots, c_n \in A \times \{g, d\}$ tels que $w = c_1 \dots c_n$ et posons $a_j = \pi_g(c_j), b_j = \pi_d(c_j)$ pour tout $j \leq n$. Fixons $i \leq n$.

Comme W_a est coaccessible, il existe un $w \in (A \times \{g, d\})^*$, de longueur au plus c , tel que $c_1 \dots c_i w \in L_a$. On a alors $(\pi_g(c_1 \dots c_i w), \pi_d(c_1 \dots c_i w)) \in R_a$. Alors

$$d(\pi_g(a_1 \dots a_i w), \pi_d(a_1 \dots a_i w)) \leq 1$$

Finalement, comme π_g et π_d sont des projections, $|\pi_g(w)| + |\pi_d(w)| = |w| \leq c$. On obtient

donc

$$\begin{aligned}
d_p(a_1 \dots a_i, b_1 \dots b_i) &\leq d_p(a_1 \dots a_i, a_1 \dots a_i \pi_g(w)) + d_p(a_1 \dots a_i \pi_g(w), b_1 \dots b_i \pi_d(w)) + \\
&\quad d_p(b_1 \dots b_i \pi_d(w), b_1 \dots b_i) \\
&\leq |\pi_g(w)| + d_p(\pi_g(c_1 \dots c_i w), \pi_d(c_1 \dots c_i w)) + |\pi_d(w)| \\
&\leq c + 1
\end{aligned}$$

□

Proposition 2.7.2. (Blanchette, Choffrut, Reutenauer, 2019) *Les dictionnaires faiblement Lipschitz de groupes sont quasi-automatiques.*

Soient $p : A^+ \rightarrow G$ un système d'écriture pour un groupe G et $L \subseteq A^+$ un dictionnaire faiblement k -Lipschitz. On construit un automate similaire à celui qu'on a construit pour montrer que les groupes Lipschitz sont automatiques. Soient $G_0 = \{g \in G : |g|_A \leq k\}$ et $W = (Q, T, I, F)$ l'automate déterministe reconnaissant L . Pour chaque $a \in A \cup \{1\}$, on considère l'automate $W_a = (Q \times Q \times G_0, \tilde{T}, \{(q_0, q_0, 1)\}, F \times F \times \{a\})$ sur $(A \cup \{1\}) \times (A \cup \{1\})$, où les flèches de \tilde{T} sont données par

$$(p, q, g) \xrightarrow{a, b} (pa, qb, a^{-1}gb)$$

pour tout $p, q \in Q, g \in G, a, b \in A \cup \{1\}$. On restreint W_a aux états coaccessibles. Montrons que $L(W_a) = R_a$ pour tout $a \in A \cup \{1\}$.

Soit (u, v) reconnu par W_a . Alors il existe un chemin $(i, i, 1) \xrightarrow{u, v} (p, q, a)$ reconnu par l'automate. Alors $q_0 u, q_0 v \in F$ et $a \sim u^{-1}v$. Par construction, on a donc $u, v \in L$ et $ua \sim v$, ce qui nous permet de conclure que $(u, v) \in R_a$.

Réciproquement, soit $(u, v) \in R_a$. Alors $u, v \in L$ et $ua \sim v$. Alors $d(u, v) \leq 1$. On peut alors écrire $u = a_1 \dots a_n$ et $v = b_1 \dots b_n$ avec des $a_j, b_j \in A \cup \{1\}$ tels que $d(a_1 \dots a_i, b_1 \dots b_i) \leq k$

pour tout $i \leq n$. Pour tout $i \leq n$, on pose

$$\begin{aligned} p_i &= q_0 a_1 \dots a_i \\ q_i &= q_0 b_1 \dots b_i \\ g_i &= (a_1 \dots a_i)^{-1} (b_1 \dots b_i) \end{aligned}$$

Remarquons que $|g_i| = |(a_1 \dots a_i)^{-1} b_1 \dots b_i| = d(a_1 \dots a_i, b_1 \dots b_i) \leq k$, et donc $g_i \in G_0$ pour tout i . De plus, $g_n = (a_1 \dots a_n)^{-1} (b_1 \dots b_n) = u^{-1}v = a$, et comme $(u, v) \in R_a \implies u, v \in L$, on a $p_n, q_n \in F$. On obtient alors un chemin

$$(q_0, q_0, 1) \xrightarrow{a_1, b_1} (p_1, q_1, g_1) \xrightarrow{a_2, b_2} \dots \xrightarrow{a_n, b_n} (p_n, q_n, g_n = a) \in F \times F \times \{a\}$$

ce qui assure que (u, v) est reconnu par W_a . □

2.8 Groupes quasi-automatiques

On montre que les groupes qui sont des semigroupes quasi-automatiques sont exactement les groupes asynchrones. Comme la notion d'asynchrone utilise une construction combinatoire plutôt complexe et difficile à manipuler, cette équivalence permet de contourner l'utilisation de ces machines abstraites au profit des dictionnaires quasi-automatiques, qui sont dans un certain sens plus naturels. On suit intégralement la preuve de Blanchette, voir [10]. On commence avec quelques lemmes.

Lemme 2.8.1. *Soit $L \subseteq A^+$ un dictionnaire quasi-automatique d'un semigroupe S . Il existe $k \in \mathbb{N}$, un dictionnaire quasi-automatique $K \subseteq L$ et un langage de Nivat $H \subseteq A_{gd}^*$ tel que $\pi(H) = R_1^K$ tel que pour tout $p, f, s \in A_{gd}^*$ on a*

$$pfs \in H, |f| > k \implies \pi_g(f) \neq 1 \neq \pi_d(f)$$

Soit $H_1 \subseteq A_{gd}^*$ un langage rationnel tel que $\pi(H_1) = R_1^L$ et soit $W = (Q, T, q_0, F)$ un automate déterministe reconnaissant H_1 . Posons $k = |Q|$. Pour chaque état $q \in Q$, on considère l'ensemble des boucles y autour de q telles que $\pi_q(y) = 1$ et $0 < |y| \leq k$. Notons que cet ensemble est fini. Soit $G(q)$ l'ensemble des mots acceptés par W dont les chemins

contiennent une telle boucle. Explicitement, on a

$$G(q) = \{x \in A_{g_d}^* | q_0x = q\} \{y \in B^+ | qy = q, \pi_g(y) = 1, |y| \leq k\} \{z \in B^* | qz \in F\}$$

Comme produit de langage rationnel, ce langage est aussi rationnel. Symétriquement, on définit $D(q)$ l'ensemble des mots dont les chemins dans W contiennent une boucle y telle que $\pi_d(y) = 1$. Ce langage est rationnel par le même raisonnement.

On prétend que $K = L - \bigcup_{q \in Q} \pi_d(G(q)) \cup \pi_g(D(q))$ est un dictionnaire quasi-automatique de S . Les relations $R_a^K = R_a^L \cap (K \times K)$ sont rationnelles par intersection. Montrons que $p(K) = S$. Considérons $s \in S$ et $w \in L$ un mot de longueur minimale tel que $p(w) = s$. Supposons pour une contradiction que $w \notin K$. Alors soit $w \in \pi_d(G(q))$ ou $w \in \pi_g(D(q))$. On montre le premier cas; le second est identique. Alors $w = \pi_d(xyz)$ avec y un boucle autour de q et $\pi_g(y) = 1, q_0x = q, qz \in F$. Alors $q_0xz = qz \in F$, si bien que $xz \in H_1$. Ceci implique que $\pi(xz) \in R_1^L$, ce qui implique $\pi_g(xz) \sim \pi_d(xz)$. Similairement, $\pi_g(xyz) \sim \pi_d(xyz)$. Alors

$$\pi_d(xyz) \sim \pi_g(xyz) = \pi_g(x)\pi_g(y)\pi_d(z) = \pi_g(x)1\pi_g(z) = \pi_g(xz) \sim \pi_d(xz)$$

On conclue que $\pi_d(xz)$ et $\pi_d(xyz)$ représentent le même élément de S . Comme $\pi_g(y) = 1$, on a $\pi_d(y) \neq 1$. Alors $\pi_d(xz)$ est plus court que $\pi_d(xyz)$, une contradiction à la minimalité de w .

Maintenant posons $H = \pi^{-1}(K \times K) \cap H_1$. Comme π^{-1} est un morphisme inverse dans un monoïde quelconque, H est reconnaissable. Mais comme H est une partie de B^* , un monoïde libre, le théorème de Kleene assure que H est aussi rationnel. De plus, on a

$$\pi(H) = \pi(\pi^{-1}(K \times K) \cap H_1) = (K \times K) \cap \pi(H_1) = (K \times K) \cap R_1^L = R_1^K$$

Montrons que H a bien la propriété du lemme. Soit $w = pfs \in H$ avec $|f| > k$. Supposons pour une contradiction que $\pi_g(f) = 1$; à nouveau, le cas symétrique est identique. Comme $H \subseteq H_1$, pfs est reconnu par W . Comme la longueur de f est plus grand que le nombre d'état de W , son chemin lors de la lecture de w doit contenir une boucle de longueur au plus k autour d'un sommet q . Aussi, comme y est un facteur de f , on sait que $\pi_g(y) = 1$. Comme w est accepté et contient une boucle appropriée, $w \in G(g)$ et donc

$\pi_d(w) \notin K$. C'est une contradiction car $w \in H$ implique $\pi(H) \in R_1^K$ et donc $\pi_d(w) \in K$. \square

Lemme 2.8.2. *Avec les notations précédentes, il existe $k' \in \mathbb{N}$ tel que*

$$(u, v) \in R_1^K \implies |u| \leq k'|v|$$

Soit $w \in H$ tel que $\pi(w) = (u, v)$. On décompose w en facteurs de longueur k . On obtient alors $w = f_1 \dots f_{h+1}$ où $|f_i| = k$ pour tout $i \leq h$ et $|f_{h+1}| \leq k$. Le lemme précédent nous assure donc que $\pi_g(f_i) \neq 1 \neq \pi_d(f_i)$ pour tout $i \leq h$. On a

$$|u| = |\pi_g(f_1 \dots f_{h+1})| = |\pi_g(f_1)| + \dots + |\pi_g(f_{h+1})|$$

et donc $h \leq |u| \leq kh + k$. Symétriquement, on a $h \leq |v| \leq kh + k$. Finalement,

$$|u| \leq kh + k \leq k|v| + k \leq 2k|v|$$

et $k' = 2k$ satisfait les conditions du lemme. \square

Définition 2.8.3. Une fonction de départ pour un dictionnaire L est une fonction $D : \mathbb{N} \rightarrow \mathbb{N}$ telle que si $xyz \in L$ et $y > D(n)$, alors $|y|_G \geq n$.

Proposition 2.8.4. *Soit $L \subseteq A^+$ un dictionnaire quasi-automatique pour un groupe G . Alors il existe $K \subseteq L$ un dictionnaire quasi-automatique de G avec une fonction de départ.*

On considère $K \subseteq L$ le dictionnaire quasi-automatique construit dans les lemmes précédents. Soit $W = (Q, T, q_0, F)$ un nouvel automate, accessible et coaccessible, reconnaissant K . Posons $c = |Q|$ et k la constante donnée par le lemme précédent. Pour tous les triplets (q, q', g) avec $q, q' \in Q$ et $g \in G$, posons $m(q, q', g) = \min\{|w| : qw = q', p(w) = g\}$ s'il existe un w avec $qw = q'$ et $p(w) = g$ et $m(q, q', g) = 0$ sinon. On définit $D : \mathbb{N} \rightarrow \mathbb{N}$ en posant

$$D(n) = 2ck + k \max\{m(q, q', g) \mid q, q' \in Q, |g|_G \leq n\}$$

On prétend que D est une fonction de départ pour K . Soit $xyz \in K$ tel que $|y| > D(n)$ est supposons pour une contradiction que $|y|_G \leq n$. Considérons le chemin $q_0 \xrightarrow{x} q_1 \xrightarrow{y} q_2 \xrightarrow{z} q_3 \in F$. On choisit un mot y' tel que $q_1y' = q_2$ et $y' \sim y$ de longueur minimale $m(q_1, q_2, p(y))$. Comme W est accessible, coaccessible et a c états, on peut choisir x' et z' tels que $|x'|, |z'| \leq c$, $q_0x' = q_1$ et $q_2z' \in F$. Ceci implique que $x'y'z'$ et $x'y'z'$ sont dans K . De plus, comme $y \sim y'$, on a $x'y'z' \sim x'y'z'$. Ce sont les conditions pour savoir que $(x'y'z', x'y'z') \in R_1^K$. Le lemme précédent nous assure que $|x'y'z'| \leq k|x'y'z'|$. Alors

$$|y| \leq |x'y'z'| \leq k|x'y'z'| = k(|x'| + |y'| + |z'|) \leq k(c + |y'| + c) = 2ck + k|y'| \leq D(n)$$

une contradiction au choix de y . □

Théorème 2.8.5. (*Blanchette, 2019*) *Un groupe admet un dictionnaire quasi-automatique si et seulement s'il admet un dictionnaire asynchrone.*

On a déjà démontré que les dictionnaires asynchrones sont quasi-automatiques pour les semigroupes en général avec la Proposition 2.1.2. Pour l'autre direction, soient G un groupe quasi-automatique et K le dictionnaire quasi-automatique construit dans les lemmes précédents, muni de la fonction de départ. Par la Proposition 2.7.1, comme dictionnaire quasi-automatique, il est faiblement Lipschitz. Il est donc Lipschitz Hausdorff par la Proposition 1.8.1. Le théorème suivant nous permet donc de conclure que G est asynchrone. □

Théorème 2.8.6. (*Epstein et Levy, 1992*) *Un groupe est asynchrone si et seulement s'il admet un dictionnaire Lipschitz Hausdorff muni d'une fonction de départ.*

La preuve d'Epstein et al. utilise une construction géométrique d'automate qu'ils appellent le *multiplicateur asynchrone standard*. Pour une preuve, voir Epstein et al. [8], Theorem 7.2.8. □

2.9 Semigroupes gradués

Un semigroupe est dit *gradué* s'il admet un degré, c'est-à-dire un morphisme $deg : S \rightarrow (\mathbb{N}, +)$ tel que $deg^{-1}(1)$ engendre S . Un très grand nombre de semigroupe étant gradué, la

proposition suivante est particulièrement puissante; elle permet de dire qu'il suffit de montrer qu'un semigroupe gradué est quasi-automatique pour utiliser l'ensemble des résultats classiques sur les dictionnaires automatiques.

Proposition 2.9.1. *(Blanchette, Choffrut, Reutenauer, 2019) Les semigroupes quasi-automatiques gradués sont automatiques.*

Soit S un semigroupe quasi-automatique muni d'un degré $S \rightarrow \mathbb{N}$. Alors $\text{deg}^{-1}(1)$ engendre S . Comme S est quasi-automatique, il est finiment engendré; il existe donc $A \subseteq \text{deg}^{-1}(1)$ fini qui engendre S . Le Théorème 2.6.1 assure qu'il existe donc un dictionnaire quasi-automatique $L \subseteq A^+$. Comme tous les éléments de A sont de degré 1, les mots de longueur n de L sont des orthographe d'éléments de degré n dans S . Pour tout $(u, v) \in R_1$, on a $u \sim v$, donc $|u| = \text{deg}(u) = \text{deg}(v) = |v|$. La Proposition 1.6.6 nous assure alors que R_1 est une partie rationnelle de $(A \times A)^* \subseteq A_{(2)}^*$. Similairement, pour tout $(u, v) \in R_a$ on a $ua \sim v$ et

$$|u *| = |u| + 1 = \text{deg}(u) + 1 = \text{deg}(ua) = \text{deg}(v) = |v|$$

et donc $\{(u*, v) \mid (u, v) \in R_a\}$ est une partie rationnelle de $A_{(2)}^*$. □

CHAPITRE 3

ALGORITHMES ET COMPLEXITÉ

Ce chapitre présente des algorithmes répondant à des problèmes importants portant sur les structures algébriques en général. Le plus fondamental est le problème du mot, qui est indécidable pour les groupes en général. On montre qu'il est décidable, en temps exponentiel pour les semigroupes quasi-automatiques, et en temps quadratique pour les semigroupes automatiques. On montre qu'on peut déterminer si un monoïde quasi-automatique est un groupe. Finalement, on montre que les groupes quasi-automatiques et automatiques satisfont respectivement une inégalité isopérimétrique exponentielle et quadratique.

3.1 Décomposition d'une relation rationnelle

Un théorème de Eilenberg (voir [2], Theorem IX.8.2) énonce que toute relation rationnelle contient une relation rationnelle fonctionnelle ayant le même domaine. Un autre théorème, dû à Elgot et Mezei (voir [9]), énonce que toute fonction qui est une relation rationnelle se décompose en une composition de fonctions séquentielles, une miroir et une standard. Combinés, ces théorèmes sont équivalents au suivant, ce qui rend effective la structure de dictionnaire quasi-automatique.

Théorème 3.1.1. (*Arnold, Latteux, 1979*) *Soit $R \subseteq A^* \times A^*$ une relation rationnelle. Il existe deux fonctions séquentielles f, g telles que $f \circ g \subseteq R$ et $\text{Dom}(f \circ g) = \text{Dom}(R)$.*

On suit la construction de Arnold et Latteux qui prouve directement le théorème, voir [1]. Soit $H \subseteq A_{gd}^*$ un langage de Nivat tel que $\pi(H) = R$ et $W = (Q, T, I, F)$ un automate déterministe le reconnaissant. Pour tout $P \subseteq Q$ et $u \in A^*$, on pose

$$P(u) = \{q \in Q \mid \exists w \in A_{gd}^*; \pi_q(w) = u \text{ et } qw \in P\}$$

On définit $M_1 = (2^Q, T_1, I_1, F_1)$, un transducteur séquentiel miroir $A \rightarrow 2^Q \times A$, en posant

$$\begin{aligned} I_1 &= F \\ F_1 &= \{P \mid I \subseteq P\} \\ P &\xrightarrow{a} P(a) \in T_1 \quad \forall P, a \\ (P, a) &\mapsto (P, a) \end{aligned}$$

On définit $M_2 = (Q, T_2, I, F)$, un transducteur séquentiel $2^Q \times A \rightarrow A$, en définissant T_2 itérativement de la façon suivante: pour chaque P, a et tout $q \in P(a)$ on choisit $w \in A_{gd}^*$ tel que $\pi_g(w) = a$ et $qw \in P$ et on pose

$$q \xrightarrow{P, a} qw \in T_2 \text{ et } (q, (P, a)) \mapsto \pi_d(w)$$

On pose f la fonction séquentielle donnée par le transducteur miroir M_1 et g la fonction séquentielle donnée par le transducteur M_2 . Montrons que ces fonctions répondent aux conditions du lemme. Soit $u = a_1 \dots a_n$. On a

$$\begin{aligned} F &\xrightarrow{u} F(u) \in M_1 \\ (F, u) &\mapsto (F(a_2 \dots a_n), a_1) \dots (F(a_n), a_{n-1} a_n) (F, a_n) = f(u) \end{aligned}$$

De plus, pour tout $q \in F(u)$, il existe $w \in A_{gd}^*$ avec $\pi_g(w) = u$ et $qw \in F$ tel que

$$\begin{aligned} q &\xrightarrow{f(u)} qw \in M_2 \\ (q, f(u)) &\mapsto \pi_d(w) \end{aligned}$$

Si $u \in \text{Dom}(R)$, il existe $w \in H$ tel que $\pi_g(w) = u$, si bien que $Iw \in F$. On a donc $I \in F(u)$ et donc $F(u) \in F_1$. De plus, $I \xrightarrow{f(u)} Iw \in F$ pour un certain tel w . On a donc $u \in \text{Dom}(f \circ g)$. Réciproquement, si $u \notin \text{Dom}(R)$, il n'existe de $w \in H$ tel que $\pi_g(w) = u$, si bien qu'aucun tel mot est l'étiquette d'un chemin $I \rightarrow F$ dans l'automate. On a $I \notin F(u)$, ce qui assure que $u \notin \text{Dom}(f) \supseteq \text{Dom}(f \circ g)$. On a donc $\text{Dom}(R) = \text{Dom}(f \circ g)$.

De plus, soit $(u, v) \in f \circ g$. Par construction, on a $u = \pi_g(w)$ pour un $w \in H$ et $v = \pi_d(w)$. Alors $(u, v) = \pi(w) \in R$. On a donc $f \circ g \subseteq R$. \square

3.2 Problème du mot

On dit qu'un algorithme répond au problème du mot d'un semigroupe S muni d'un système d'écriture $A^+ \rightarrow S$ s'il prend comme entrée une paire de mot $(u, v) \in A^+ \times A^+$ et décide si $u \sim v$. On montre que le problème du mot est décidable pour les semigroupes quasi-automatiques, en temps exponentiel en général et en temps quadratique pour ceux qui admettent des dictionnaires automatiques.

Théorème 3.2.1. *(Blanchette, Choffrut, Reutenauer, 2019) Le problème du mot d'un semigroupe quasi-automatique est décidable.*

On construit une fonction $l : A^+ \rightarrow L$, calculable algorithmiquement, qui à un mot quelconque représentant un élément s du semigroupe associe une orthographe de s . Ainsi, donné (u, v) , on n'a qu'à déterminer si $(l(u), l(v)) \in R_1$ pour répondre au problème du mot.

Pour chaque lettre $a \in A$, on considère les fonctions séquentielles f_a, g_a telles que $f_a \circ g_a \subseteq R_a$ données par le lemme précédent et on pose $h_a = f_a \circ g_a$. Comme L est un dictionnaire, il existe des mots $w_a \in L$ tel que $w_a \sim a$ pour tout $a \in A$. On en choisit un pour chaque lettre et on pose $l(a) = w_a$. On étend l à A^+ en posant

$$l(a_1 \dots a_n) = (h_{a_n} \circ \dots \circ h_{a_1})(l(a_1))$$

Pour tout $u \in A^+$ et $a \in A$, on a $l(ua) = h_a(l(u))$ et donc $(l(u), l(ua)) \in R_a$. On obtient donc $l(u) \in L$ et $l(u)a \sim l(ua)$. Finalement, montrons par récurrence que $u \sim l(u)$. Par construction $l(a) \sim a$ pour tout $a \in A$. Supposons que $u \sim l(u)$. Alors $l(ua) \sim l(u)a \sim ua$. \square

Proposition 3.2.2. *(Blanchette, Choffrut, Reutenauer, 2019) Avec les notations du théorème précédent, il existe $c \in \mathbb{N}$ tel que $|l(u)| \leq c^{|u|}$ et la complexité temporelle de l'algorithme répondant au problème du mot est exponentielle en fonction de $\max\{|u|, |v|\}$.*

Déterminer si un couple (u, v) appartient à une relation rationnelle est décidable en temps quadratique en fonction de $\max\{|u|, |v|\}$, voir par exemple l'algorithme classique de Leeuwen

et Nivat [13], Theorem 2.3. Cette dernière étape est négligeable étant donné que le calcul de $l(u)$ se fait en temps exponentiel.

Soit $t_a(u)$ le temps nécessaire pour calculer $h_a(u)$. Calculer l'image d'un mot u sous une fonction séquentielle se fait en temps linéaire en fonction de sa longueur $|u|$. De plus, la longueur de l'image est elle aussi au plus linéaire en $|u|$. Intuitivement, ceci est dû au fait qu'une fonction séquentielle se calcule avec un automate déterministe; on n'a qu'à suivre l'unique chemin de l'automate donné par u pour effectuer le calcul. Il existe alors des $c, k > 0$ tels que

$$|h_a(u)| \leq c|u| \quad |l(a)| \leq c \quad t_a(u) \leq k|u|$$

pour tout $a \in A$ et $u \in A^+$. Montrons par récurrence que $|l(u)| \leq c^{|u|}$. On a directement $|l(u)| \leq c$ si $|u| = 1$. Supposons maintenant que $|l(u)| \leq c^{|u|}$. On a donc $|l(ua)| \leq |h_a(l(u))| \leq c(c^{|u|}) = c^{|u|+1}$.

Soit $t(u)$ le temps nécessaire pour calculer $l(u)$. Montrons que $t(u) \leq k \frac{c^{|u|}-1}{c-1}$, ce qui est exponentiel. On procède à nouveau par récurrence; si $|u| = 1$, $t(u) = t(a) = 0$ car on a une liste finie de $l(a)$ préalablement calculée. On a $t(ua) = t(u) + t_a(l(u))$; en effet, on calcule d'abord $l(u)$ puis on applique la fonction séquentielle h_a pour obtenir $l(ua) = h_a(l(u))$. On a donc, par hypothèse de récurrence,

$$t(ua) = t(u) + t_a(l(u)) \leq k \frac{c^{|u|}-1}{c-1} + k|u| \leq k \frac{c^{|u|}-1}{c-1} + kc^{|u|} = k \frac{c^{|ua|}-1}{c-1}$$

□

Pour les dictionnaires automatiques, il existe un algorithme plus efficace. Le résultat est d'abord dû à Epstein et al. et demande une structure de groupe. Une généralisation de l'algorithme est donné par Campbell et al. pour les semigroupes automatiques. On simplifie la construction mais l'algorithme est le même.

Proposition 3.2.3. (*Esptein et al. pour les groupes, Campbell et al. pour la généralisation aux semigroupes*)

Si un semigroupe admet un dictionnaire automatique L , il existe une fonction $l : A^+ \rightarrow L$ qui à un mot quelconque u associe une orthographe de $p(u)$, de longueur au plus linéaire en

$|u|$, en temps quadratique en fonction de $|u|$. En particulier, on peut répondre au problème du mot en temps quadratique.

On choisit $w_a \in L$ tel que $w_a \sim a$ pour tout $a \in A$. Soient W_a des automates déterministes et complets reconnaissant $r(R_a^L)$ et soit k un nombre plus grand que le nombre d'états de tous ces automates ainsi que tous les $|w_a|$. Pour simplifier, on note q_0 l'état initial de chacun de ces automates.

Soit $u = a_1 \dots a_n$. On pose $u_1 = w_{a_1}$. L'élément du groupe $p(u_1 a_2)$ doit admettre au moins un orthographe; ceci implique que dans W_{a_2} , il existe un mot p_1 tel que $q_0(r(u_1, p_1))$ est coaccessible. Comme l'automate a moins de k états, il existe $s_1 \in A^*$ un mot tel que $q_0(r(u_1 * |s_1|, p_1 s_1)) \in F$ et $|s_1| \leq k$. On pose $u_2 = p_1 s_1$.

On continue le processus de façon itérative; on choisit à chaque étape un mot $p_i s_i$ tel que $(u_i * |s_i|, p_i s_i) \in r(R_{a_{i+1}}^L)$ et $|s_i| \leq k$ et on pose $u_{i+1} = p_i s_i$. On continue jusqu'à avoir choisit un u_n tel que $(u_{n-1}, u_n) \in R_{a_n}^L$. On obtient

$$u_n \sim u_{n-1} a_n \sim u_{n-2} a_{n-1} a_n \sim \dots \sim a_2 a_3 \dots a_{n-1} a_n \sim a_1 \dots a_n = u$$

On pose alors $l(u) = u_n$. Par construction, c'est bien une orthographe de $|u|$. On a $|u_{i+1}| = |p_i| + |s_i| \leq |u_i| + k$ pour tout i . Montrons que $|u_n| \leq kn$ par récurrence. D'abord, $|u_1| \leq k$. Puis, par hypothèse de récurrence, $|u_{n+1}| \leq |u_n| + k \leq kn + k = k(n+1)$.

Posons $t(i)$ le temps nécessaire pour calculer u_i à partir de u_{i-1} . On a $t(i+1) \leq t(i) + |u_i| + k$. Montrons que $t(n) \leq \sum_{j \leq n} kj + k$ par récurrence. D'abord, $t(1) = 0 \leq 2k$. Puis, par hypothèse de récurrence, on a

$$t(n+1) = t(n) + |u_n| + k = \sum_{j \leq n} kj + k + kn + k = \sum_{j \leq n} kj + k(n+1) + k = \sum_{j \leq n+1} kj + k$$

Comme $k \sum_{j \leq n} j + k = k \frac{n(n+1)}{2} + k$ est quadratique en n , le temps de calcul est au plus quadratique en n . \square

3.3 Éléments inversibles d'un monoïde quasi-automatique

Déterminer si un monoïde finiment engendré est un groupe ou non est un problème fondamental qu'on sait indécidable en général. On donne un algorithme répondant à ce problème dans le cas des monoïdes quasi-automatiques.

Proposition 3.3.1. *(Blanchette, Choffrut, Reutenauer, 2019) Déterminer si un monoïde M quasi-automatique est un groupe est décidable.*

Soient $p : A^+ \rightarrow M$ un système d'écriture, $L \subseteq A^+$ un dictionnaire quasi-automatique et $e \in L$ tel que $p(e) = 1_M$. D'abord, pour $a \in A$, $p(a)$ est inversible à gauche si et seulement s'il existe $w \in L$ tel que $(w, e) \in R_a^L$. En effet, si $(w, e) \in R_a^L$, alors $wa \sim 1_M$ et $p(w)$ est un inverse à gauche de $p(a)$ et s'il existe g tel que $gp(a) = 1_M$, g admet au moins un orthographe $w \in L$, si bien que $w, e \in L$ et $wa \sim e$, et donc $(w, e) \in R_a^L$.

On vérifie donc qu'il existe un tel w pour chaque a . C'est équivalent à déterminer si $(L \times \{e\}) \cap R_a^L \neq \emptyset$ pour chaque a . Mais $L \times \{e\}$ est reconnaissable et R_a^L est rationnelle, ce qui nous permet d'appliquer la Proposition 1.5.7 et ainsi obtenir la rationalité de l'intersection. Déterminer si une relation rationnelle est vide est décidable, voir par exemple Berstel [2], Proposition III.8.2.

Comme A engendre le monoïde et que chacun de ses éléments est inversible à gauche, tout élément $m \in M$ est aussi inversible à gauche car si $m = a_1 \dots a_n$, on a

$$a_n^{-1} \dots a_1^{-1} m = a_n^{-1} \dots a_1^{-1} a_1 \dots a_n = 1_M$$

De plus, comme tout élément est inversible à gauche, tout élément est inversible. En effet, si a est inverse à gauche de b et b inverse à gauche de c , on a

$$ab = bc = 1 \implies c = abc = a \implies ba = 1$$

□

3.4 Inégalités isopérimétriques

Une inégalité isopérimétrique met en relation une notion d'aire et de périmètre pour une classe d'objet. Par exemple, l'ensemble des courbes fermés dans le plan Euclidien, muni des notions classiques d'aire et de périmètre, satisfait l'inégalité $A \leq \frac{P^2}{2\pi}$, où A est l'aire de la région circonscrite par la courbe et P est son périmètre, ou sa longueur. En effet, il est bien connu que la courbe de périmètre donné P ayant une aire maximale est le cercle, qu'un périmètre P implique un rayon $r = \frac{P}{2\pi}$, et que l'aire du disque qu'il définit est $\pi r^2 = \pi \left(\frac{P}{2\pi}\right)^2 = \frac{P^2}{2\pi}$.

Soit $G = \langle A|R \rangle$ un groupe de présentation finie. Alors $G = \frac{F(A)}{N}$, où N est le plus petit sous-groupe normal contenant R . Ses éléments sont tous de la forme $\prod hg^{\pm 1}h^{-1}$ où $h \in A^*$ et $g \in R$.

L'ensemble des mots $w \in A^*$ tels que $w \sim 1$ sont des chemins fermés dans le graphe de Cayley de G ; une notion de périmètre s'impose donc: la longueur de $|w|$. Pour une notion d'aire, le choix n'est peut être pas aussi évident, mais demeure naturel. Tout mot représentant le neutre peut se factoriser en un produit de la forme $\prod hg^{\pm 1}h^{-1}$. Le nombre minimal de termes nécessaires pour cette factorisation est ce qu'on définit comme l'aire du mot. Cette terminologie géométrique proviennent de la théorie géométrique des groupes et les diagrammes de Van Kampen, que nous ne développerons pas ici.

On rappelle les conventions de la section 1.4 Groupe libre. On demande que les systèmes d'écritures de groupe possèdent deux propriétés supplémentaires; premièrement A doit être un alphabet stable sous inversion, c'est-à-dire que $a \in A \iff a^{-1} \in A$ et p doit respecter l'inversion, c'est-à-dire $p(w^{-1}) = p(w)^{-1}$ pour tout $w \in A^+$. De plus, on note les surjections successives qui factorisent p par

$$A^+ \xrightarrow{F} F(A) \xrightarrow{q} G$$

Définition 3.4.1. Soit $G = \langle A|R \rangle$ un groupe finiment présenté. On dit qu'il admet une inégalité isopérimétrique de classe $f : \mathbb{N} \rightarrow \mathbb{N}$ si pour tout $w \in A^*$ tel que $w \sim 1$, il existe des $g_i \in R, h_i \in F(A)$ tels que $F(w) = \prod_{i=1}^n h_i g_i^{\pm 1} h_i^{-1}$ avec $n \leq f(|w|)$.

On montrera que les groupes quasi-automatiques et automatiques admettent des inégalités isopérimétriques, respectivement exponentielle et quadratique.

Lemme 3.4.2. (*produit télescopique*) Soient $a_1, \dots, a_n, b_1, \dots, b_n, c_0, c_1, \dots, c_n \in G$ des éléments d'un groupe quelconque et soient $h_i = c_0 b_1 b_2 \dots b_{i-1} c_{i-1}^{-1}$ pour tout $i \leq n$. Alors

$$\prod_{1 \leq i \leq n} h_i (a_i c_i b_i^{-1} c_{i-1}^{-1}) h_i^{-1} = a_1 a_2 \dots a_n c_n (c_0 b_1 b_2 \dots b_n)^{-1}$$

On procède par récurrence. Pour $n = 1$, on a

$$h_1 (a_1 c_1 b_1^{-1} c_0^{-1}) h_1^{-1} = c_0 c_0^{-1} (a_1 c_1 b_1^{-1} c_0^{-1}) c_0 c_0^{-1} = a_1 c_1 b_1^{-1} c_0^{-1} = a_1 c_1 (c_0 b_1)^{-1}$$

Pour clarifier, on regarde aussi le cas $n = 2$, en tenant compte du cas $n = 1$:

$$\begin{aligned} a_1 c_1 (c_0 b_1)^{-1} (h_2 (a_2 c_2 b_2^{-1} c_1^{-1}) h_2^{-1}) &= a_1 c_1 (c_0 b_1)^{-1} (c_0 b_1 c_1^{-1}) (a_2 c_2 b_2^{-1} c_1^{-1}) (c_1 b_1^{-1} c_0^{-1}) \\ &= a_1 a_2 c_2 b_2^{-1} b_1^{-1} c_0^{-1} \\ &= a_1 a_2 c_2 (c_0 b_1 b_2)^{-1} \end{aligned}$$

Supposons maintenant l'énoncé vérifié pour un certain n . On a donc, par récurrence sur n ,

$$\begin{aligned} \prod_{1 \leq i \leq n+1} h_i (a_i c_i b_i^{-1} c_{i-1}^{-1}) h_i^{-1} &= \left(a_1 \dots a_n c_n (c_0 b_1 \dots b_n)^{-1} \right) (h_{n+1} (a_{n+1} c_{n+1} b_{n+1}^{-1} c_n^{-1}) h_{n+1}^{-1}) \\ &= a_1 \dots a_n c_n (c_0 b_1 \dots b_n)^{-1} (c_0 b_1 \dots b_n) c_n^{-1} (a_{n+1} c_{n+1} b_{n+1}^{-1} c_n^{-1}) (c_0 b_1 \dots b_n c_n^{-1})^{-1} \\ &= a_1 \dots a_{n+1} c_{n+1} b_{n+1}^{-1} c_n^{-1} c_n (c_0 b_1 \dots b_n)^{-1} \\ &= a_1 \dots a_{n+1} c_{n+1} (c_0 b_1 \dots b_{n+1})^{-1} \end{aligned}$$

□

Lemme 3.4.3. (*Blanchette, Choffrut, Reutenauer, 2019*) Soit $L \subseteq A^+$ un dictionnaire quasi-automatique d'un groupe G . Alors il existe un entier $k' \in \mathbb{N}$ tel que pour tout $u, v \in L$, $a \in A \cup \{1\}$ vérifiant $ua \sim v$, il existe $n \leq |u| + |v|$ et des mots $g_i, h_i \in A^*$ pour tout $i \leq n$ tels que $g_i \sim 1$, $|g_i| \leq k'$ et

$$uav^{-1} \sim \prod_{1 \leq i \leq n} h_i g_i^{\pm 1} h_i^{-1}$$

Comme L est quasi-automatique, il est faiblement k -Lipschitz pour un certain $k \in \mathbb{N}$. On

réécrit $u = a_1 \dots a_n$ et $v = b_1 \dots b_n$, avec $a_i, b_i \in A \cup \{1\}$ de façon à ce que $a_1 \dots a_i$ et $b_1 \dots b_i$ sont à distance au plus k l'un de l'autre pour tout i . Ceci nous permet de trouver un mot $c_i \in A^*$ pour chaque i de façon à ce que $a_1 \dots a_i c_i \sim b_1 \dots b_i$ et $|c_i| \leq k$. On peut clairement choisir $c_0 = 1$ et $c_n = a$.

On a alors $uav^{-1} = a_1 \dots a_n a (b_1 \dots b_n)^{-1} = a_1 \dots a_n c_n (c_0 b_1 \dots b_n)^{-1}$. En considérant les a_i, b_i, c_i, u, a, v comme éléments de $F(A)$, le lemme précédent nous assure que

$$uav^{-1} = \prod_{1 \leq i \leq n} h_i (a_i c_i b_i^{-1} c_{i-1}^{-1}) h_i^{-1}$$

Mais on a, pour tout i ,

$$a_1 \dots a_{i-1} (a_i c_i b_i^{-1} c_{i-1}^{-1}) \sim (b_1 \dots b_{i-1}) b_i b_i^{-1} c_{i-1}^{-1} \sim a_1 \dots a_{i-1} c_{i-1} c_{i-1}^{-1} \sim a_1 \dots a_{i-1}$$

si bien que $g_i = a_i c_i b_i^{-1} c_{i-1}^{-1} \sim 1$. Comme les c_i sont au plus de longueur k , ces mots sont de longueur au plus $2k + 2$, et les conditions du lemme sont vérifiées. \square

Théorème 3.4.4. (*Blanchette, Choffrut, Reutenauer, 2019*) *Les groupes quasi-automatiques admettent une présentation finie en tant que groupe et une inégalité isopérimétrique exponentielle pour cette présentation.*

Soient $p : A^+ \rightarrow G$ un système d'écriture d'un groupe G et $L \subseteq A^+$ un dictionnaire quasi-automatique. On considère les surjections successives $A^* \xrightarrow{F} F(A) \xrightarrow{q} G$ telles que $F \circ q = p$. Il suffit de montrer qu'il existe un $k \in \mathbb{N}$ tel que tout élément de $\ker(q)$ s'exprime comme produit d'un nombre borné exponentiellement d'éléments de la forme $hg^{\pm 1}h^{-1}$ où $g \sim 1$, $|g|_{F(A)} \leq k$ et h est un élément quelconque de $F(A)$.

Soit $g \in \ker(q)$. Comme $\ker(q) = F(\ker(p))$, on peut choisir $w \in \ker(p)$ tel que $F(w) = g$. Supposons que $w = a_1 \dots a_n$. Pour chaque $i \leq n$, on pose $u_i = l(a_1 \dots a_i)$, où l est la fonction qui à un mot quelconque associe une orthographe de l'élément qu'il représente, construite au Théorème 3.2.1. Comme, $u_n = l(a_1 \dots a_n) = l(w) \sim w \sim 1$, on a $u_n = l(1) = u_0$. Notons que ce mot est indépendant du choix de w . Par la Proposition 3.2.2, il existe un $c \in \mathbb{N}$ tel

que $|u_i| \leq c^i \leq c^n$ pour tout $i \leq n$. Notons aussi que

$$u_{i+1} \sim (a_1 \dots a_i) a_{i+1} \sim u_i a_{i+1}$$

ce qui nous permettra d'appliquer le lemme précédent. Finalement, on a

$$u_0 w u_n^{-1} = u_0 a_1 \dots a_n u_n^{-1} = u_0 a_1 (u_1^{-1} u_1) a_2 (u_2^{-1} u_2) a_3 \dots a_n (u_n^{-1} u_n) = \prod_{i \leq n} (u_{i-1} a_i u_i^{-1})$$

et par le lemme précédent, chacun des facteurs se factorise en un produit de $|u_i| + |u_{i+1}|$ termes de la forme $hg^{\pm 1}h^{-1}$. On obtient donc $|u_1| + |u_2| + |u_2| + |u_3| + \dots + |u_{n-1}| + |u_n| \leq (2n)c^n$ termes de la forme $hg^{\pm 1}h^{-1}$ avec $g \sim 1$ et $|g|_F \leq k$. Comme $u_0 = u_n \sim 1$, ils sont eux-mêmes de termes de la forme appropriée $hg^{\pm 1}h^{-1}$; ici, $h = 1$, $g = u_0$. On obtient alors l'expression

$$w = u_0^{-1} \left(\prod h g h^{-1} \right) u_n^{-1}$$

une factorisation de la forme voulue avec au plus $2 + 2nc^n$ termes, ce qui est exponentiel. \square

Corollaire 3.4.5. (*Epstein et al., 1992*) *Les groupes automatiques admettent une inégalité isopérimétrique quadratique.*

On utilise le même argument que pour le théorème précédent jusqu'à obtenir $2(|u_1| + \dots + |u_n|)$ termes, en utilisant la fonction l construite à la Proposition 3.2.3. Ceci assure que $|u_i|$ est au plus linéaire en n . Il existe donc un $c \in \mathbb{N}$ tel que $|u_i| \leq cn$ pour tout i . Après avoir ajouté les u_0 et u_n^{-1} , on obtient alors au plus $2n(cn) + 2$ ce qui est quadratique en n . \square

CONCLUSION

Ce mémoire a fait la synthèse de l'état actuel de l'étude des structures algébriques en fonction de leur complexité calculatoire, en présentant l'évolution depuis les premières structures étudiées historiquement, les groupes automatiques, jusqu'aux structures nouvellement définies, les semigroupes quasi-automatiques. Plusieurs résultats récents, dû principalement à Benjamin Blanchette, Christian Choffrut et Christophe Reutenauer y sont exposés, l'existence d'une inégalité isopérimétrique pour les groupes quasi-automatique formant en quelque sorte l'aboutissement de ces travaux.

Plusieurs questions ouvertes demeurent. D'abord, on ne connaît pas d'exemple de semigroupe quasi-automatique qui n'est pas asynchrone. Tous les groupes asynchrones (respectivement automatique) admettent un dictionnaire asynchrone (respectivement automatique) en bijection avec le groupe. On ne sait pas si c'est toujours possible pour les semigroupes quasi-automatiques. Est-il décidable de déterminer si un semigroupe quasi-automatique est aussi automatique ou asynchrone? Si un semigroupe quasi-automatique est un monoïde? Si un semigroupe quasi-automatique est fini? Comme les semigroupes de cette classe admettent des propriétés clés permettant de les traiter de façon algorithmique, ces problèmes pourraient s'avérer décidables dans d'éventuels travaux.

BIBLIOGRAPHIE

- [1] A. Arnold, M. Latteux, *A new proof of two theorems about rational transductions*, Theoretical Computer Science 8, 1979
- [2] J. Berstel, *Rational transduction and context-free languages*, Teubner, 1979
- [3] B. Blanchette, *Quasi-automatic groups are asynchronously automatic*, note acceptée pour publication à Theoretical Computer Science, 2019
- [4] B. Blanchette, C. Choffrut, C. Reutenauer, *Quasi-automatic semigroups*, Theoretical Computer Science, 2019
- [5] C.M. Campbell, E.F. Robertson, N. Ruskuc, *Automatic semigroups*, Theoretical Computer Science 250, 2001
- [6] A.J. Duncan, E.F. Robertson, N. Ruskuc, *Automatic monoids and change of generators*, Mathematical Proceedings of the Cambridge Philosophical Society 127, 1999
- [7] S. Eilenberg, *Automata, languages and machines*, Volume A, 1974, Academic Press
- [8] D.B.A. Epstein, J.W. Cannon, D. Holt, S.V.F. Levy, M.S. Paterson, W.P. Thurston, *Word Processing in groups*, Jones and Barlett Publishers, Boston, 1992
- [9] C.C Elgot, G. Mezei, *On relations defined by generalized finite automata*, IBM Journal of research and development 9, 1965
- [10] M. Nivat, *Transduction des langages de Chomsky*, Annales de l'institut Fourier 18, 1968
- [11] J-E. Pin, *Mathematical Foundation of Automata Theory*, 2012
- [12] J. Sakarovitch, *Easy multiplication I*, Information and Computation, 74, 1987
- [13] J. Van Leeuwen, M. Nivat, *Efficient recognition of rational relations*, Information and Processing Letters 14, 1982

INDEX

- étoile, 10
- actif, 17
- alphabet, 5
- anneau, 5
- automate, 15
- automate accessible, 17
- automate coaccessible, 17
- automate déterministe, 15
- automate miroir, 16

- bijective, 4

- complexité algorithmique, 43, 44
- composition, 3

- dictionnaire, 6
- dictionnaire asynchrone, 20, 39
- dictionnaire automatique, 20
- dictionnaire faiblement Lipschitz, 21
- dictionnaire Lipschitz, 20, 24
- dictionnaire Lipschitz Hausdorff, 21
- dictionnaire quasi-automatique, 20, 39
- dictionnaires asynchrones, 22
- dictionnaires automatiques, 22
- dictionnaires faiblement Lipschitz, 34
- dictionnaires quasi-automatiques, 24

- facteur, 5
- finiment engendré, 6
- fonction, 3
- fonction de départ, 38

- fonction de remplissage, 18
- fonction séquentielle, 16, 41

- groupe, 4
- groupe automatique, 26
- groupe libre, 9
- groupes quasi-automatiques, 36

- identité, 3
- image, 3
- inégalité isopérimétrique, 47
- inactif, 17
- injective, 4
- inverse, 4
- isomorphisme, 6

- langage, 5
- langage de Nivat, 14
- langage rationnel, 11
- longueur réduite, 10

- métrique, 6
- métrique du mot, 7, 9
- monoïde, 4
- monoïde libre, 5
- monoïde quasi-automatique, 46
- monoïdes automatiques, 29
- morphisme, 5
- mot vide, 5

- norme, 6

orthographe, 6

parties rationnelles, 11

parties reconnaissables, 12

post-inverse, 4

pré-inverse, 4

préfixe, 5

problème du mot, 43

produit, 10

projection à gauche (droite), 14

relation, 3

relation inverse, 3

relation rationnelle, 41

relations multiplicatives, 19

relations multiplicatives élémentaires, 20

relations rationnelles, 14

semi-anneau, 4

semigroupe, 4

semigroupe automatique, 44

semigroupe gradué, 39

semigroupe libre, 5

semigroupe quasi-automatique, 33

semigroupe rationnel, 32

suffixe, 5

surjective, 4

système d'écriture, 6

système d'écriture de groupe, 9

transducteur, 16, 41

unité, 5