Machines de Mealy, (semi-)groupes d'automate, problèmes de décision et génération aléatoire

Thibault Godin

Université Sorbonne Paris Cité
Université Paris Diderot - Paris 7

Institut de Recherche en Informatique Fondamentale

Thèse

présentée pour l'obtention du diplôme de

Docteur de l'Université Paris Diderot,
spécialité Informatique

à l'École doctorale de Sciences Mathématiques de Paris Centre

---

Machines de Mealy, (semi-)groupes d'automate, problèmes de décision et génération aléatoire

---

Par : Thibault Godin

Soutenue publiquement le 13 juillet 2017 à Paris *devant le jury constitué de :*

Nathalie Aubrun	CR	CNRS & ENS de Lyon	*Examinatrice*
Ines Klimann	MC	Université Paris Diderot	*Directrice de thèse*
Markus Lohrey	PU	Université de Siegen	*Examinateur*
Jean Mairesse	DR	CNRS & Université Pierre et Marie Curie	*Rapporteur*
Cyril Nicaud	PU	Université Paris Est Marne la Vallée	*Président du jury*
Matthieu Picantin	MC	Université Paris Diderot	*Directeur de thèse*
Dmytro Savchuk	PU	Université de Floride du Sud	*Examinateur*
Olivier Serre	DR	CNRS & Université Paris Diderot	*Examinateur*
Après avis des rapporteurs			
Jean Mairesse	DR	CNRS & Université Pierre et Marie Curie	*Rapporteur*
Pascal Weil	DR	CNRS & Université de Bordeaux	*Rapporteur*

Résumé

Dans cette thèse, on se propose d'étudier les automates de Mealy, c'est-à-dire des transducteurs complets déterministes lettre à lettre ayant même alphabet d'entrée et de sortie. Ces automates sont utilisés depuis les années 60 pour engendrer des (semi-)groupes qui ont parfois des propriétés remarquables, permettant ainsi de résoudre plusieurs problèmes ouverts en théorie des (semi-)groupes. Dans ce travail, on s'intéresse plus particulièrement aux apports possibles de l'informatique théorique à l'étude de ces (semi-)groupes engendrés par automate. La thèse présentée s'articule autours de deux grands axes. Le premier, qui correspond aux chapitres II et III, traite des problèmes de décision et plus spécifiquement du problème de Burnside dans le chapitre II et des points singuliers dans le chapitre III. Dans ces deux chapitres on met en lien des propriétés structurelles de l'automate avec des propriétés du groupe engendré ou de son action. Le second axe, représenté par le chapitre IV, se rapporte à la génération aléatoire de groupes finis. On cherche, en tirant des automates de Mealy aléatoirement dans des classes spécifiques, à engendrer des groupes finis, et on aboutit à un résultat de convergence pour la distribution ainsi obtenue. Ce résultat fait écho au théorème de Dixon pour les groupes de permutations aléatoires.

Mots clefs : Automates de Mealy, Groupes, Semi-groupes, Transducteurs, Problèmes de décision, Génération aléatoire

Abstract

In this thesis, we study Mealy automata, i.e. complete, deterministic, letter-to-letter transducers which have same input and output alphabet. These automata have been used since the 60s to generate (semi)groups that sometimes have remarkable properties, that were used to solve several open problems in (semi)group theory. In this work, we focus more specifically on the possible contributions that theoretical computer science can bring to the study of these automaton (semi)groups. The thesis consists of two main axis. The first one, which corresponds to the Chapters II and III, deals with decision problems and more precisely with the Burnside problem in Chapter II and with singular points in Chapter III. In these two chapters, we link structural properties of the automaton with properties of the generated group or of its action. The second axis, which comprises the Chapter IV, is related with random generation of finite groups. We seek, by drawing random Mealy automata in specific classes, to generate finite groups, and obtain a convergence result for the resulting distribution. This result echoes Dixon's theorem on random permutation groups.

Keywords : Mealy automata, Groups, Semigroups, Transducers, Decision problems, Random generation

Remerciements

Ce mémoire représente la conclusion de trois ans passés en thèse au LIAFA/IRIF. Trois ans de recherche, de rencontres, de discussions et de moments partagés avec de nombreuses personnes, et j'ai donc énormément de remerciements à formuler. En voici une partie, qui ne peut malheureusement qu'être incomplète.

Avant tout, je souhaite sincèrement remercier mes directeurs de thèse, Ines et Matthieu, bien entendu pour m'avoir permis de faire mon doctorat avec eux, mais surtout pour la manière dont ils l'ont encadré. J'ai eu la chance d'avoir deux super directeurs qui m'ont suivi aussi bien scientifiquement qu'humainement, qui ont toujours été disponibles pour m'expliquer quand je ne comprenais pas et m'écouter quand je croyais comprendre. Ils ont su me faire progresser sur le plan mathématique/informatique, mais aussi sur tous les autres aspects qui l'entourent, en particulier la communication (même s'il reste du travail). Désolé enfin pour la peine que je leur ai infligée avec les nombreuses relectures de cette thèse, merci infiniment.

Je voudrais aussi remercier Jean et Pascal pour avoir accepté d'être rapporteurs de ce manuscrit et d'en avoir pointé les approximations et les manques. Merci également aux autres membres du jury, Natalie, Markus, Cyril, Dmytro et Olivier qui me font le plaisir de s'intéresser un peu à mes travaux. In particular I want to thanks Markus and Dima for having accepted to come from far away even if this thesis is written in French. J'en profite pour remercier Cyril, qui participait à la réunion qui est à l'origine de mon article sur la génération aléatoire de groupes finis et qui a ensuite souvent répondu à mes questions à ce sujet. Ma soutenance étant l'occasion de revoir de nombreuses personnes que j'ai croisées et avec qui j'ai travaillé durant cette thèse, je voudrais aussi dire *grazie* Daniele e Emanuele for the work we've done together, the trips in Porto, Graz and Rome and the work we'll do ! Merci aussi à Laurent pour sa pédagogie et sa culture.

J'ai donc passé trois ans dans le Laboratoire d'Informatique Algorithmique : Fondements et Applications, qui est devenu l'Institut de Recherche en Informatique Fondamentale. Quel que soit le nom choisi, ce labo a été le meilleur environnement que j'aurais pu espérer pour ma thèse. Sans parler de la qualité scientifique de ses membres, je veux souligner leur gentillesse générale, qui rend faciles les échanges, scientifiques ou non. J'aimerais donc remercier toutes les personnes qui y travaillent, et plus spécialement du côté des permanents les deux Olivier, Valérie, Reem, Anne, Dominique, Thomas, Jean-Baptiste, Arnaud, Yann, Sophie et Sylvain pour ces moments partagés.
L'IRIF n'est toutefois pas le seul laboratoire au monde et je tiens aussi à remercier les gens que j'ai rencontrés à Créteil, Pascal, Sabrina, Youssouf et Paul-Elliot ; ceux que j'ai connu au LaBRI, Patxi, Tatiana, Claire, Jean-François et spécialement Hugo et Anca qui ont encadré mon

mémoire de M2 et m'ont aidé à trouver ma thèse ; ceux de Montpellier, Jérémie, Guilhem et Anaël ; ceux de Marseille, Pierre et Guillaume ; ceux de Lyon, Sebastián, Matthieu et Paul ; ou encore ceux de Poitiers, de Toulouse, de Belgique, d'Allemagne, d'ALEA, de SDA2, des EJCIM, de YGGT, d'Highlights et d'ailleurs ...

Vient le tour des thésards (et post-doc/ATER) du labo, avec qui j'ai partagé café, repas et surtout plein de bons moments. J'ai appris beaucoup de choses utiles grâce à eux, et encore plus de choses inutiles (les concombres de mer sont majoritairement benthiques®). Je dois aussi m'excuser auprès d'eux (et de plein d'autres gens) pour leur avoir posé les questions qui m'embêtaient [1], merci pour avoir régulièrement fait semblant d'y réfléchir. Obrigado, gracias, danke et merci au Power Rangers Alex, Bruno, Fabian et Raphaël, mention spéciale à la machine à conjectures Charles, et plus généralement merci aux fidèles du coin café, Alexandre, Benjamin, Bruno, Finn, Guillaume, Khaled, Laurent, Simon, Victor ; du gâteau, Amina, Étienne les Pierre et Yann ; et à tous ceux que je croisais régulièrement, Alkida, Arthur, Anna Carla, Daniela, Dennis, Greg, Jehanne, Jonas, Lucas, Maria Rita Mathieu, Mehdi, Pablo, Vincent. J'espère vous revoir très régulièrement.

En dehors du labo je peux aussi compter sur la présence indéfectible de tous mes amis, à Poitiers, Paris et partout ailleurs. Pas d'inventaire à la Prévert ici de peur d'oublier quelqu'un mais merci de me supporter même quand je suis insupportable.

Un grand merci aussi à mes parents, ma famille qui m'ont toujours soutenu, y compris quand ils ne comprenaient pas vraiment ce que je faisais ou quand je ne savais pas vraiment où j'allais. Ils m'ont permis de faire ce qui me plaisait dans les meilleurs conditions possibles. Un gros bisou aussi à mes deux grands-mères et merci à François pour son amour fraternel sans faille.

Le dernier remerciement est pour Lucie, même si mes mots ne suffisent pas.

1. Par exemple, prenons deux permutations aléatoires dans S_k, comment prouve-t-on que la probabilité qu'elles soient de même ordre est asymptotiquement proportionnelle à $1/k^2$? Question devenue célèbre comme "le truc de Thibault sur les permutations", forte récompense offerte pour une réponse.

Table des matières

Notations

$\mathcal{A}$ Automate de Mealy, c'est-à-dire un quadruplet $(Q, \Sigma, \delta, \rho)$.

Q Ensemble (fini) des états d'un automate de Mealy.

Σ Alphabet (fini) d'un automate de Mealy.

δ Ensemble des fonctions de transition $\delta_x : Q \to Q$, $x \in \Sigma$ d'un automate de Mealy.

ρ Ensemble des fonctions de production $\rho_q : \Sigma \to \Sigma$, $q \in Q$ d'un automate de Mealy.

$\equiv$ Équivalence de Nerode.

$\sim$ Équivalence sur les tiges.

$\wedge$ Équivalence de voisinage sur les tiges.

$|A|$ Cardinal de l'ensemble A.

A^* Ensemble des mots finis sur l'ensemble A.

A^ω Ensemble des mots infinis sur l'ensemble A.

$\widetilde{A}$ Ensemble involutif de A, *i.e.* $A \sqcup A^{-1}$.

$\mathfrak{m}\mathcal{A}$ Minimisé d'un automate de Mealy $\mathcal{A}$.

$\mathfrak{t}(\mathcal{A})$ Arbre lexicographique de Schreier d'un automate de Mealy $\mathcal{A}$.

$\mathfrak{d}\mathcal{A}$ Dual d'un automate de Mealy $\mathcal{A}$.

$\mathfrak{e}\mathcal{A}$ Expansé d'un automate de Mealy $\mathcal{A}$.

e État-puits d'un automate $\mathcal{A}$.

$\langle S \rangle_+$ Semi-groupe engendré par S.

$\langle S \rangle$ Groupe engendré par S.

$\mathbf{St}_G(\boldsymbol{\xi})$ Stabilisateur d'un mot $\boldsymbol{\xi}$ dans le groupe G.

$\mathbb{N}$ Nombres naturels, *i.e.* entiers positifs ou nuls.

S_k Groupe symétrique sur k éléments.

A_k Groupe alterné sur k éléments, permutations de S_k de signature 1.

$\mathbb{1}$ Élément neutre du groupe.

$|g|$ Ordre de l'élément g.

$H \leq G$ Le groupe H est un sous-groupe du groupe G.

$\boldsymbol{\xi}[i:j]$ Facteur du mot $\boldsymbol{\xi}$ compris entre les positions i (incluse) et j (exclue).

$\boldsymbol{\xi}[:j]$ Préfixe du mot $\boldsymbol{\xi}$ jusqu'à la position j (exclue).

$\boldsymbol{\xi}[i:]$ Suffixe du mot $\boldsymbol{\xi}$ à partir de la position i (incluse).

$|\boldsymbol{u}|$ Longueur du mot $\boldsymbol{u}$.

Chapitre I

Automates de Mealy et théorie des groupes

Quelques définitions et exemples

Cette thèse est à l'intersection des mathématiques et de l'informatique. La partie mathématique provient de la *théorie des (semi-)groupes*, une théorie qui s'est initialement développée à la fin du XVIII^{e} siècle avec Lagrange, mais surtout au siècle suivant avec Galois et Cauchy. Conçue à l'origine pour étudier les racines de polynômes, cette notion de groupe s'est rapidement révélée utile car elle généralise de façon abstraite l'idée de *symétrie*. De fait, le théorème de Frucht [39] dit, en substance, que tout groupe fini peut être vu comme l'ensemble des symétries d'un graphe. Au cours du XX^{e} siècle, cette notion de (semi-)groupe est devenue plus abstraite tout en incorporant des éléments de divers horizons des mathématiques (topologie, analyse, algèbre multi-linéaire), pour devenir une branche majeure des mathématiques contemporaines.

La partie informatique de cette thèse, la *théorie des automates*, a été formalisée plus tardivement, dans les années 1950 [4], mais est une des briques de base de l'informatique théorique, et se retrouve très tôt dans la notion de calcul. En effet, on peut voir les automates comme une abstraction simple d'un modèle de calcul, moins puissante que les fameuses machines de Turing, mais tout de même capable de modéliser de nombreux phénomènes. La théorie des automates est naturellement en lien avec la logique [4] et la théorie des langages (formels ou naturels).

Ces deux théories, des (semi-)groupes et des automates ont très tôt été reliées, notamment par Schützenberger qui introduit dès les balbutiements de la théorie des automates, en 1956 [90], la notion de *monoïde syntaxique* qui permet de caractériser dans des termes d'algèbre les langages reconnus par un automate. Par exemple, dans [89], Schützenberger montre que les automates

reconnaissant les langages sans étoile sont exactement ceux dont le monoïde syntaxique est apériodique. Dès lors, une branche importante de l'étude des langages formels et de la théorie des automates a utilisé les semi-groupes comme un outil, voir par exemple [88, 85].

À l'inverse, dès les années 60, Gluškov [43] propose d'utiliser les automates, et plus exactement les *automates de Mealy*, pour engendrer des (semi-)groupes. C'est cette construction qui nous intéresse plus particulièrement dans cette thèse. En effet, cette idée s'avère extrêmement fructueuse en théorie des (semi-)groupes, puisque nombre de conjectures et de problèmes ouverts ont été résolus en utilisant ces ***(semi-)groupes engendrés par des automates de Mealy***. On peut résumer grossièrement et subjectivement la chronologie des groupes de Mealy en quelques dates : en **1972**, Alešin donne un exemple d'un groupe de Burnside infini comme sous-groupe d'un groupe d'automate [2]. Puis, en **1980** Grigorchuk améliore le résultat d'Alešin en exhibant un exemple de 2-groupe infini engendré par un automate de Mealy [50]. Grigorchuk montre en **1984** que le groupe d'Alešin-Grigorchuk est à croissance intermédiaire, répondant ainsi à une question de Milnor [49]. Gupta et Fabrykowski donnent en **1985** un nouvel exemple de groupe d'automate ayant une croissance intermédiaire [36], et Gupta et Sidki donnent, dans [57], en utilisant les automates de Mealy, en **1989** des exemples de p-groupes infinis pour tout nombre premier p.
En **2000**, Grigorchuk et Zuk effectuent des calculs sur le spectre et la mesure spectrale de l'opérateur de Markov de la marche aléatoire simple sur le groupe de l'allumeur de réverbères [55]. Ces calculs les conduiront à réfuter une conjecture d'Atiyah peu après, tandis qu'en **2004**, Wilson montre, en présentant l'exemple d'un groupe d'automate, qu'un groupe peut avoir une suite de systèmes de générateurs telle que le taux de croissance de ce groupe soit aussi proche de 1 que désiré, répondant ainsi à une question de Gromov. En **2005**, Glasner et Mozes montrent que le groupe libre de rang 2 peut être engendré par un automate (biréversible) de Mealy [42]. Dans la foulée, Steinberg, M. Vorobets et Y. Vorobets démontrent que tous les groupes libres de rangs finis pouvaient être engendrés par des automates de Mealy [97].
En **2010**, I. Bondarenko, V. Bondarenko, Sidki et Zapata utilisent la structure de l'automate pour montrer que les problèmes de l'ordre et de la conjugaison sont décidables pour une certaine classe de groupes d'automate [19]. Et en **2014**, Gillibert montre que le problème de l'ordre et de la finitude sont indécidables pour les semi-groupes d'automate [41], tandis que Klimann démontre que le problème de finitude est décidable pour une classe très structurée d'automates [63].

On voit qu'ici la situation est renversée par rapport au paragraphe précédent : la théorie des (semi-)groupes se sert des automates de Mealy comme d'un outil. En fait, dans un certain nombre de cas, les automates sont même utilisés comme une boîte noire, qui fournit un (semi-)groupe et que l'on peut oublier après coup. Dans cette thèse nous allons au contraire nous concentrer sur cet automate et ses propriétés, en vue de fournir des informations sur le (semi-)groupe engendré.

Organisation de la thèse

Cette thèse est organisée en quatre grands chapitres :

Tout d'abord, un chapitre I, **Automates de Mealy et théorie des groupes**, lui même divisé en une première partie informelle (section 1) qui donne les motivations qui ont conduit à la thèse, puis une introduction plus technique (section 2), qui définit formellement les objets utilisés. Cette deuxième partie contient néanmoins quelques exemples afin d'en faciliter la lecture et la compréhension.

Dans le chapitre II, **Automates de Mealy et problème de Burnside**, on s'attaque au problème de décision *"le groupe engendré par l'automate est-il un groupe de Burnside infini ?"* dans le cas de la sous-classe importante formée des *automates de Mealy réversibles*. Après avoir mis en place un outil adapté à l'étude des problèmes d'ordre dans cette classe, on montre que les propriétés structurelles de l'automate influent fortement sur le groupe engendré, et cela en deux temps.
Tout d'abord on se place dans le cadre des automates inversibles et réversibles mais non-biréversibles, et on montre qu'alors la réponse est toujours négative. Puis on étudie la classe des automates biréversibles. Dans cette classe nous n'avons pas réussi à conclure dans tous les cas, mais on aboutit à un critère qui donne une réponse négative pour tous les automates connexes ayant un nombre premier d'états, ainsi que dans quelques autres cas moins bien cernés. Ce chapitre est basé sur deux articles publiés pendant la thèse, le premier avec Ines Klimann et Matthieu Picantin [46], le second avec Ines Klimann [45].

Le chapitre III, **Dynamique de l'action du groupe d'automate sur l'arbre enraciné infini**, traite du groupe engendré par l'automate via son action sur les mots infinis. On s'intéresse en particulier à des mots qui sont stabilisés mais dont le voisinage ne l'est pas, et on explique comment des outils classiques de théorie des automates et des langages permettent d'exprimer, sous certaines conditions de structure de l'automate, l'ensemble de ces points comme un langage reconnu par un automate sur les mots infinis. Enfin on met en lien cette action avec un problème de pavage par des tuiles de Wang, et l'on se sert de cet objet pour prouver un résultat d'indécidabilité. Ce chapitre correspond à un travail soumis, écrit avec Daniele D'Angeli, Ines Klimann, Matthieu Picantin et Emanuele Rodaro.

Enfin, le dernier chapitre, intitulé **Génération aléatoire de groupes**, est consacré à un problème de génération aléatoire de groupes finis. Le but est d'obtenir une distribution homogène, ou tout au moins contrôlée sur les groupes finis, ce qu'on ne sait pas faire présentement. On part alors d'une idée assez simple : pour engendrer aléatoirement un groupe, une méthode possible est de générer aléatoirement un automate de Mealy, puis d'engendrer un groupe avec celui-ci. On obtient ainsi une méthode originale, qu'on essaye d'appliquer à la génération de groupes

finis (car en pratique, on considère souvent les groupes finis et les groupes infinis séparément). Cette méthode, initiée avec Cyril Nicaud et Sven de Felice, mène à l'étude spécifique de certains automates et aboutit à un résultat analogue à un théorème important en théorie des groupes finis, le théorème de Dixon. Ce chapitre correspond à l'article [44], et contient des réflexions sur d'autres méthodes pour la génération de groupes finis avec des automates de Mealy.

1 À la chasse aux papillons

Ou, j'espère, un exemple intéressant d'automate.

Dans cette section, on procède à l'étude détaillée d'un automate de Mealy, dont on montre entre autres qu'il engendre un groupe de Burnside infini. Elle nécessite d'avoir déjà rencontré, au moins de loin, les automates de Mealy ou tout au moins les transducteurs. Dans le cas contraire, la section 2 présente une introduction complète et détaillée des notions utilisées ici.

L'automate Bread-and-Butterfly est l'automate de Mealy $\mathcal{BBF}$, à 7 états et 4 lettres, dessiné figure I.1. Sur cette figure on a représenté en bleu l'automate de Grigorchuk $\mathcal{G}$ qui est à la base de la construction du Bread-and-Butterfly.

Pourquoi le Bread-and-Butterfly ?

Dans le cadre de l'article [29], nous cherchions des automates ayant une quantité indénombrable de points singuliers (voir le chapitre III pour plus de détails). On a réussi en modifiant l'automate de Grigorchuk. Prenons deux copies de cet automate, inversons les lettres sur l'une des copies puis identifions certains états : on obtient l'automate représenté figure III.5. On s'est alors intéressé à cet exemple, et on s'est demandé quelles propriétés de l'automate de Grigorchuk étaient conservées. Au final, l'automate ne nous a pas semblé avoir de propriétés réellement remarquables, en dehors de celle que l'on recherchait initialement.
Cependant, on a continué de regarder ce type de constructions, en se concentrant sur la propriété de Burnside.
On a de nouveau modifié l'automate $\mathcal{G}$ de Grigorchuk pour obtenir l'automate $\mathcal{BBF}$. On a choisi de dédoubler l'alphabet entre lettres négatives sur une copie de l'automate et positives sur l'autre (d'où le choix surprenant de ± 0). On a alors identifié les états a, b et e des deux automates. Restait à définir les actions sur l'alphabet de signe opposé. On a choisi de calquer l'idée du produit direct (voir plus loin, dans l'introduction technique, section 2), et on a défini l'action comme étant triviale sur l'alphabet de signe opposé et envoyant certains états sur l'identité et d'autres sur a (sans que cette décision semble changer profondément le groupe engendré). Comme on le voit, ces choix sont assez arbitraires (trois "on a choisi" dans le paragraphe) et suivent, pour l'instant, une démarche de type "essai-échec" plus qu'une théorie construite. On espère bien entendu pouvoir obtenir une formalisation dans un second temps.

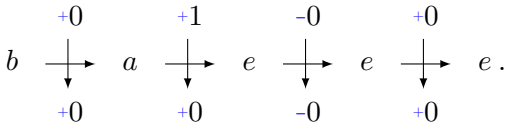
Commençons par un peu de vocabulaire : l'ensemble $Q = \{a, b, \pm c, \pm d, e\}$ est appelé l'*ensemble*

des états de $\mathcal{BBF}$. L'ensemble $\Sigma = \{\pm 0, \pm 1\}$ est quant à lui appelé son *alphabet*.

Le Bread-and-Butterfly, et de manière plus générale les automates de Mealy, sont des *transducteurs*. L'intérêt de ces objets est de pouvoir *lire* des mots sur l'alphabet depuis un état, tout en écrivant un mot en retour, tout cela en suivant les transitions (flèches) étiquetées par les lettres du mot. Par exemple, depuis l'état b, si on lit le mot $+0+1-0+0$, on commence par suivre la flèche $b \xrightarrow{+0|+0} a$, on a donc produit la lettre $+0$, et on arrive dans l'état a. Il nous reste la fin du mot à lire, ce que l'on va faire depuis l'état a où l'on vient d'arriver. On suit maintenant la flèche $a \xrightarrow{+1|+0} e$, et ainsi on a produit la lettre $+0$, et on se retrouve dans l'état e alors qu'il nous reste à lire $-0+0$. On réitère le processus jusqu'à épuisement des lettres en entrée. Au final, on aura produit la suite de lettres $+0+0-0+0$, en étant passé par b (état de départ), a, e, e et e (état d'arrivée). Graphiquement on a

$$b \xrightarrow{+0|+0} a \xrightarrow{+1|+0} e \xrightarrow{-0|-0} e \xrightarrow{+0|+0} e$$

ou encore



On va maintenant voir ce que l'on peut dire plus spécifiquement sur les automates de Mealy et le Bread-and-Butterfly.

1.1 Semi-groupe et groupe d'automate

Dans l'automate $\mathcal{BBF}$, on remarque que chaque état induit une *fonction* de l'alphabet vers lui-même. Par exemple, l'état a transpose -0 et -1 d'une part, et $+0$ et $+1$ d'autre part. Cette fonction peut aussi être étendue aux mots sur l'alphabet : on a vu que b transforme $+0+1-0+0$ en $+0+0-0+0$, et on peut raisonner de même pour obtenir une *fonction de production* $\rho_b : \Sigma^* \to \Sigma^*$.

Ainsi on obtient un ensemble de fonctions induites par les états de $\mathcal{BBF}$ allant de Σ^* vers lui-même, conservant la longueur des mots. Ces fonctions conservent aussi les préfixes : si $\rho_b(\boldsymbol{s}) = \boldsymbol{s'}$ pour un certain $\boldsymbol{s} \in \Sigma^\ell$ (et donc $\boldsymbol{s'} \in \Sigma^\ell$), alors pour tout mot $\boldsymbol{t} \in \Sigma^m$ on a $\rho_b(\boldsymbol{st}) = \boldsymbol{s't'}$, où $\boldsymbol{t'} \in \Sigma^m$ (il en va de même pour les autres états de l'automate).
Comme ces fonctions ont le même ensemble de départ et d'arrivée, on peut les composer entre elles sans restriction. On obtient alors le *semi-groupe* :

$$\langle \rho_a, \rho_b, \rho_{-c}, \rho_{+c}, \rho_{-d}, \rho_{+d}, \rho_e \rangle_+ .$$

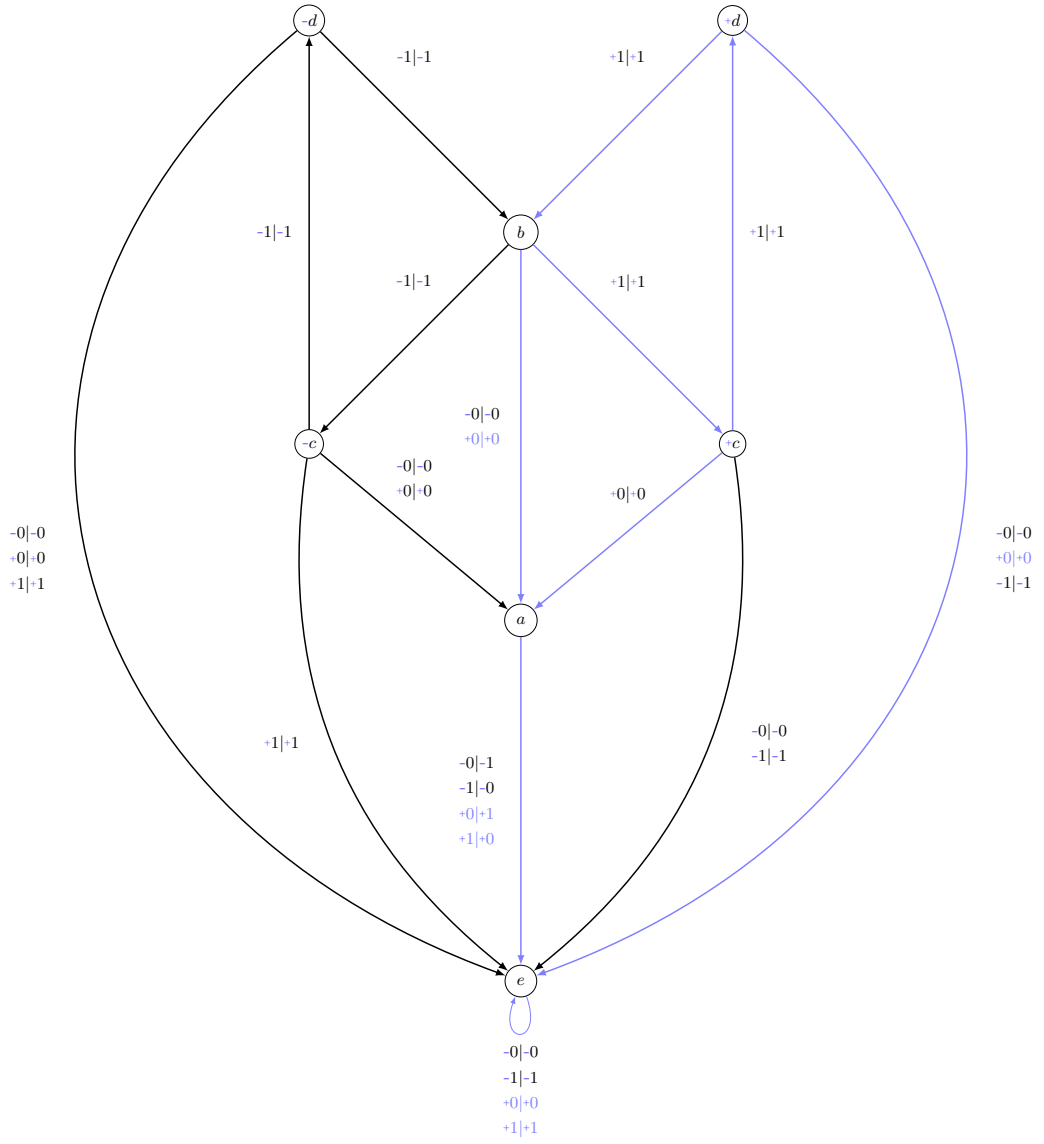
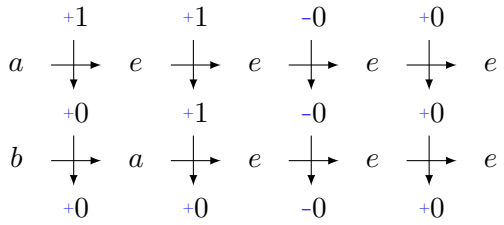


FIGURE I.1 – Ceci est un automate de Mealy.
On l'appelle l'automate Bread-and-Butterfly et on le note $\mathcal{BBF}$. Il est construit à partir de l'automate $\mathcal{G}$ de Grigorchuk, que l'on retrouve, dessiné en bleu, comme un sous-automate du Bread-and-Butterfly.

C'est ce semi-groupe, que l'on appelle *semi-groupe engendré* par $\mathcal{BBF}$ et note $\langle \mathcal{BBF} \rangle_+$, et qui fait l'objet de notre attention dans cette thèse.

Si l'on pose $\rho_{ab} = \rho_b \circ \rho_a$ on remarque que



et donc que la composition de fonctions correspond au *produit d'automates*.

Dans le Bread-and-Butterfly, on voit facilement que $\rho_e = \mathbb{1}_{\Sigma^*}$, l'identité sur les mots, ce qui implique que $\langle \mathcal{BBF} \rangle_+$ est en fait un monoïde.

Il est à noter que toutes les transformations induites par les états de l'automate $\mathcal{BBF}$ sont des *permutations* de Σ : a induit la permutation $(\text{-}0, \text{-}1)(\text{+}0, \text{+}1)$, tandis que les autres états induisent l'identité. Dans ce cas, les fonctions de production sont bijectives (on qualifie alors l'automate d'*inversible*), et l'on peut définir, pour chaque état q, la fonction inverse ρ_q^{-1}. On peut alors considérer une structure algébrique plus riche, le *groupe engendré* par l'automate $\mathcal{BBF}$, donné par

$$\langle \mathcal{BBF} \rangle = \langle \rho_a, \rho_b, \rho_{\text{-}c}, \rho_{\text{+}c}, \rho_{\text{-}d}, \rho_{\text{+}d}, \rho_e \rangle = \langle \rho_q, {\rho_q}^{-1},\ q \in Q^* \rangle_+ \ .$$

Cette condition d'inversibilité n'est pas toujours vérifiée (et donc on ne peut pas toujours définir le groupe engendré par l'automate). La figure I.2 montre comment on peut déterminer graphiquement si un automate est inversible.

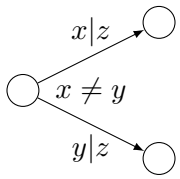
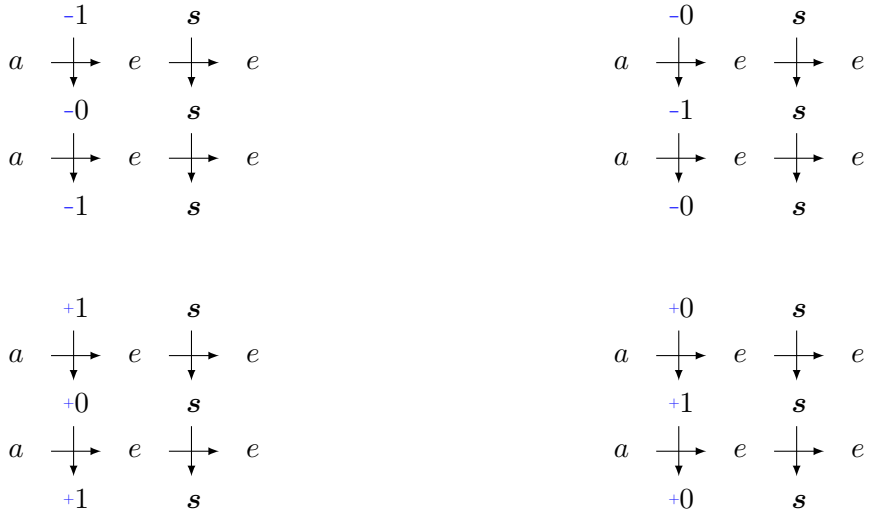


FIGURE I.2 – Configuration interdite pour les automates inversibles.

Ces groupes d'automate ont été étudiés à partir des années 60, suite à une suggestion de Gluškov [43]. En général, il est difficile d'en comprendre entièrement la structure car elle peut rapidement s'avérer complexe, surprenante ou inhabituelle, mais donc intéressante. En revanche, on peut déduire de nombreuses informations de l'*action* du groupe sur Σ^* (c'est-à-dire des transformations que l'automate induit sur Σ^*) et de la structure d'automate.

Une des propriétés majeures de ces groupes d'automate est que, si l'on se donne deux mots d'états, on peut déterminer s'ils représentent le même élément dans le (semi-)groupe engendré par l'automate. On dit que le *problème du mot* est *décidable*. On peut par exemple utiliser des techniques de minimisation sur l'automate. Ainsi, on peut toujours comparer des éléments en se basant sur leur représentation en terme de mots d'états, ce qui n'est pas toujours le cas pour un groupe, même finiment engendré.

On cherche à décrire quelques propriétés de notre groupe $\langle \mathcal{BBF} \rangle$. Par exemple, on peut voir que tous les états induisent une transformation non triviale dont le carré est l'identité (excepté pour e qui induit l'identité). On parle d'éléments d'ordre 2 ou encore d'involutions. Pour a, c'est assez facile :



Ces relations étant valides pour tout mot $\boldsymbol{s} \in \Sigma^*$, on a bien $\rho_{a^2} = \rho_a^2 = \mathbb{1}$. Pour b, c'est un peu plus fastidieux :

Puisque a^2 représente l'identité, b^2 induit l'identité sur les mots commençant par un $+0$. En revanche, si b^2 est sans effet sur le premier $+1$ d'un mot, il reste à analyser l'action de $+c^2$ sur le reste du mot :

Là encore, on peut conclure si le mot commence par ± 0 mais il convient de regarder $+d^2$.

On revient donc à b^2. Ainsi, toutes les situations soit mènent à l'identité (car on peut faire la même analyse pour les lettres/états négatifs), soit reviennent à b^2, donc on n'utilise jamais une transformation non triviale sur les lettres, et on conclut $\rho_{b^2} = \rho_{(\pm c)^2} = \rho_{(\pm d)^2} = \rho_{a^2} = \mathbb{1}$.

On voit cependant qu'en dépit de leur simplicité les calculs peuvent vite devenir d'une longueur rédhibitoire. Il s'agit du type d'opérations qui sont bien mieux gérées par une machine que par un humain, et on utilise donc la puissance de calcul de l'ordinateur, via, par exemple, le système de calcul **GAP** (Groups, Algorithms and Programming [40]). Il existe dans ce système de nombreux outils adaptés à l'étude des groupes en général et des groupes d'automate en particulier, et on peut également assez facilement programmer ses propres outils. À l'aide des paquets **FR** de Bartholdi [6] et **AutomGrp** de Muntyan et Savchuk [77], ainsi que de nombreuses petites fonctions programmées au long de la thèse, on simplifie les passages purement calculatoires.

Définissons notre automate $\mathcal{BBF}$ dans **GAP** (en utilisant la syntaxe **AutomGrp**[1] [77], où la première partie du vecteur code les transitions et la seconde donne la transformation induite par l'état sur la première lettre) :

1. On aurait pu utiliser **FR** [6], avec `gap> BBF_FR:=MealyMachine([[7,7,7,7],[1,1,3,5],[1,1,4,7],[7,7,2,7],[7,1,7,6],[7,7,7,2],[7,7,7,7]],[(1,3)(2,4),(),(),(),(),(),()],true);` où la première matrice code les transitions et la seconde les productions.

gap

```
 gap> BBF:=MealyAutomaton([[7,7,7,7,(1,3)(2,4)],[1,1,3,5,()],[1,1,4,7,()],
[7,7,2,7,()],[7,1,7,6,()], [7,7,7,2,()],[7,7,7,7,()]]);
-<automaton>
```

On peut alors considérer dans ce système le groupe engendré par $\mathcal{BBF}$, via

gap

```
 gap> GBBF:=AutomatonGroup(BBF);
-< a1, a2, a3, a4, a5, a6 >
```

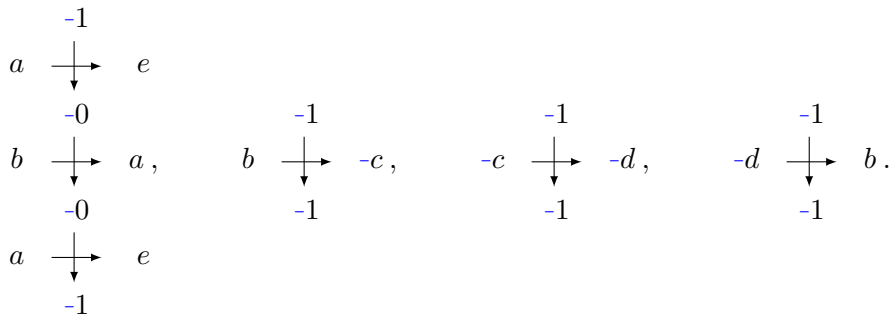
On peut même "demander à **GAP**" si le groupe engendré est fini ou infini, mais (malheureusement) on ne connaît pas d'algorithme permettant de résoudre systématiquement ce problème et en l'occurrence le programme ne fournit pas de réponse dans le cas de $\langle \mathcal{BBF} \rangle$, il faut donc le résoudre à la main.
Dans ce cas précis, on peut montrer assez aisément que le groupe est en fait infini, en s'inspirant d'une preuve de [58] pour démontrer l'infinitude du groupe engendré par l'automate de Grigorchuk :

Soit η définie par

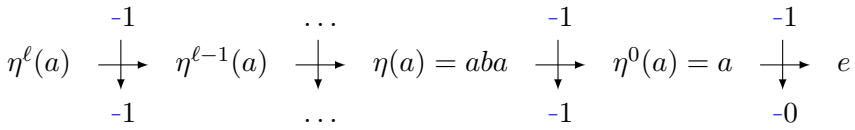
$$\begin{aligned} \eta : (Q \setminus \{e\})^* &\longrightarrow Q^* \\ a &\longmapsto aba \\ b &\longmapsto {-}d \\ {-}c &\longmapsto b \\ {-}d &\longmapsto {-}c \\ {+}c, {+}d &\longmapsto e \end{aligned}$$

On montre que les éléments $\eta^\ell(a)$ agissent tous différemment sur le mot -1^ω, ce qui témoigne que le groupe $\langle \mathcal{BBF} \rangle$ est infini.
Pour cela, remarquons que, pour η, les transitions suivant -1 correspondent presque à l'inverse

de la fonction. En effet on a les diagrammes en croix :



On a donc



et on voit que les actions diffèrent deux à deux : pour chaque $\ell > 0$, l'élément $\eta^\ell(a)$ transforme le mot $\text{-}1^\omega$ en le mot $\text{-}1^\ell\text{-}0\text{-}1^\omega$. Comme les actions des éléments ne coïncident pas, les éléments sont deux à deux différents, et ainsi on a :

Le groupe $\langle \mathcal{BBF} \rangle$ engendré par l'automate Bread-and-Butterfly est infini.

1.2 Groupe de Burnside

Un groupe de Burnside est un groupe ayant un nombre fini de générateurs, et où tous les éléments ont une puissance non nulle qui vaut l'identité. En 1902, Burnside demande dans [24] s'il existe un groupe infini satisfaisant ces conditions. On voit que tous les groupes finis sont des groupes de Burnside, tandis que $\mathbb{Z}$ et $\bigotimes_{\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ sont infinis mais ne sont pas des groupes de Burnside, respectivement car $\mathbb{Z}$ possède des éléments d'ordre infini (tous les éléments différents de 0 en fait), et $\bigotimes_{\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$ ne peut être engendré par un nombre fini d'éléments. La réponse à la question de Burnside, qui ne fut donnée que 62 ans plus tard, est positive. Cependant ces premiers exemples ne sont pas vraiment manipulables. Alešin en 1972 [2], puis Grigorchuk en 1980 [50], proposent des exemples de groupes de Burnside infinis sous la forme, chronologiquement, d'un sous-groupe puis d'un groupe d'automate. Ces exemples ont certainement constitué un tournant dans l'étude des groupes d'automate, et continuent d'être décortiqués, analysés et généralisés.

Après expérimentations en **GAP**, il nous a semblé que le groupe $\langle \mathcal{BBF} \rangle$ était peut-être un groupe de Burnside infini. Nous montrons que c'est bien le cas en adaptant une démonstration présente dans [58].

Une des propriétés cruciales du groupe de Grigorchuk qui permet aisément de montrer que tous ses éléments sont d'ordre fini est que $\langle b, c, d\rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On a l'analogue pour le groupe engendré par les états différents de a dans le Bread-and-Butterfly :

gap

```
gap> StructureDescription(Group(a2,a3,a4,a5,a6));
-"C2 x C2 x C2 x C2 x C2"
```

Cependant, le point réellement important ici est que, pour le groupe de Grigorchuk, on a $\langle b, c, d\rangle = \{\mathbb{1}, b, c, d\}$, et, comme chaque générateur a, b, c et d est d'ordre 2, on obtient une forme normale pour les éléments du groupe de Grigorchuk : tout élément g de ce groupe peut s'écrire comme un produit $g = (a)x_1ax_2a\cdots ax_{\ell-1}ax_\ell(a), x_i \in \{b, c, d\}$. On n'a pas cette propriété dans $\langle \mathcal{BBF}\rangle$ avec $\{b, \pm c, \pm d\}$, mais on peut tout de même arriver à une forme normale analogue en posant pour la suite $S = \langle b, \pm c, \pm d\rangle \setminus \{\mathbb{1}\}$. Posons également $S_a = S \sqcup \{a\}$, de sorte que S_a forme un système de 32 générateurs pour $\langle \mathcal{BBF}\rangle$. On a donc, pour tout élément $g \in \langle \mathcal{BBF}\rangle$,

$$g = (a)x_1ax_2a\cdots ax_{\ell-1}ax_\ell(a), x_i \in S\,.$$

Le code suivant montre que tout élément de S représente un élément d'ordre 2 dans $\langle \mathcal{BBF}\rangle$ et que tout mot de longueur inférieure à 2 sur S_a représente un élément d'ordre au plus 128 dans $\langle \mathcal{BBF}\rangle$.

gap

```
gap> S1:=Group(a2,a3,a4,a5,a6);
-<a2, a3, a4, a5, a6>
gap> S:=Elements(S1)[2..32];;
gap> List(S, x->Order(x));
-[ 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2 ]
gap> List(S, x->Order(a1*x));
-[4, 4, 8, 8, 16, 4, 64, 32, 32, 8, 32, 16, 8, 16, 4, 64, 32, 32, 8, 16,
4, 32, 8, 4, 128, 32, 8, 4, 32, 128, 32 ]
```

On utilise la fonction `Decompose` de **GAP**, qui, à un élément associe ses successeurs dans l'automate.

gap

```
gap>decomp:=List(S,x->[x,Decompose(x),Decompose(a1*x*a1)]);
-[ [ a6, (1, 1, 1, a2), (1, a2, 1, 1) ],
[ a5, (1, a1, 1, a6), (1, a6, 1, a1) ],
[ a3, (a1, a1, a4, 1), (a4, 1, a1, a1) ],
[ a2, (a1, a1, a3, a5), (a3, a5, a1, a1) ],
[ a6*a4, (1, 1, a2, a2), (a2, a2, 1, 1) ],
[ a6*a5, (1, a1, 1, a2*a6), (1, a2*a6, 1, a1) ],
[ a6*a3, (a1, a1, a4, a2), (a4, a2, a1, a1) ],
[ a6*a2, (a1, a1, a3, a2*a5), (a3, a2*a5, a1, a1) ],
[ a4*a5, (1, a1, a2, a6), (a2, a6, 1, a1) ],
[ a4*a3, (a1, a1, a2*a4, 1), (a2*a4, 1, a1, a1) ],
[ a4*a2, (a1, a1, a2*a3, a5), (a2*a3, a5, a1, a1) ],
[ a5*a3, (a1, a1^2, a4, a6), (a4, a6, a1, a1^2) ],
[ a5*a2, (a1, a1^2, a3, a6*a5), (a3, a6*a5, a1, a1^2) ],
[ a3*a2, (a1^2, a1^2, a4*a3, a5), (a4*a3, a5, a1^2, a1^2) ],
[ a6*a4*a5, (1, a1, a2, a2*a6), (a2, a2*a6, 1, a1) ],
[ a6*a4*a3, (a1, a1, a2*a4, a2), (a2*a4, a2, a1, a1) ],
[ a6*a4*a2, (a1, a1, a2*a3, a2*a5), (a2*a3, a2*a5, a1, a1) ],
[ a6*a5*a3, (a1, a1^2, a4, a2*a6), (a4, a2*a6, a1, a1^2) ],
[ a6*a5*a2, (a1, a1^2, a3, a2*a6*a5), (a3, a2*a6*a5, a1, a1^2) ],
[ a6*a3*a2, (a1^2, a1^2, a4*a3, a2*a5), (a4*a3, a2*a5, a1^2, a1^2) ],
[ a4*a5*a3, (a1, a1^2, a2*a4, a6), (a2*a4, a6, a1, a1^2) ],
[ a4*a5*a2, (a1, a1^2, a2*a3, a6*a5), (a2*a3, a6*a5, a1, a1^2) ],
[ a4*a3*a2, (a1^2, a1^2, a2*a4*a3, a5), (a2*a4*a3, a5, a1^2, a1^2) ],
[ a5*a3*a2, (a1^2, a1^3, a4*a3, a6*a5), (a4*a3, a6*a5, a1^2, a1^3) ],
[ a6*a4*a5*a3, (a1, a1^2, a2*a4, a2*a6), (a2*a4, a2*a6, a1, a1^2) ],
[ a6*a4*a5*a2, (a1, a1^2, a2*a3, a2*a6*a5), (a2*a3, a2*a6*a5, a1, a1^2)],
[ a6*a4*a3*a2, (a1^2, a1^2, a2*a4*a3, a2*a5), (a2*a4*a3, a2*a5, a1^2, a1^2) ],
[ a6*a5*a3*a2, (a1^2, a1^3, a4*a3, a2*a6*a5),  (a4*a3, a2*a6*a5, a1^2, a1^3) ],
[ a4*a5*a3*a2, (a1^2, a1^3, a2*a4*a3, a6*a5), (a2*a4*a3, a6*a5, a1^2, a1^3) ],
[ a6*a4*a5*a3*a2, (1, a1, a2*a4*a3, a2*a6*a5),(a2*a4*a3, a2*a6*a5, 1, a1) ] ]
```

Ainsi, tout conjugué d'un élément de S par un élément de S_a se décompose dans le groupe $\langle \mathcal{BBF} \rangle$ comme un état ayant tous ses successeurs dans S_a (et où la permutation est triviale sur la première lettre). En d'autres termes, si on lit n'importe quel mot en partant d'un conjugué de S par un élément de S_a, alors on agit trivialement sur la première lettre puis on se comporte sur le reste du mot comme un élément de S_a.

On montre maintenant que tout élément de $\langle \mathcal{BBF} \rangle$ est d'ordre une puissance de 2. On

commence par :

Tout mot sur $\{a, b\}$ représente un élément dont l'ordre divise 16 dans $\langle \mathcal{BBF} \rangle$.

Rappelons que $a^2 = b^2 = \mathbb{1}$, donc tout mot sur $\{a, b\}$ peut se réécrire comme un mot $\boldsymbol{w} = (a)bab \cdots bab(a)$. Si la longueur de $\boldsymbol{w} \in \{a, b\}^*$ est impaire, alors $\boldsymbol{w}^2 = \mathbb{1}$, car la première et la dernière lettre de $\boldsymbol{w}$ sont égales et d'ordre 2. Sinon, $\boldsymbol{w} = \boldsymbol{v}^{k/2}$, avec $k/2 \in \mathbb{N}$ et $\boldsymbol{v} \in \{ab, ba\}$. Alors $\boldsymbol{w}^{16} = (\boldsymbol{v}^{k/2})^{16} = (\boldsymbol{v}^{16})^{k/2} = \mathbb{1}$, car $|ab| = |ba| = 16$.

Rappelons que si un élément est d'ordre fini, alors il en va de même pour tous ses conjugués. Notons aussi que, si un état q induit l'identité sur la première lettre, alors l'ordre de ρ_q est égal au plus petit commun multiple des ordres de ses successeurs dans l'automate selon chaque lettre de l'alphabet.

On a maintenant les outils pour montrer :

Proposition 1.1

Le groupe $\langle \mathcal{BBF} \rangle$ est un 2-groupe, c'est-à-dire que tout élément de $\langle \mathcal{BBF} \rangle$ est d'ordre une puissance de 2.

Démonstration. Soit $g \in \langle \mathcal{BBF} \rangle$. Considérons un de ses plus courts représentants $\boldsymbol{w}$ sur S_a et raisonnons par récurrence sur la longueur ℓ de $\boldsymbol{w}$. Par construction de S, on peut supposer que $\boldsymbol{w}$ s'écrit comme une alternance de a et d'une lettre de S. On a montré pour l'initialisation que tous les conjugués de S_a par un élément de S_a sont d'ordres une puissance de 2, et donc, pour $\ell < 3$, g est d'ordre une puissance de 2.
Supposons que ℓ soit *impaire*. Si $\boldsymbol{w}$ commence par un a, alors on a $\boldsymbol{w} = a\boldsymbol{u}a = \boldsymbol{u}^a$ (car $a^{-1} = a$), avec $\boldsymbol{u}$ un mot sur S_a de longueur $\ell - 2$. Donc par hypothèse de récurrence, et comme la conjugaison préserve l'ordre, g est d'ordre une puissance de 2.
Si $\boldsymbol{w}$ commence par un $p \in S$, alors on a $\boldsymbol{w} = p\boldsymbol{u}q$ avec $q \in S$. On peut, sans changer l'ordre, conjuguer par p^{-1} : $g^{p^{-1}} = p^{-1}p\boldsymbol{u}qp$. Cet élément est représenté ainsi par un mot $\boldsymbol{u}r$ de longueur $\ell - 1$ (car $qp = r \in S$), et donc g est d'ordre une puissance de 2 par hypothèse de récurrence.
Supposons maintenant ℓ *paire*. Par conjugaison, on peut supposer sans perte de généralité que $\boldsymbol{w}$ commence par un a.
On va distinguer plusieurs sous-cas, selon la longueur de $\boldsymbol{w}$.
Si ℓ est divisible par 4, alors $\boldsymbol{w} = aw_1au_1aw_2a \cdots aw_{\ell/4}au_{\ell/4}$ et on peut grouper les lettres de $\boldsymbol{w}$ en blocs de la forme aw_ia et u_i, avec les w_i et les u_i des lettres de S. Comme $\boldsymbol{w}$ a un nombre

pair de a agit comme l'identité sur la première lettre des mots. Par décomposition, on obtient $\boldsymbol{w} = (\boldsymbol{w}_{-0}, \boldsymbol{w}_{+0}, \boldsymbol{w}_{-1}, \boldsymbol{w}_{+1})()$, où les mots $\boldsymbol{w}_\alpha$ sont les successeurs de $\boldsymbol{w}$ selon $\alpha \in \{\pm 0, \pm 1\}$ et sont de longueur au plus $\ell/2$, car les blocs de la forme aw_ia se décomposent dans S. Ainsi, l'ordre de g est le ppcm des ordres des $\boldsymbol{w}_\alpha$, qui sont des puissances de 2 par hypothèse de récurrence. Si maintenant $\ell = 4j-2$ est divisible par 2 mais pas par 4, on va considérer g^2, représenté par $\boldsymbol{ww}$.

1. Si $\boldsymbol{w}$ contient une lettre x parmi un sous-ensemble de S de cardinal 7 alors, $x = (e, e, y, z)()$ et $axa = (y', z', e, e)()$, on a $\ell(\boldsymbol{w}_\alpha) \leq 4j - 3$ et on peut conclure (7 des 31 éléments de S).
2. Sinon, si $\boldsymbol{w}$ contient une lettre parmi un nouveau sous-ensemble de S privé des lettres considérées précédemment alors les mots $\boldsymbol{w}_\alpha$ soit sont de taille inférieure à $4j - 2$, soit contiennent une des lettres de l'étape précédente. On peut alors conclure en utilisant la preuve précédente sur $\boldsymbol{w}_\alpha$ (7 des $31 - 7 = 24$ éléments restants de S).
3. Ainsi, en appliquant cette procédure à des sous-ensembles de tailles successives $4, 8, 3$ et 2, on parvient à couvrir les 31 lettres de S, en se ramenant à chaque fois à des mots contenant des lettres où l'on sait conclure.

□

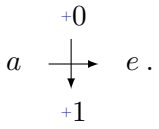
Comme on a montré que le groupe $\langle \mathcal{BBF} \rangle$ est infini, on a donc bien le théorème :

Théorème 1.2

L'automate de Mealy $\mathcal{BBF}$ engendre un groupe de Burnside infini.

1.3 Structure des fonctions de transitions, automate dual

Quand on dessine une transition de l'automate sous la forme d'une croix, on remarque une symétrie entre lettres et états :



Cela conduit à définir la notion de *dual* d'un automate de Mealy, où l'on échange les rôles des états et des lettres. Le dual du Bread-and-Butterfly $\mathfrak{d}\mathcal{BBF}$ est dessiné figure I.3.

On a vu que, pour que l'automate soit à même d'engendrer un groupe, il est nécessaire qu'il soit inversible, c'est-à-dire que les fonctions de productions ρ_q soient toutes des permutations

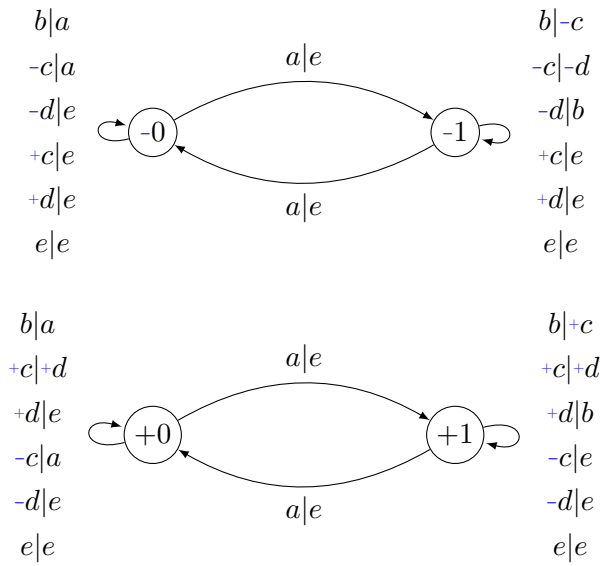


FIGURE I.3 – Le dual de l'automate Bread-and-Butterfly.

de l'alphabet. On peut aussi se demander ce qui se passe quand les fonctions de transitions de l'automate sont des permutations de l'ensemble des états, *i.e.* quand son dual est inversible. On dit alors que l'automate est *réversible*. Le Bread-and-Butterfly n'est pas réversible : par exemple la lettre $+0$ n'induit pas une permutation de Q : on a $a \mapsto e$ et $e \mapsto e$.

En considérant les automates de Mealy connus pour engendrer des groupes de Burnside infinis, on peut s'apercevoir qu'aucun de ces exemples n'est réversible. C'est d'ailleurs aussi le cas pour notre Bread-and-Butterfly.

Question

Un automate de Mealy réversible peut-il engendrer un groupe de Burnside infini ?

Klimann, Picantin et Savchuk ont apporté des réponses négatives à ce problème dans le cas d'automates ayant un petit nombre d'états dans [63] et [67]. Dans le chapitre II, on présentera des travaux effectués avec eux sur cette question, et qui y répondent négativement pour un grand nombre de situations.

Malgré leur structure plus rigide, les automates inversibles et réversibles forment une classe intéressante et étonnement difficile à étudier. De fait, la plupart des résultats algorithmiques connus nécessitent que l'automate ne soit pas réversible.

De manière plus globale, il est intéressant de se demander :

Dans quelle mesure la structure de l'automate de Mealy influe sur les propriétés du (semi-)groupe qu'il engendre ?

Cette question a été considérée, entre autres, par I. Bondarenko, V. Bondarenko, Sidki et Zapata dans [19] ; ainsi que par Antonenko et Russiev dans deux papiers indépendants mais thématiquement proches [3, 86] qui ont été complétés par Klimann et Picantin dans [66]. Tous ces travaux définissent des classes d'automates de Mealy, puis étudient les (semi-)groupes engendrés et leurs propriétés. Cette approche est riche et il reste de nombreuses classes intéressantes et peu explorées à étudier, telle que la classe des automates biréversibles.

1.4 Action sur les mots et points singuliers

Une donnée fondamentale d'un groupe d'automate est son action sur les mots de Σ^*. De fait, cette action définit le groupe, mais on peut aussi l'étudier comme objet propre. Pour cela, la vision de Σ^* comme un arbre est particulièrement appropriée : Σ^* est identifiable à un arbre d'arité $|\Sigma|$, enraciné en le mot vide et dont les enfants de chaque sommet sont étiquetés par Σ. Dans le cas du Bread-and-Butterfly, l'action est sur l'arbre quaternaire, et on la définit de la même manière que sur les mots. On donne figure I.4 un exemple d'action sur l'arbre binaire pour l'automate de Grigorchuk.

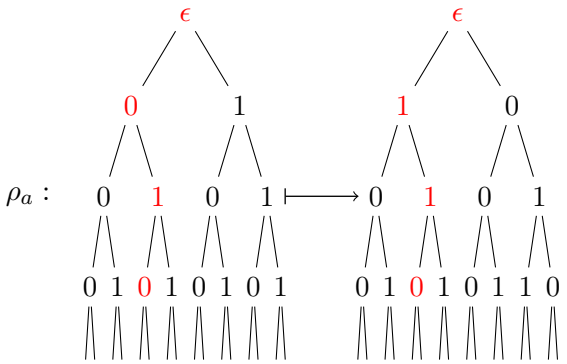


FIGURE I.4 – Action de l'état a de l'automate de Grigorchuk sur l'arbre binaire.

Un des avantages de cette vision de l'ensemble des mots comme un arbre est que l'on peut naturellement définir une topologie (deux mots sont proches s'ils ont un grand préfixe commun dans l'arbre) et une mesure (par exemple la mesure de Bernoulli uniforme, où chaque sous-arbre maximal ayant un préfixe de longueur ℓ est de mesure $(1/|\Sigma|)^\ell$).

Quand on regarde l'action du groupe sur cet arbre, on peut par exemple se demander si l'action du groupe est *transitive par niveau*, à savoir si chaque élément d'un niveau de l'arbre

peut être envoyé sur n'importe quel autre élément du même niveau de l'arbre. C'est le cas par exemple pour le groupe de Grigorchuk, et l'on remarque que ça ne peut pas être le cas pour un groupe fini. Pour le Bread-and-Butterfly, l'action ne peut pas être transitive par niveau, car une lettre n'est jamais envoyée sur une lettre d'un signe contraire. Ce problème a été étudié d'un point de vue algorithmique par Steinberg [96].

À l'opposé, des branches $\boldsymbol{\xi} \in \Sigma^\omega$ (on se place sur la frontière Σ^ω de l'arbre pour des raisons topologiques) peuvent avoir un comportement spécial vis-à-vis de certains éléments du groupe car elles sont laissées invariantes par ces éléments. On notera $\mathrm{St}_{\langle \mathcal{BBF} \rangle}(\boldsymbol{\xi}) = \{g \in \langle \mathcal{BBF} \rangle, g.\boldsymbol{\xi} = \boldsymbol{\xi}\}$ ce sous-groupe des *stabilisateurs* de $\boldsymbol{\xi}$. Par exemple, pour l'automate star de cette section, le mot -1^ω est stabilisé par l'élément du groupe $\langle \mathcal{BBF} \rangle$ induit par b. Plus intéressant encore, pour tout voisinage de -1^ω, il existe un mot dans ce voisinage (aussi proche que l'on veut donc), qui n'est pas stabilisé par l'action induite par b : on dit que -1^ω est *singulier*, car c'est un point de discontinuité de la fonction qui, à un mot infini, associe son stabilisateur dans $\langle \mathcal{BBF} \rangle$. Cette notion de point singulier sera étudiée dans le chapitre III.

1.5 Croissance du groupe

Quand on a fait la démonstration que le groupe du Bread-and-Butterfly est de Burnside infini, on a beaucoup utilisé la longueur de la représentation, dans l'automate, d'un élément du groupe. La question *"combien d'éléments peut-on représenter avec des mots de longueur au plus ℓ ?"* vient alors à l'esprit [73]. Si l'on se pose cette question pour le groupe des entiers, avec comme générateurs 1 et -1, alors on crée à chaque pas deux nouveaux éléments, la croissance est donc linéaire. Dans le cas du plan discret cette croissance est quadratique, et si l'on regarde le groupe libre, alors cette croissance est exponentielle. L'une des grandes réussites des groupes d'automate a été, en 1984 avec l'article de Grigorchuk [49], de montrer qu'il existait des groupes qui croissent plus vite que tout polynôme mais moins vite que toute exponentielle. On parle alors de croissance intermédiaire, et Grigorchuk a ainsi résolu un problème ouvert vingt ans plus tôt par Milnor [76].

Dans le groupe Bread-and-Butterfly, on retrouve par construction le groupe de Grigorchuk comme quotient. On en déduit un résultat sur la croissance de $\langle \mathcal{BBF} \rangle$, puisqu'il contient un quotient à croissance super polynomiale :

Corollaire 1.3

Le groupe $\langle \mathcal{BBF} \rangle$ est à croissance super-polynomiale.

On a vu que la croissance du groupe était au moins aussi rapide que celle du groupe de Grigorchuk. On peut donc se demander si ce groupe est à croissance intermédiaire ou bien exponentielle. Le second cas répondrait à une question de D'Angeli, Grigorchuk et Rodaro en donnant le premier exemple d'un groupe d'automate à la fois de Burnside infini et à croissance exponentielle. Les premières valeurs de la fonction de croissance tendent à suggérer une croissance exponentielle, mais il convient de rester prudent et de tester les approches utilisées pour montrer que le groupe de Grigorchuk est à croissance sous-exponentielle.

gap

```
gap> WordGrowth(GBBF,15);
- [ 1, 6, 20, 60, 179, 496, 1317, 3474, 9049, 23152, 58157, 143669,
351066, 851482, 2050315, 4899173 ]
```

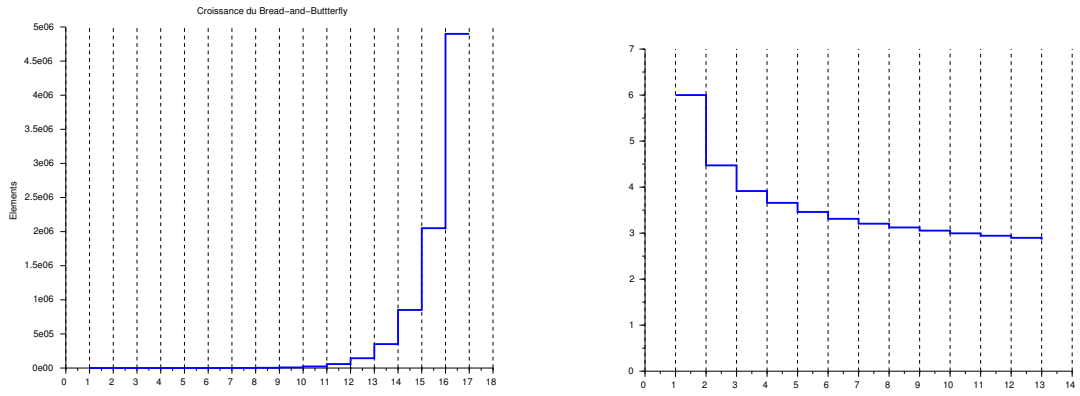


FIGURE I.5 – Croissance $\gamma(\ell)$ du groupe engendré par le Bread-and-Butterfly (à gauche), et fonction $\ell \mapsto \sqrt[\ell]{\gamma(\ell)}$ (à droite)

.

Dans l'avenir, on va essayer d'appliquer des constructions de type Bread-and-Butterfly (qui restent à définir plus formellement) à d'autres groupes de Burnside (comme les groupes de Gupta-Sidki [57]) ou à des groupes à croissance intermédiaire (par exemple les groupes de Fabrykowski-Gupta [36]), et essayer de comprendre quels traits d'un automate sont conservés par quelles caractéristiques de la construction.

1.6 Génération aléatoire

L'automate $\mathcal{BBF}$ a été construit en effectuant diverses opérations et essais. De nombreux "petits" automates engendrent des (semi-)groupes intéressants (par exemple, l'automate de Grigorchuk est formé de seulement 5 états et 2 lettres). On peut donc essayer de décrire, dans un premier temps, tous les groupes engendrés par des automates de Mealy de petite taille. Ce travail a été effectué pour les automates à 3 états et 2 lettres dans [22] et, partiellement, pour les automates à 4 états et 2 lettres dans [27].

On peut aussi penser à utiliser la diversité de ces groupes engendrés par des automates de Mealy pour générer des groupes de manière aléatoire. En effet on peut, par cette approche, espérer découvrir des groupes ayant des propriétés intéressantes. De plus, si l'on se restreint à l'étude des groupes finis, il n'existe pas réellement de méthode efficace pour générer aléatoirement des groupes finis variés. Dans le chapitre IV, on s'attaque à cette question, mais de manière générale on peut se demander quels groupes sont engendrés par un automate de Mealy tiré aléatoirement. Cette question en soulève une autre : comment générer aléatoirement uniformément des automates de Mealy ? Pour certaines classes (inversible, réversible, inversible-réversible, quelconque), la réponse est directe, mais elle peut s'avérer technique dans d'autres. Par exemple, de Felice et Nicaud ont montré [30] comment générer uniformément des automates dans la classe étudiée par Antonenko et Russiev, mais l'on ne sait pas actuellement générer efficacement des automates biréversibles.

2 Théorie des groupes et automates de Mealy

Définissons maintenant plus formellement ce que l'on a vu dans la section précédente. On commence par décrire les objets principaux de cette thèse, les *automates de Mealy* et les (semi-)groupes qu'ils engendrent.

2.1 Automates de Mealy, groupes d'automate

En informatique théorique, un automate (fini) (encore appelé système de transition d'états fini) est un triplet (Q, Σ, λ), où

— Q est un ensemble fini, l'ensemble des *états*,

— Σ est un ensemble fini, l'*alphabet* (ensemble des *lettres*),

— λ est un sous-ensemble de $Q \times \Sigma \times Q$, l'ensemble des *transitions*.

On peut voir un automate comme l'abstraction d'une procédure, d'un algorithme : une machine possède un ensemble de configurations possibles (représentées par les états de l'automate) et les actions (les lettres) induisent un changement d'état. On définit généralement en plus un

ou plusieurs états initiaux et des états finaux, en vue d'accepter ou de refuser des mots.

On peut restreindre les transitions de l'automate, de manière à ce qu'il y ait au plus une transition pour un couple état-lettre donné $((p,x,q),(p,x,q') \in \lambda \Rightarrow q = q')$. On dit alors que l'automate est *déterministe*.
On peut aussi imposer que les transitions soient définies pour chaque couple état-lettre $(\forall p \in Q, \forall x \in \Sigma, \exists q \in Q, (p,x,q) \in \lambda)$. On dit que l'automate est *complet*. Si l'automate est déterministe et complet, alors on peut redéfinir les transitions comme un ensemble de $|\Sigma|$ fonctions de Q dans Q, une fonction étant associée à une lettre de l'automate.

En parallèle, on peut généraliser le modèle des automates finis en ajoutant une sortie aux transitions, c'est-à-dire en définissant maintenant λ comme un sous-ensemble de $Q \times \Sigma \times Q \times \Sigma$, avec l'idée que, si $(p,x,q,y) \in \lambda$, alors en lisant $(p,x) \in Q \times \Sigma$, on va dans l'état q et on produit la lettre y (de manière encore plus générale on aurait pu prendre un autre alphabet pour la sortie, mais on n'utilisera pas ce modèle dans cette thèse). On obtient alors un *transducteur* (lettre-à-lettre, car on a choisi de prendre les sorties dans Σ et non dans Σ^*).

En combinant ces deux approches on obtient un transducteur lettre-à-lettre complet et déterministe. Cette classe a été étudiée par Mealy dans [75] pour synthétiser des circuits combinatoires, et on parle donc d'*automates de Mealy*. Dans ce cas-là, si on fixe une lettre x, $\lambda(\cdot,x) = \delta_x : Q \to Q$ est une fonction, de même que $\lambda(p,\cdot) = \rho_p : \Sigma \to \Sigma$ si on fixe un état p, et ces deux fonctions suffisent à définir l'ensemble des transitions. On va donc définir formellement les automates de Mealy comme un quadruplet (Q,Σ,δ,ρ).

Définition 2.1

Un *automate de Mealy* est un quadruplet (Q,Σ,δ,ρ) avec :
- Q un ensemble fini, l'ensemble des *états*,
- Σ un ensemble fini, l'*alphabet* (ensemble des *lettres*),
- $\delta = \{\delta_x\}_{x\in\Sigma}$ un ensemble de fonctions de Q dans Q, les fonctions de *transition*,
- $\rho = \{\rho_q\}_{q\in Q}$ un ensemble de fonctions de Σ dans Σ, les fonctions de *production*.

Des exemples d'automates de Mealy sont dessinés figures I.6 et I.7.

Si les fonctions $\rho_q, q \in Q$ sont définies sur l'alphabet Σ, on peut étendre l'*action de l'automate* aux mots par la définition récursive :

$$\forall i \in \Sigma,\ \forall \boldsymbol{s} \in \Sigma^*, \qquad \rho_q(i\boldsymbol{s}) = \rho_q(i)\rho_{\delta_i(q)}(\boldsymbol{s})\,. \tag{I.1}$$

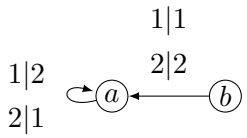


FIGURE I.6 – Un automate de Mealy inversible mais pas réversible, engendrant $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

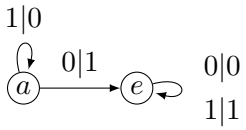


FIGURE I.7 – La machine à additionner, engendrant le groupe $\mathbb{Z}$.

De même, ρ s'étend aux mots d'états $\boldsymbol{u} \in Q^*$ par composition des fonctions associées aux lettres de $\boldsymbol{u}$:

$$\forall q \in Q,\ \forall \boldsymbol{u} \in Q^*, \qquad \rho_{q\boldsymbol{u}} = \rho_{\boldsymbol{u}} \circ \rho_q\ . \tag{I.2}$$

On obtient alors naturellement une structure de *semi-groupe* pour l'ensemble des fonctions $\rho_{\boldsymbol{u}} : \Sigma^* \to \Sigma^*$ avec $\boldsymbol{u} \in Q^*$.

Définition 2.2 (Semi-groupe d'automate)

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy. On appelle *semi-groupe engendré par* $\mathcal{A}$ et l'on note $\langle \mathcal{A} \rangle_+$ le semi-groupe

$$\langle \rho_q, q \in Q \rangle_+ = (\{\rho_{\boldsymbol{u}} : \Sigma^* \to \Sigma^*; \boldsymbol{u} \in Q^*\}, \circ)$$

De plus, si pour chaque $q \in Q$ la fonction $\rho_q : \Sigma \to \Sigma$ est une permutation de Σ alors les fonctions $\rho_{\boldsymbol{u}} : \Sigma^* \to \Sigma^*$, $\boldsymbol{u} \in Q^*$, sont bijectives. On peut alors définir les fonctions associées à Q^{-1} l'ensemble des inverses formels des fonctions ρ_q et donc le *groupe engendré par l'automate*.

On définit les fonctions $\rho_{q^{-1}} : \Sigma^* \to \Sigma^*$ par $\rho_q \circ \rho_{q^{-1}} = \rho_{q^{-1}} \circ \rho_q = \mathbb{1},$ pour tout $q \in Q$.

Définition 2.3 (Groupe d'automate)

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy dont toutes les fonctions de production $\rho_q : \Sigma \to \Sigma$ sont des permutations de l'alphabet. On appelle *groupe engendré par* $\mathcal{A}$ et l'on note $\langle \mathcal{A} \rangle$ le groupe

$$\langle \rho_q, q \in Q \sqcup Q^{-1} \rangle_+ = \left(\{ \rho_{\boldsymbol{u}} : \Sigma^* \to \Sigma^* ; \boldsymbol{u} \in \left(Q \sqcup Q^{-1} \right)^* \}, \circ \right) = \langle \rho_q, q \in Q \rangle$$

De la même manière que pour ρ, l'action de δ s'étend aux mots :

$$\forall p \in Q,\ \forall \boldsymbol{u} \in Q^*, \qquad \delta_x(p\boldsymbol{u}) = \delta_x(p)\delta_{\rho_p(x)}(\boldsymbol{u})\ . \tag{I.3}$$

et

$$\forall x \in \Sigma,\ \forall \boldsymbol{s} \in \Sigma^*, \qquad \delta_{x\boldsymbol{s}} = \delta_{\boldsymbol{s}} \circ \delta_s\ . \tag{I.4}$$

Exemple 2.4

Le groupe engendré par l'automate dessiné figure I.6 est le *Klein Vierergruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Le groupe engendré par la machine à additionner dessinée figure I.7 est $\mathbb{Z}$.

Il faut bien noter la différence entre ces *(semi-)groupes d'automate* (où automate est en fait une abréviation d'automate de Mealy), constitués de fonctions sur les mots de l'alphabet ; les *monoïdes syntaxiques* d'automates (au sens classique du terme automate) ; et les *(semi-)groupes automatiques*, où l'on peut décider si deux mots représentent le même élément modulo la multiplication par un générateur à l'aide d'un automate.
Il existe cependant des liens entre ces notions, notamment entre semi-groupes d'automate et groupes automatiques, qui sont décrits dans le papier de Picantin [84]. Le monoïde syntaxique peut quant à lui être vu comme un quotient du groupe engendré par l'automate dual.

Descriptions équivalentes

Il est souvent agréable d'avoir une description plus graphique de l'action de l'automate. À ce titre, les *diagrammes en croix* ont été introduits dans [1]. On les trouve aussi, mais dans un contexte différent, dans le travail de Glasner et Mozes [42].

Pour chaque transition de l'automate $q \xrightarrow{x|\rho_q(x)} \delta_x(q)$, on associe la *transition en croix* comme suit :

$$\begin{array}{ccc} & x & \\ q & \longrightarrow & \delta_x(q)\,. \\ & \downarrow & \\ & \rho_q(x) & \end{array}$$

Clairement, ces transitions décrivent complètement l'automate, on peut en voir un exemple figure I.8.

L'intérêt de ces transitions en croix est que, en les "collant" côte à côte, on décrit l'action de l'automate :

$$\rho_q(x_1x_2\cdots x_n) = \rho_q(x_1)\,\rho_{\delta_{x_1}(q)}(x_2\cdots x_n)$$

peut aussi être décrit par le diagramme en croix

$$\begin{array}{ccccc} & x_1 & & x_2\cdots x_n & \\ p & \longrightarrow & \delta_{x_1}(p) & \longrightarrow & \\ & \downarrow & & \downarrow & \\ & \rho_p(x_1) & & \rho_{\delta_{x_1}(p)}(x_2\cdots x_n) & \end{array}\quad .$$

et de la même façon la composition peut se construire en "collant" horizontalement ces diagrammes :

peut aussi être décrit par le diagramme en croix :

$$\begin{array}{ccccc} & x_1 & & x_2 & \\ p & \longrightarrow & \delta_{x_1}(p) & \longrightarrow & \\ & \downarrow & & \downarrow & \\ & \rho_p(x_1) & & \rho_{\delta_{x_1}(p)}(x_2) & \\ q & \longrightarrow & \delta_{\rho_p(x_1)}(q) & \longrightarrow & \\ & \downarrow & & \downarrow & \\ & \rho_q(\rho_p(x_1)) & & \rho_{\delta_{\rho_p(x_1)}(q)}(\rho_{\delta_{x_1}(p)}(x_2)) & \end{array}\quad .$$

Dans un esprit semblable, dans [1] a été introduit la notion de *graphe en hélice* d'un automate. Le graphe en hélice d'ordre (n,k) d'un automate de Mealy $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ est le graphe $\mathcal{H}_{n,k}(\mathcal{A})$ orienté dont les sommets sont les éléments de $Q^n \times \Sigma^k$ et les arêtes sont données par

$$(\boldsymbol{u}, \boldsymbol{s}) \longrightarrow (\delta_{\boldsymbol{s}}(\boldsymbol{u}), \rho_{\boldsymbol{u}}(\boldsymbol{s}))\ ,$$

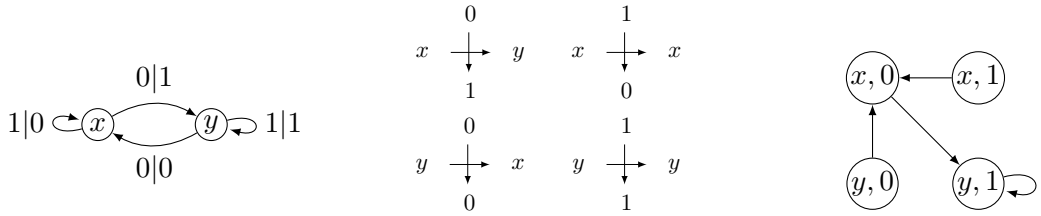


FIGURE I.8 – L'automate de Mealy $\mathcal{L}$ engendrant le groupe de l'allumeur de réverbères, son ensemble de transitions en croix, et son graphe en hélice $\mathcal{H}_{1,1}(\mathcal{L})$.

pour tous les $(\boldsymbol{u}, \boldsymbol{s}) \in Q^n \times \Sigma^k$ (voir l'exemple figure I.8).
Là aussi, le graphe en hélice d'ordre $(1, 1)$ décrit entièrement l'automate.

Notons également que nos (semi-)groupes agissent naturellement sur les mots de Σ^*, c'est-à-dire que chaque élément du (semi-)groupe induit une transformation de l'ensemble des mots dans lui même. Quand on parle d'un groupe abstrait G agissant sur un ensemble X, ce qu'on note $G \curvearrowright X$, on a

$$g.x \in X$$

la transformation de $x \in X$ induite par $g \in G$.

On peut décrire les (semi-)groupes d'automate de manière plus abstraite, par les *récursions en couronne* (en anglais *wreath recursion*). La récursion couronne correspond, intuitivement à la conjonction de deux notions de théorie des (semi-)groupes, le *produit couronne* et l'*action auto-similaire*.
Le produit en couronne $G \wr H$ d'un groupe G par un groupe de permutations fini $H \leq S_k$ est défini par $(g_1, \ldots, g_k)h \in G^k \times H$ avec comme loi de multiplication $(g_1, \ldots, g_k)h \circ (g'_1, \ldots, g'_k)h' = (g_1 g'_{h^{-1}(1)}, \ldots, g_k g'_{h^{-1}(k)})hh'$.
D'autre part, on dit que l'action d'un groupe G agissant sur un ensemble X est *auto-similaire* si

$$\forall g \in G, \forall \boldsymbol{u} \in X^*, \forall x \in X, \exists h \in G, \exists y \in X, g.x\boldsymbol{u} = yh.\boldsymbol{u}$$

On peut dans ce cadre décrire chaque élément de par une relation de récurrence (en posant $X = \{x_1, x_2, \ldots, x_k\}$) :

$$g = \left(g_{|x_1}, \ldots, g_{|x_k}\right) \pi(g)$$

On appelle $g_{|x_1}$ la *section de l'automorphisme g en x_1* et $\pi(g)$ la *permutation associée à g*. Comme pour l'action d'un automate, on peut étendre la section aux mots : $\forall \boldsymbol{u}x \in X^+, g_{|\boldsymbol{u}x} = g_{|\boldsymbol{u}|x}$.
Si tout élément g du groupe G est tel que l'ensemble $\{g_{|\boldsymbol{u}}, \boldsymbol{u} \in X^*\}$ est fini, on dit que l'action

auto-similaire est *à états finis*. On montre qu'un groupe finiment engendré admet une action auto-similaire à état fini si et seulement s'il est engendré par un automate. On a en effet la traduction :

$$q \xrightarrow{x|y} p \ \in \mathcal{A} \quad \Longleftrightarrow \quad q_{|x} = p \text{ et } \pi(q)(x) = y \, .$$

La récursion couronne consiste alors à décrire le groupe G agissant sur les mots de l'alphabet à k lettre en donnant la décomposition de l'action des générateurs dans $G \wr S_k$ (*resp.* $G \wr \mathcal{T}_k$, où $\mathcal{T}_k$ est le semi-groupe des transformation d'un ensemble à k éléments), et en prenant comme multiplication de groupe la multiplication du produit couronne.

Exemple 2.5

Le groupe $\mathbb{Z}$ engendré par la machine à additionner dessinée figure I.7 est décrit par les récursions :

$$a = (e, a)(0, 1) \quad ; \quad e = (e, e)() \, ,$$

et on a

$$a^2 = (e, a)(1, 2)(e, a)(1, 2) = (ea, ae)(1, 2)^2 = (a, a)() \, .$$

D'autre part, si on a un automate $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ définissant un groupe $\langle \mathcal{A} \rangle$, alors l'action de $\langle \mathcal{A} \rangle$ sur Σ^* peut aussi être vue comme une action sur un arbre régulier enraciné T d'arité $|\Sigma|$. En fait, Σ^* est isomorphe à T, l'arbre k-aire enraciné en le mot vide ϵ et dont le i-ème enfant de chaque sommet est la i-ème lettre de Σ. L'action de $\langle \mathcal{A} \rangle$ peut donc s'exprimer comme une action sur T. En particulier, l'action d'un élément de $\langle \mathcal{A} \rangle$ est entièrement déterminée par la permutation induite par cet élément sur chaque sommet de T, c'est la notion de *portrait* d'un élément [78], utilisée notamment pour étudier le problème de finitude par Klimann dans [63].

Ces différents points de vue dans l'étude des groupes d'automate permettent une vision riche de ces objets, en plus de suggérer qu'ils sont assez naturels. En effet, on peut utiliser simultanément plusieurs théories mathématiques et informatiques. Un bon exemple de cela est l'étude des points singuliers de l'action (chapitre III) où l'on étudiera un problème plutôt issu de la vision "action sur un arbre" mais où l'utilisation des automates et de leurs propriétés permet d'obtenir des résultats intéressants.
De manière générale, on adoptera dans cette thèse la vision "automate", ce qui ne nous empêchera pas de parfois passer à un autre point de vue, ou d'utiliser des résultats que l'on traduira en terme d'automates.

2.2 Propriétés structurelles des automates de Mealy et des (semi-)groupes d'automate

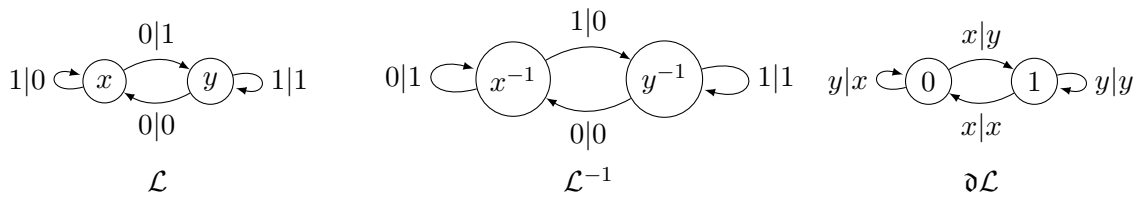
Dans un automate de Mealy, lettres et états jouent des rôles symétriques, comme on l'a remarqué dans la section précédente. On peut donc assez naturellement définir l'automate où l'on inverse ces rôles :

Définition 2.6 (Dual d'un automate)

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy. Le *dual* de $\mathcal{A}$ est l'automate $\mathfrak{d}\mathcal{A} = (\Sigma, Q, \rho, \delta)$, c'est-à-dire l'automate dont les transitions sont données par :

$$x \xrightarrow{p|q} y \ \in \mathfrak{d}\mathcal{A} \quad \Longleftrightarrow \quad p \xrightarrow{x|y} q \ \in \mathcal{A}\,.$$

Le dual d'un automate de Mealy est toujours un automate de Mealy.



$\mathcal{L}$ $\quad$ $\mathcal{L}^{-1}$ $\quad$ $\mathfrak{d}\mathcal{L}$

FIGURE I.9 – L'automate $\mathcal{L}$ de l'allumeur de réverbères, son inverse $\mathcal{L}^{-1}$, et son dual $\mathfrak{d}\mathcal{L}$.

Si les (semi-)groupes engendrés par un automate et son dual ne sont pas directement liés, on a toutefois l'importante contrainte :

Théorème 2.7 ([78, 1])

Un automate de Mealy engendre un groupe fini si et seulement si son dual engendre un groupe fini.

On donnera une démonstration élémentaire de ce théorème dans la sous-section 2.3.

Les deux (semi-)groupes peuvent tout de même être relativement indépendants. De fait, on peut même prouver qu'on peut avoir n'importe quelle paire de (semi-)groupes finis engendrée par un automate et son dual.

Proposition 2.8 ([1])

Soient G et H deux semi-groupes finis. Il existe un automate de Mealy $\mathcal{A}$ qui engendre G et dont le dual engendre H.

Là aussi, les outils mis en place dans la sous-section 2.3 nous permettront de donner une démonstration simple de ce résultat.

Dans la partie précédente, on a vu que l'on peut définir un groupe à partir d'un automate dès lors que chaque état induit une permutation sur les lettres car, en particulier, on peut définir l'*inverse* de chaque état de l'automate. On peut alors définir l'inverse de l'automate.

Définition 2.9 (Inverse d'un automate)

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy, tel que toutes les fonctions $\rho_q : \Sigma \to \Sigma$, $q \in Q$ sont des permutations. L'*inverse* de $\mathcal{A}$ est l'automate $\mathcal{A}^{-1} = \left(Q^{-1}, \Sigma, \delta', \rho'\right)$, où les transitions sont données par :

$$p^{-1} \xrightarrow{y|x} q^{-1} \in \mathcal{A}^{-1} \quad \Longleftrightarrow \quad p \xrightarrow{x|y} q \ \in \mathcal{A}\,.$$

On a alors $\rho_q \circ \rho'_{q^{-1}} = \mathbb{1}$.

On remarque que, par définition du groupe engendré par un automate, on a $\langle \mathcal{A} \rangle = \langle \mathcal{A}^{-1} \rangle = \langle \mathcal{A} \sqcup \mathcal{A}^{-1} \rangle$ dès lors que $\mathcal{A}^{-1}$ est bien défini.

Cette propriété structurelle qui permet de définir l'inverse est facile à vérifier sur l'automate. De même, on peut demander aux fonctions de transition d'être des permutations de l'ensemble des états, voire que les sorties induisent des permutations des états : on introduit à cet effet et pour toute lettre $x \in \Sigma$ la fonction $\hat{\delta} : Q \to Q$ qui correspond à la transition induite par la lettre de sortie d'une arête.

Définition 2.10 (Automate inversible, réversible, biréversible)

Un automate $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ est dit :

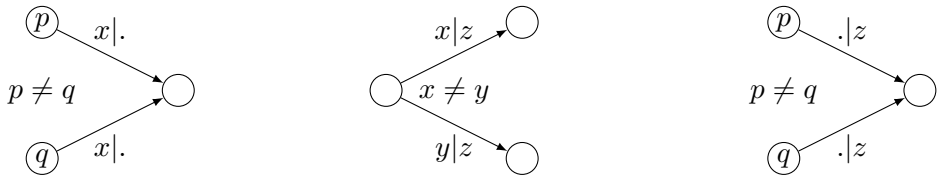
— *inversible* si ρ_q est une permutation de Σ, pour tout $q \in Q$,

— *réversible* si δ_x est une permutation de Q, pour tout $x \in \Sigma$,

— *coréversible* si la fonction associée $\hat{\delta}_z$ à la lettre de sortie z est une permutation de Q, pour tout $z \in \Sigma$,

— *biréversible* s'il est simultanément : inversible, réversible et coréversible.

Toutes ces propriétés peuvent aisément être lues, par configurations interdites, sur la représentation graphique de l'automate, comme illustré en figure I.10.



(A) (B) (C)

FIGURE I.10 – La configuration (A) est proscrite pour les automates réversibles, la configuration (B) l'est pour les inversibles, et la configuration (C) pour les coréversibles.

Par définition $\mathcal{A}$ est inversible si et seulement si $\mathfrak{d}\mathcal{A}$ est réversible. De même $\mathcal{A}$ est inversible et coréversible si et seulement si $\mathcal{A}^{-1}$ est inversible et réversible.

Un des intérêts des automates biréversibles vient de la possibilité d'effectuer toute combinaison de dualisations et d'inversions possibles :

Lemme 2.11

Soit $\mathcal{A}$ un automate de Mealy. On a

$$\mathcal{A} \text{ est biréversible} \iff \text{les éléments de } \left\{\mathcal{A}, \mathcal{A}^{-1}, \mathfrak{d}\mathcal{A}, \mathfrak{d}\mathcal{A}^{-1}, (\mathfrak{d}\mathcal{A})^{-1}, \left(\mathfrak{d}\mathcal{A}^{-1}\right)^{-1}, \mathfrak{d}\left(\mathfrak{d}\mathcal{A}\right)^{-1}\right\} \text{ sont tous des automates de Mealy.}$$

Il existe des automates inversibles et réversibles mais qui ne sont pas biréversibles (par exemple l'automate dessiné figure I.11). Cependant, on peut alléger un peu les hypothèses :

Lemme 2.12

Un automate de Mealy réversible et coréversible est biréversible.

Démonstration. Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate réversible et coréversible. Montrons que $\mathcal{A}$ est également inversible. Soit $p \in Q$ un état de $\mathcal{A}$, montrons que ρ_p est une permutation de Σ. Supposons par l'absurde que $\rho_p(x) = \rho_p(y) = z$ avec $x \neq y$. Comme l'automate est coréversible on a $\delta_x(p) = \delta_y(p) = q$ (car $\hat{\delta_z}$ est une permutation). Mais alors, comme il y a deux z arrivant sur q par deux lettres différentes, il est nécessaire qu'au moins $|\Sigma| - 1$ arêtes (comptées avec multiplicité) mènent à q pour assurer la complétude de l'automate en sortie. Donc au moins deux lettres en entrée mènent à q, ce qui contredit l'hypothèse de réversibilité, donc $\mathcal{A}$ doit être inversible. □

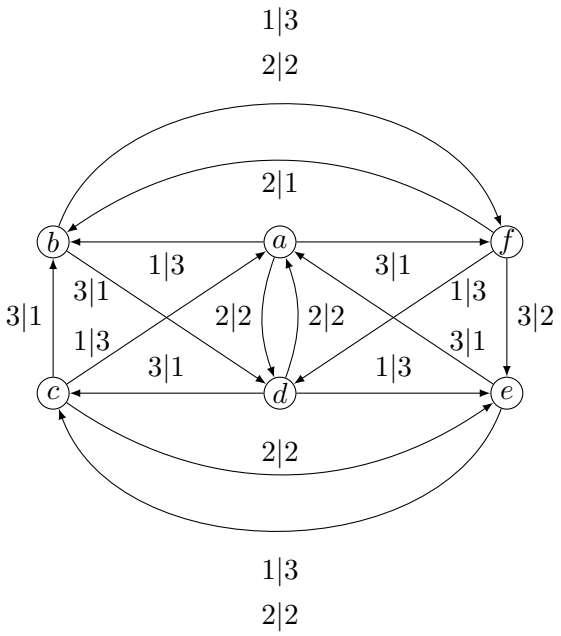


FIGURE I.11 – Un automate à 3 lettres 6 états inversible réversible non-biréversible.

Une autre donnée structurelle que l'on peut étudier est la structure en cycle de l'automate. Comme l'automate est complet, il est certain qu'il contient des cycles. On peut contraindre leur structure.

Antonenko [3] et Russyev [86] ont indépendamment étudié les *automates de Mealy avec cycles sans échappatoire*, c'est-à-dire les automates tels que, si $\boldsymbol{u} = u_0 \cdots u_{\ell-1} \in Q^\ell$ est un cycle dans l'automate (vu comme un multi-graphe), et que $u_i u'$ est une arête de l'automate, alors $u' = u_{i+1 \bmod \ell}$.

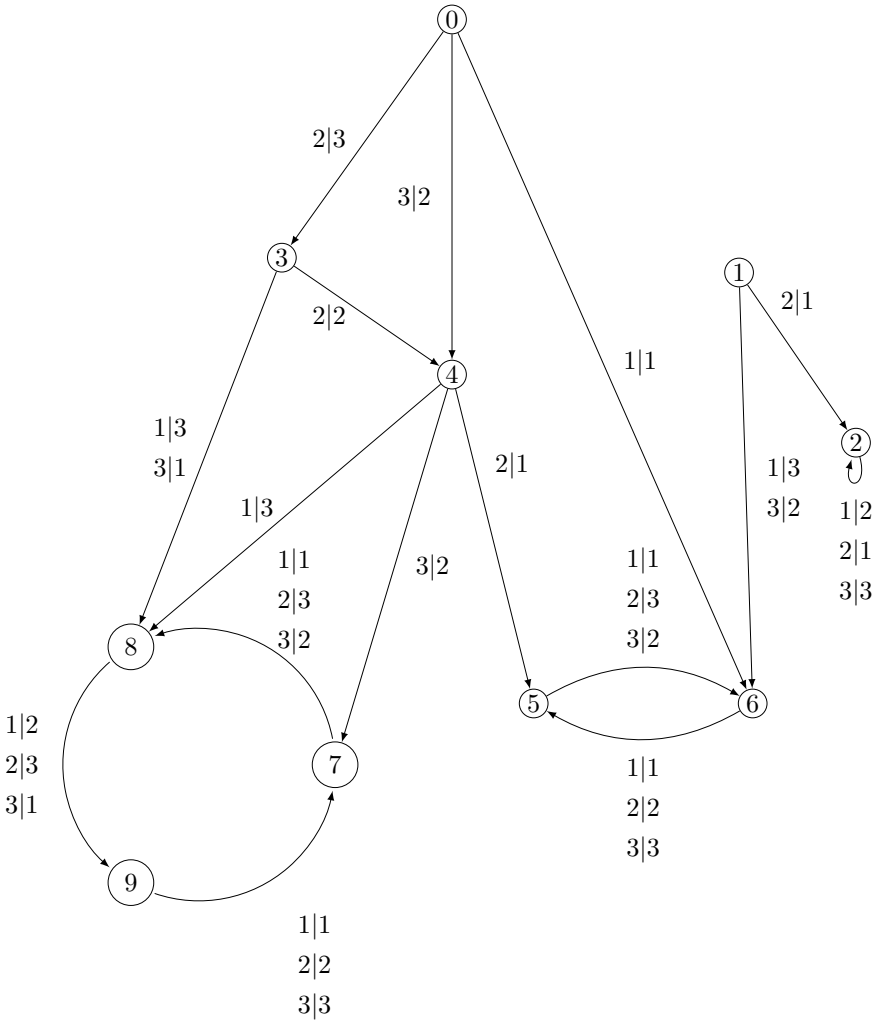


FIGURE I.12 – Un automate à cycles sans échappatoire à 10 états et 3 lettres.

D'autre part, Sidki [93], puis Bondarenko, Bondarenko, Sidki et Zapata [19] ont étudié les groupes d'*automate à activité polynomiale*. L'*activité* d'un automorphisme g agissant sur les mots de Σ^* est la suite

$$\left| \{ \boldsymbol{v} \in \Sigma^\ell, \quad g_{|\boldsymbol{v}} \text{ agit de manière non triviale sur } \Sigma \} \right| .$$

L'activité d'un groupe est toujours bornée par $e^{|\Sigma|\ell}$, mais on peut prouver plus précisément qu'elle est bornée par une fonction polynomiale ou bien minorée par une fonction exponentielle.

On note $\mathbf{Pol}(n)$ l'ensemble des automates dont l'activité de tout élément est bornée par un polynôme de degré n et on dit que le groupe est *borné* si $n = 0$, donc s'il existe une constante K telle que : $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ où

$$\forall g \in \langle \mathcal{A} \rangle \quad \left| \{ \boldsymbol{v} \in \Sigma^{\ell}, \quad g_{|\boldsymbol{v}} \text{ agit de manière non triviale sur } \Sigma \} \right| \leq K \, .$$

Il est remarquable que ces propriétés de l'action du groupe se traduisent en propriétés structurelles des automates qui les engendrent. Soit $\mathcal{A}$ un automate (minimisé) et soit n_q le nombre de cycles élémentaires (avec $\mathcal{A}$ vu comme un multi-graphe) non-triviaux (qui ne sont pas sur l'état représentant l'identité dans $\langle \mathcal{A} \rangle$) accessibles depuis un état q de $\mathcal{A}$. Alors l'automorphisme ρ_q appartient à $\mathbf{Pol}(n_q)$.

On voit que la notion d'activité d'un automorphisme est une propriété liée à l'action du groupe. Les notions suivantes sont également des propriétés classiques de l'action d'un groupe d'automate :

Un automate de Mealy $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ est dit *contractant* s'il existe un automate de Mealy $\mathcal{N} = (Q', \Sigma, \delta', \rho')$ appelé *noyau* de $\mathcal{A}$, tel que

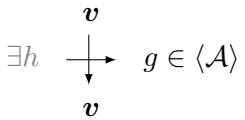
$$\forall \boldsymbol{q} \in Q^*, \forall \boldsymbol{\xi} \in \Sigma^{\omega}, \exists \ell, \delta_{\boldsymbol{\xi}[1:n]}(\boldsymbol{q}) \in \mathcal{N} \, .$$

En d'autre termes, à partir de n'importe quel élément du groupe (qui se représente donc dans une certaine puissance de l'automate, arbitrairement grande), et en agissant sur n'importe quel mot, l'action après avoir agit sur un certain préfixe fini par être équivalente à l'action d'un élément appartenant à un ensemble fini qui ne dépend ni du mot lu, ni de l'élément du groupe duquel on part. Le principe de cette propriété est illustré figure I.13 tandis qu'un non-exemple est donné figure I.14.

D'autre part, l'automate de Mealy $\mathcal{A}$ est dit *fractal* si on peut agir sur un mot en choisissant à partir de quel moment et sans changer le préfixe, c'est-à-dire si

$$\forall g \in \langle \mathcal{A} \rangle, \forall \boldsymbol{v} \in \Sigma^*, \exists h \in \langle \mathcal{A} \rangle, h_{|\boldsymbol{v}} = g \text{ et } h.\boldsymbol{v} = \boldsymbol{v} \, .$$

Cela se traduit en terme de diagramme en croix (étendu aux éléments du groupe $\mathcal{A}$) par :



De nombreux automates de Mealy connus pour engendrer des groupes intéressants sont dans une de ces classes. En particulier l'automate de Grigorchuk est à la fois contractant et

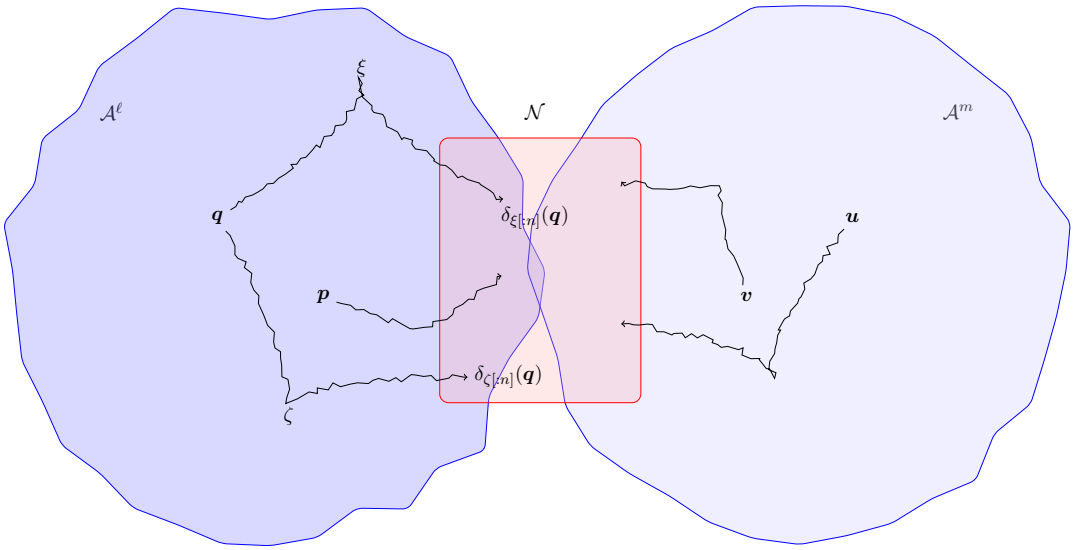


FIGURE I.13 – Principe d'un automate contractant : après avoir lu un préfixe suffisamment long, on se retrouve invariablement dans un automate fini.

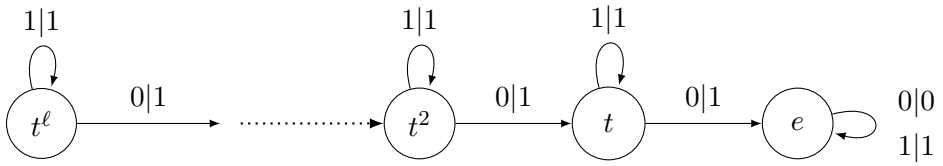


FIGURE I.14 – Un exemple d'automate non-contractant : qu'importe la puissance ℓ de l'automate choisie, $t^{2^{\ell+1}}$ n'est pas représentable dans cette puissance.

fractal, tout comme l'automate de la Basilique (figure I.16), tandis que le Bread-and-Butterfly est contractant mais pas fractal. On verra comment ces propriétés du groupe peuvent être utilisées dans le chapitre III.

2.3 Outils pour les automates de Mealy

Mettons maintenant en place quelques outils de théorie des automates et relions-les aux groupes engendrés par des automates de Mealy.
Le premier de ces outils est le *produit d'automates*, aussi appelé composition d'automates car il correspond à une composition des fonctions de production.

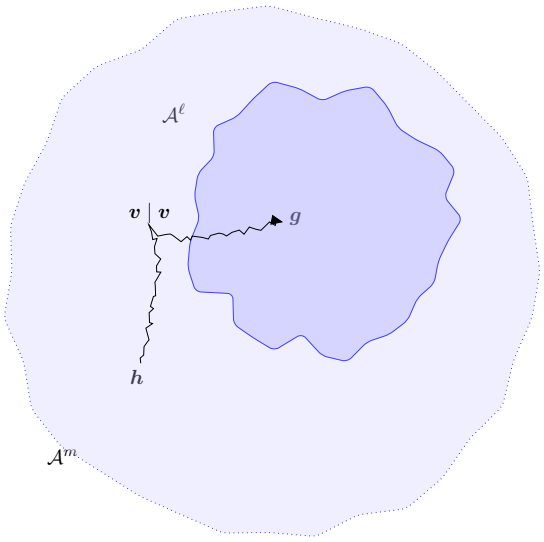


FIGURE I.15 – Principe d'un automate fractal : quitte à se placer dans une puissance supérieure, on peut arriver dans n'importe quel élément après avoir stabilisé un préfixe quelconque.

Définition 2.13 (Produit d'automates)

Soient $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ et $\mathcal{B} = (Q', \Sigma, \delta', \rho')$ deux automates de Mealy sur le même alphabet. Le *produit* de $\mathcal{A}$ par $\mathcal{B}$ est l'automate $\mathcal{A} \times \mathcal{B} = (Q \times Q', \Sigma, \gamma, \pi)$ dont les transitions

$$qq' \xrightarrow{x|\rho'_q(\rho_{q'}(x))} \delta_x(q)\delta'_{\rho_p(x)}(q') \,,$$

peuvent être vues comme le diagramme en croix :

$$\begin{array}{ccc} & x & \\ q & \longrightarrow & \delta_x(q) \\ & \downarrow & \\ \rho_q(x) & & \\ q' & \longrightarrow & \delta'_{\rho_q(x)}(q') \,, \\ & \downarrow & \\ & \rho'_{q'}(\rho_q(x)) & \end{array}$$

où $q \in Q, q' \in Q'$ et $x \in \Sigma$.

Ce produit n'est pas commutatif.

On voit que ce produit était déjà sous-entendu dans la notation $\rho_q \circ \rho_p = \rho_{pq}$. On remarque aussi que l'action de l'automate correspond à la composition horizontale de transitions en croix et que

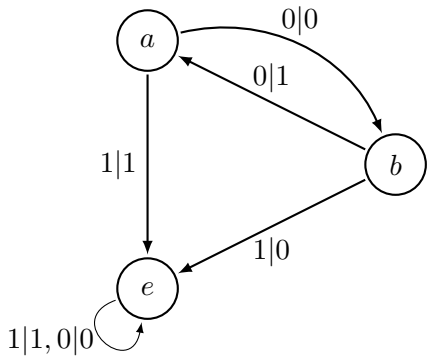


FIGURE I.16 – L'automate engendrant le groupe de la Basilique.

le produit (la composition de fonctions) correspond à la composition verticale de transitions en croix. Cette remarque sera utile dans le chapitre III.
Par ailleurs, ce produit d'automates conserve les propriétés structurelles : si $\mathcal{A}$ et $\mathcal{B}$ sont deux automates inversibles (*resp.* réversibles, coréversibles, biréversibles), alors leur produit $\mathcal{AB}$ l'est aussi.

On remarque donc que, comme un élement g de $\langle\mathcal{A}\rangle_+$ peut toujours s'écrire comme $\rho_{\boldsymbol{u}}$ avec $\boldsymbol{u} \in Q^\ell$, cet élément correspond à l'action d'un état dans l'automate puissance $\mathcal{A}^\ell$, et de même pour les éléments du groupe si on considère $\mathcal{A} \sqcup \mathcal{A}^{-1}$. De là on déduit qu'un groupe engendré par un automate est fini si et seulement si le groupe engendré par son dual l'est :

Démonstration du théorème 2.7. Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$, tel que $\langle\mathfrak{d}\mathcal{A}\rangle_+$ soit d'ordre fini. Alors les tailles les composantes connexes de $\mathcal{A}^\ell$ (qui sont elles-mêmes des automates de Mealy) sont de tailles bornées par $|\langle\mathfrak{d}\mathcal{A}\rangle_+|$, pour tout ℓ. En effet le semi-groupe engendré par l'automate dual agit sur Q^ℓ et les tailles des orbites des mots sur Q sont bornées par l'ordre $\langle\mathfrak{d}\mathcal{A}\rangle_+$. Ainsi, comme il n'existe qu'un nombre fini d'automates de Mealy de taille bornée par une constante sur l'alphabet Σ, on obtient qu'il n'existe qu'un nombre fini de $\rho_{\boldsymbol{u}}, \boldsymbol{u} \in Q^*$, et donc que le semi-groupe $\langle\mathcal{A}\rangle_+$ est fini. La réciproque s'obtient par symétrie.

□

En théorie des (semi-)groupes, il existe aussi une notion de produit, appelé produit direct de (semi-)groupes et noté $\times$. Ces deux notions de produits sont indépendantes, et on n'a pas en général égalité entre $\langle\mathcal{AB}\rangle_+$ et $\langle\mathcal{A}\rangle_+ \times \langle\mathcal{B}\rangle_+$. On a cependant $\langle\mathcal{A}^2\rangle_+ \leq \langle\mathcal{A}\rangle_+$ (avec égalité dès que $\mathcal{A}$ possède un état qui induit l'identité dans le groupe), et $\langle\mathfrak{d}(\mathfrak{d}\mathcal{A})^k\rangle_+ = \langle\mathcal{A}\rangle_+$, pour tout $k \geq 1$. Pour cette dernière égalité, notons que $\mathfrak{d}(\mathfrak{d}\mathcal{A})^k$ correspond à l'automate où l'on lit les

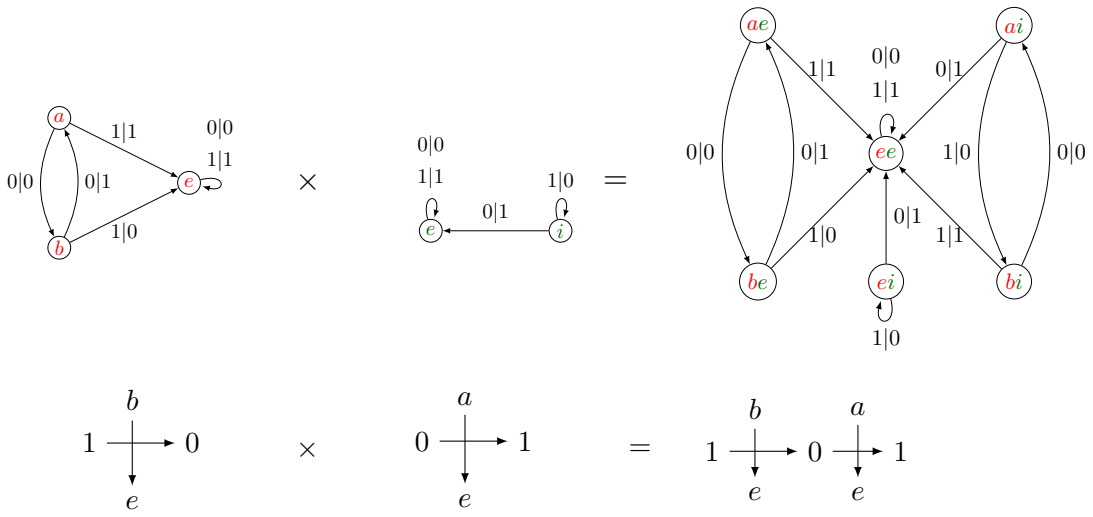


FIGURE I.17 – Produit de l'automate de la Basilique avec la machine à additionner.

lettres par tranches de longueur k.

Il est cependant possible d'exprimer en termes de produit d'automates le produit direct de (semi-)groupes. Cela a d'abord été fait par Cain [26]. Lors d'un séjour à Graz pour travailler avec Daniele D'Angeli, on a pu constater avec l'aide d'Emanuele Rodaro et d'Amnon Rosenmann qu'il était possible d'obtenir des produits directs par d'autres constructions dont deux sont présentées maintenant. Elles sont intéressantes car on voit comment l'action peut être "tordue" sans pour autant changer le (semi-)groupe engendré.

Définition 2.14

Soient $\mathcal{A}_1 = (Q_1, \Sigma_1, \delta_1, \rho_1)$ et $\mathcal{A}_2 = (Q_2, \Sigma_2, \delta_2, \rho_2)$ deux automates de Mealy. Le *produit direct bouclé* de $\mathcal{A}_1$ et $\mathcal{A}_2$ est l'automate $\mathcal{A}_1 \times_\ell \mathcal{A}_2 = (Q_1 \sqcup Q_2, \Sigma_1 \sqcup \Sigma_2, \delta, \rho)$, avec

- $\delta_{x_1}(q_1) = \delta_{1x_1}(q_1)$,
- $\delta_{x_2}(q_1) = q_1$,
- $\delta_{x_2}(q_2) = \delta_{2x_2}(q_2)$,
- $\delta_{x_1}(q_2) = q_2$,
- $\rho_{q_1}(x_1) = \rho_{1q_1}(x_1)$,
- $\rho_{q_1}(x_2) = x_2$,
- $\rho_{q_2}(x_2) = \rho_{2q_2}(x_2)$,
- $\rho_{q_2}(x_1) = x_1$

pour $x_1 \in \Sigma_1$, $x_2 \in \Sigma_2$, $q_1 \in Q_1$, $q_2 \in Q_2$.

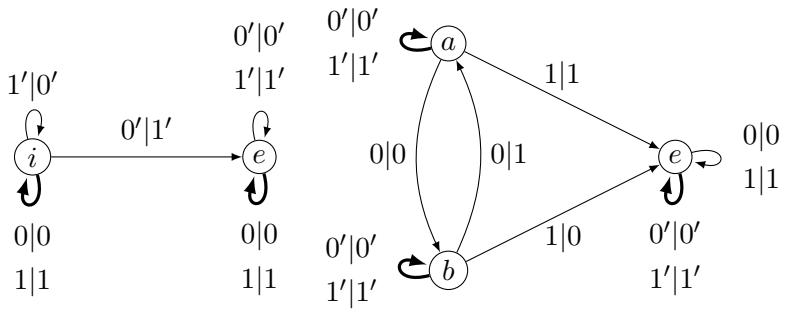


FIGURE I.18 – Produit direct bouclé de la machine à additionner et de l'automate de la Basilique. Les nouvelles transitions sont en gras.

Proposition 2.15

Soient $\mathcal{A}_1$ et $\mathcal{A}_2$ deux automates de Mealy. On a $\langle \mathcal{A}_1 \times_\ell \mathcal{A}_2 \rangle_+ = \langle \mathcal{A}_1 \rangle_+ \times \langle \mathcal{A}_2 \rangle_+$

Démonstration. Posons $\mathcal{A}_1 = (Q_1, \Sigma_1, \delta_1, \rho_1)$, $\mathcal{A}_2 = (Q_2, \Sigma_2, \delta_2, \rho_2)$ et donc $\mathcal{A}_1 \times_\ell \mathcal{A}_2 = \mathcal{A} = (Q_1 \sqcup Q_2, \Sigma_1 \sqcup \Sigma_2, \delta, \rho)$. On montre que $\rho_{\boldsymbol{u}_1}\rho_{\boldsymbol{u}_2} = \rho_{\boldsymbol{u}_2}\rho_{\boldsymbol{u}_1}$, $\forall \boldsymbol{u}_1 \in Q_1^*, \boldsymbol{u}_2 \in Q_2^*$. Soit $\boldsymbol{s}_1 \in \Sigma_1^*, \boldsymbol{s}_2 \in \Sigma_2^*$. On a les transitions en croix :

$$\begin{array}{ccccc}
 & \boldsymbol{s}_1 & & \boldsymbol{s}_2 & \\
\boldsymbol{u}_1 & \downarrow & \delta_{\boldsymbol{s}_1}(\boldsymbol{u}_1) = \delta_{1\boldsymbol{s}_1}(\boldsymbol{u}_1) & \downarrow & \delta_{1\boldsymbol{s}_1}(\boldsymbol{u}_1) \\
\rho_{\boldsymbol{u}_1}(\boldsymbol{s}_1) = \rho_{1\boldsymbol{u}_1}(\boldsymbol{s}_1) & & & \boldsymbol{s}_2 & \\
\boldsymbol{u}_2 & \downarrow & \boldsymbol{u}_2 & \downarrow & \delta_{\boldsymbol{s}_2}(\boldsymbol{u}_2) = \delta_{2\boldsymbol{s}_2}(\boldsymbol{u}_2) \\
\rho_{1\boldsymbol{u}_1}(\boldsymbol{s}_1) & & & \rho_{\boldsymbol{u}_2}(\boldsymbol{s}_2) = \rho_{2\boldsymbol{u}_2}(\boldsymbol{s}_2) &
\end{array}$$

Et inversement :

$$\begin{array}{ccccc}
 & \boldsymbol{s}_1 & & \boldsymbol{s}_2 & \\
\boldsymbol{u}_2 & \downarrow & \boldsymbol{u}_2 & \downarrow & \delta_{\boldsymbol{s}_2}(\boldsymbol{u}_2) = \delta_{2\boldsymbol{s}_2}(\boldsymbol{u}_2) \\
 & \boldsymbol{s}_1 & & \rho_{\boldsymbol{u}_2}(\boldsymbol{s}_2) = \rho_{2\boldsymbol{u}_2}(\boldsymbol{s}_2) & \\
\boldsymbol{u}_1 & \downarrow & \delta_{\boldsymbol{s}_1}(\boldsymbol{u}_1) = \delta_{1\boldsymbol{s}_1}(\boldsymbol{u}_1) & \downarrow & \delta_{1\boldsymbol{s}_1}(\boldsymbol{u}_1) \\
\rho_{\boldsymbol{u}_1}(\boldsymbol{s}_1) = \rho_{1\boldsymbol{u}_1}(\boldsymbol{s}_1) & & & \rho_{2\boldsymbol{u}_2}(\boldsymbol{s}_2) &
\end{array}$$

Donc, par récurrence, les éléments représenté par des mots sur Q_1 commutent avec les éléments représentés par des mots sur Q_2. Ainsi, tout élément représenté par un mot dans $(Q_1 \sqcup Q_2)^*$ est équivalent à un autre représenté par un mot dans $(Q_1 \times Q_2)^*$. On obtient que $\langle \mathcal{A}_1 \times_\ell \mathcal{A}_2 \rangle_+ \leq \langle \mathcal{A}_1 \rangle_+ \times \langle \mathcal{A}_2 \rangle_+$.

D'autre part tout élément (a_1, a_2) de $\langle \mathcal{A}_1 \rangle_+ \times \langle \mathcal{A}_2 \rangle_+$ est représenté par un mot dans $\langle \mathcal{A}_1 \times_\ell$

$\mathcal{A}_2\rangle_+$: par hypothèse $a_1 = \rho_{1\boldsymbol{u}_1}$ et $a_2 = \rho_{2\boldsymbol{u}_2}$, donc $(a_1, a_2) = (\rho_{1\boldsymbol{u}_1}, \rho_{2\boldsymbol{u}_2}) = \rho_{\boldsymbol{u}_1\boldsymbol{u}_2}$. On peut conclure que $\langle \mathcal{A}_1 \times_\ell \mathcal{A}_2\rangle_+ = \langle \mathcal{A}_1\rangle_+ \times \langle \mathcal{A}_2\rangle_+$. □

On remarque également que $\mathfrak{d}(\mathcal{A} \times_\ell \mathcal{B}) = \mathfrak{d}\mathcal{A} \times_\ell \mathfrak{d}\mathcal{B}$. Cela nous donne :

Démonstration de la proposition 2.8. Soient G et H deux semi-groupes finis. Par le théorème de Cayley pour les semi-groupes, on peut exprimer G (*resp.* H) comme le semi-groupe engendré par les transformations $g_1, \dots, g_i$ (*resp.* $h_1, \dots, h_j$) d'un ensemble à k_G (*resp.* k_H) éléments. Alors l'automate $\mathcal{A}$ (*resp.* $\mathcal{B}$), représenté figure I.19, ayant i (*resp.* j) états, k_G (*resp.* k_H) lettres, dont les fonctions de transition sont la fonction identité et les fonctions de production sont les g_ℓ (*resp.* les h_ℓ) satisfait $\langle \mathcal{A}\rangle_+ = G$ et $\langle \mathfrak{d}\mathcal{A}\rangle_+ = \{\mathbb{1}\}$ (*resp.* $\langle \mathcal{B}\rangle_+ = H$ et $\langle \mathfrak{d}\mathcal{B}\rangle_+ = \{\mathbb{1}\}$). D'après la proposition 2.15, on a donc

$$\langle \mathcal{A} \times_\ell \mathfrak{d}\mathcal{B}\rangle_+ = G \quad \text{et} \quad \langle \mathfrak{d}(\mathcal{A} \times_\ell \mathfrak{d}\mathcal{B})\rangle_+ = \langle \mathfrak{d}\mathcal{A} \times_\ell \mathcal{B}\rangle_+ = H\,.$$

□

FIGURE I.19 – Un automate de Mealy engendrant le semi-groupe fini $\langle g_1, \dots, g_i\rangle_+$ et dont le dual engendre le groupe trivial.

Définition 2.16

Soient $\mathcal{A}_1 = (Q_1 \sqcup \{e_1\}, \Sigma_1, \delta_1, \rho_1)$ et $\mathcal{A}_2 = (Q_2 \sqcup \{e_2\}, \Sigma_2, \delta_2, \rho_2)$ deux automates de Mealy, où e_1 et e_2 sont respectivement les (éventuels, que l'on peut supposer unique après minimisation) états-puits des automates. Le *produit direct puisé* de $\mathcal{A}_1$ et $\mathcal{A}_2$ est l'automate $\mathcal{A}_1 \times_{\mathcal{S}} \mathcal{A}_2 = (Q_1 \sqcup Q_2 \sqcup \{e\}, \Sigma_1 \sqcup \Sigma_2, \delta, \rho)$, avec

- $\delta_{x_1}(q_1) = \delta_{1x_1}(q_1)$,
- $\delta_{x_2}(q_1) = e$,
- $\delta_{x_2}(q_2) = \delta_{2x_2}(q_2)$,
- $\delta_{x_1}(q_2) = e$,
- $\rho_{q_1}(x_1) = \rho_{1q_1}(x_1)$,
- $\rho_{q_1}(x_2) = x_2$,
- $\rho_{q_2}(x_2) = \rho_{2q_2}(x_2)$,
- $\rho_{q_2}(x_1) = x_1$

pour $x_1 \in \Sigma_1$, $x_2 \in \Sigma_2$, $q_1 \in Q_1$, $q_2 \in Q_2$, et avec e un état-puits auquel sont identifiés les éventuels états-puits des automates $\mathcal{A}_1$ et $\mathcal{A}_2$.

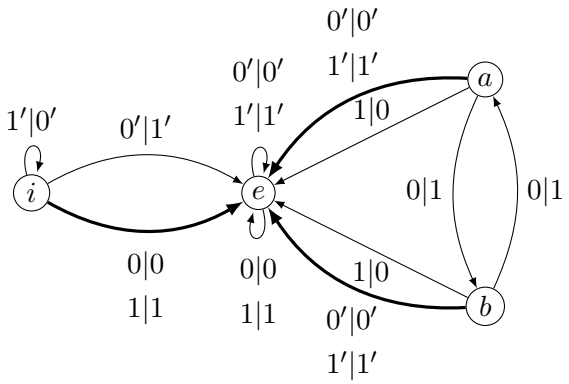


FIGURE I.20 – Produit direct puisé de la machine à additionner et de l'automate de la Basilique. Les nouvelles transitions sont en gras.

Proposition 2.17

Soient $\mathcal{A}_1$ et $\mathcal{A}_2$ deux automates de Mealy. On a $\langle \mathcal{A}_1 \times_{\mathcal{S}} \mathcal{A}_2 \rangle_+ = \langle \mathcal{A}_1 \rangle_+ \times \langle \mathcal{A}_2 \rangle_+$

Démonstration. Posons $\mathcal{A}_1 = (Q_1, \Sigma_1, \delta_1, \rho_1), \mathcal{A}_2 = (Q_2, \Sigma_2, \delta_2, \rho_2)$. On montre tout d'abord que les éléments représentés par des mots sur Q_1 commutent avec les éléments représentés par des mots sur Q_2 : soient $\boldsymbol{u}_1 \in Q_1^*, \boldsymbol{u}_2 \in Q_2^*$, $\boldsymbol{s}_1 \in \Sigma_1^+$ et $\boldsymbol{s}_2 \in \Sigma_2^+$.

$$\begin{array}{ccccc} & \boldsymbol{s}_1 & & \boldsymbol{s}_2 & \\ \boldsymbol{u}_1 & \downarrow & \delta_{\boldsymbol{s}_1}(\boldsymbol{u}_1) = \delta_{1\boldsymbol{s}_1}(\boldsymbol{u}_1) & \downarrow & e^{|\boldsymbol{u}_1|} \\ & \rho_{\boldsymbol{u}_1}(\boldsymbol{s}_1) = \rho_{1\boldsymbol{u}_1}(\boldsymbol{s}_1) & & \boldsymbol{s}_2 & \\ \boldsymbol{u}_2 & \downarrow & e & \downarrow & e^{|\boldsymbol{u}_2|} \\ & \rho_{1\boldsymbol{u}_1}(\boldsymbol{s}_1) & & \boldsymbol{s}_2 & \end{array}$$

Réciproquement :

$$\begin{array}{ccccc} & \boldsymbol{s}_1 & & \boldsymbol{s}_2 & \\ \boldsymbol{u}_2 & \downarrow & e & \downarrow & e^{|\boldsymbol{u}_2|} \\ & \boldsymbol{s}_1 & & \boldsymbol{s}_2 & \\ \boldsymbol{u}_1 & \downarrow & \delta_{\boldsymbol{s}_1}(\boldsymbol{u}_1) = \delta_{1\boldsymbol{s}_1}(\boldsymbol{u}_1) & \downarrow & e^{|\boldsymbol{u}_1|} \\ & \rho_{\boldsymbol{u}_1}(\boldsymbol{s}_1) = \rho_{1\boldsymbol{u}_1}(\boldsymbol{s}_1) & & \boldsymbol{s}_2 & \end{array}$$

Après la deuxième alternation des alphabets, on se retrouve dans l'état $e^{|\boldsymbol{u}_1|+|\boldsymbol{u}_2|}$, qui agit comme l'identité sur le reste du mot. On obtient ainsi la commutativité des mots sur les alphabets différents.

De plus, si $r \in Q_1 \sqcup Q_2$ est une relation dans $\langle \mathcal{A}_1 \times_{\mathcal{S}} \mathcal{A}_2 \rangle_+$, alors c'est un mélange (au sens produit de mélange, ou shuffle, noté $\sqcup\!\sqcup$) de relations dans $\langle \mathcal{A}_1 \rangle_+$ et $\langle \mathcal{A}_2 \rangle_+$. C'est alors une relation dans $\langle \mathcal{A}_1 \rangle_+ \times \langle \mathcal{A}_2 \rangle_+$: par commutativité, on peut exprimer $\rho_{\boldsymbol{r}} = \rho_{\boldsymbol{r}_1 \boldsymbol{r}_2} = \rho_{\boldsymbol{r}_2 \boldsymbol{r}_1}, \boldsymbol{r}_1 \in Q_1^*, \boldsymbol{r}_2 \in Q_2^*$. Alors, pour $\boldsymbol{v}_1 \in \Sigma_1$ $\rho_{\boldsymbol{r}}(\boldsymbol{v}_1) = \rho_{\boldsymbol{r}\boldsymbol{r}_2}(\boldsymbol{v}_1) = \rho_{1_{\boldsymbol{r}_1}}(\boldsymbol{v}_1) = \boldsymbol{v}_1$, donc $\boldsymbol{r}_1$ est une relation dans $\langle \mathcal{A}_1 \rangle_+$. D'autre part, si $(\boldsymbol{r}_1, \boldsymbol{r}_2)$ est une relation dans $\langle \mathcal{A}_1 \rangle_+ \times \langle \mathcal{A}_2 \rangle_+$, alors un mélange $\boldsymbol{r} \in \boldsymbol{r}_1 \sqcup\!\sqcup \boldsymbol{r}_2$ est une relation dans $\langle \mathcal{A}_1 \times_{\mathcal{S}} \mathcal{A}_2 \rangle_+$, et on peut donc conclure. □

On pourrait aussi se demander ce qui se passe si les états envoyés dans l'état identité par une lettre de l'autre alphabet ne porte pas l'identité. Cette construction préserve la finitude.

D'autre part, Brough et Cain ont étudié dans [23] des constructions d'automates permettant de produire des produits semi-directs et des produits couronnes de groupes d'automate, sans toutefois parvenir à des constructions tout à fait générales.

Une autre construction très importante est la *minimisation* de l'automate : l'idée globale est de grouper les états qui représentent le même élément dans le (semi-)groupe. Cela peut être effectué algorithmiquement sur l'automate, via la notion de *classe de Nerode*.

Définition 2.18 (Classe de Nerode)

L'*équivalence de Nerode* $\equiv$ est la limite de la suite $\equiv_k$ de relations de plus en plus fines sur les états de l'automate, définie par

$$\forall p, q \in Q,\ p \equiv_0 q \iff \forall x \in \Sigma \colon \rho_p(x) = \rho_q(x)\ ,$$
$$\forall k \geqslant 0\ p \equiv_{k+1} q \iff p \equiv_k q \quad \wedge \quad \forall x \in \Sigma \colon \delta_x(p) \equiv_k \delta_x(q)\ .$$

Comme l'ensemble des états est fini, cette suite est ultimement constante et on notera $\equiv$ la relation limite.

À l'aide de cette relation, on peut simplifier l'automate en identifiant les états d'une même classe :

Définition 2.19 (Minimisé d'un automate)

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy. Son *minimisé* est l'automate $\mathfrak{m}\mathcal{A} = \big(Q/\equiv, \Sigma, \overline{\delta}, \overline{\rho}\big)$, dont les transitions sont données par :

$$[p]_\equiv \xrightarrow{x|y} [q]_\equiv \in \mathfrak{m}\mathcal{A} \quad \Longleftrightarrow \quad p \xrightarrow{x|y} q \in \mathcal{A}\,,$$

où $[p]_\equiv$ désigne la classe d'équivalence de p pour le relation de Nerode.

On obtient :

Lemme 2.20

Un automate de Mealy et son minimisé engendrent le même semi-groupe (*resp.* groupe le cas échéant).

Ainsi, Akhavi, Klimann, Lombardy, Mairesse et Picantin ont eu l'idée d'alterner minimisations et dualisations (voir la figure I.21), de manière à déterminer si le (semi-)groupe engendré par un automate donné est fini. En effet, si la suite $(\mathfrak{m}\mathfrak{d}\mathfrak{m}\mathfrak{d})^*\mathcal{A}$ (dite suite des $\mathfrak{m}\mathfrak{d}$ réductions) converge vers un automate engendrant un (semi-)groupe fini, alors le (semi-)groupe engendré par $\mathcal{A}$ est lui-même fini. On a de plus que la limite de cette suite est la même que celle de $(\mathfrak{d}\mathfrak{m}\mathfrak{d}\mathfrak{m})^*\mathcal{A}$ ([1, Proposition 3.5]). On dit que l'automate $\mathcal{A}$ est $\mathfrak{m}\mathfrak{d}$-*réduit* quand $\mathfrak{d}\mathfrak{m}\mathfrak{d}\mathfrak{m}\mathcal{A} = \mathcal{A}$ et qu'il est $\mathfrak{m}\mathfrak{d}$-*trivial* si la suite des $\mathfrak{m}\mathfrak{d}$ réductions converge vers l'automate trivial (un état et une lettre). Notons qu'il existe des automates de Mealy non $\mathfrak{m}\mathfrak{d}$ triviaux et qui engendre des groupes finis [1]

On a mis en place quelques moyens pour étudier les groupes engendrés par les automates de Mealy. On va maintenant voir quelles sont les questions qui se posent à leur sujet.

3 Quelques problématiques sur les (semi-)groupes d'automate

Dans les années 60, Gluškov [43] suggère de considérer les automates de Mealy pour attaquer des problèmes de théorie des groupes. Cette idée s'avère fructueuse et permet de nombreuses avancées en théorie des groupes, mais lance aussi l'étude des automates de Mealy comme objet propre ou pour la classe des groupes qu'ils engendrent.

On va commencer par décrire les propriétés communes à tous les groupes d'automate.

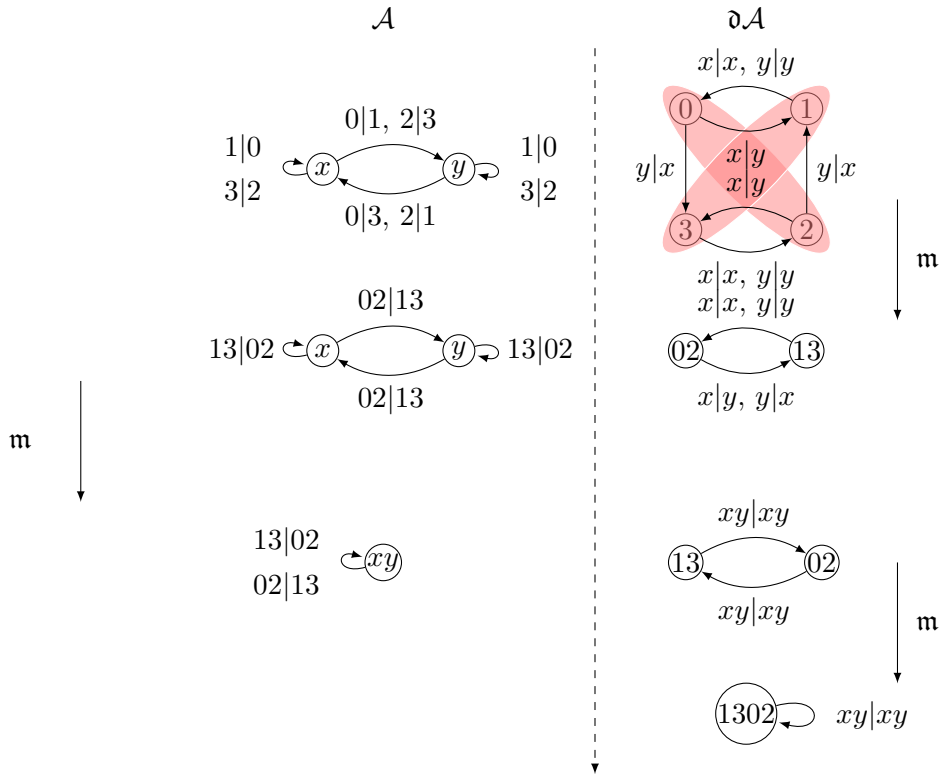


FIGURE I.21 – Une suite de $\mathfrak{m}\mathfrak{d}$-réductions conduisant à un automate trivial.

3.1 Propriétés des (semi-)groupes d'automate

On a vu dans les premiers exemples représentés figures I.6 et I.7 que les (semi-)groupes engendrés par les automates de Mealy peuvent être finis comme infinis, et dans la proposition 2.8 que n'importe quel (semi-)groupe fini peut être engendré par un automate.
Il est clair qu'un (semi-)groupe engendré par un automate est *finiment engendré*, puisque l'ensemble (fini) des fonctions associées aux états de l'automate forme un système de générateurs.
On peut aussi montrer que les (semi-)groupes d'automates sont *résiduellement finis* :

Définition 3.1 ((semi-)groupe résiduellement fini)

On dit qu'un (semi-)groupe G est *résiduellement fini* si, pour toute paire d'éléments différents $g, h \in G$, il existe un (semi-)groupe fini F et un morphisme de (semi-)groupes $\varphi : G \to F$ tels que $\varphi(g) \neq \varphi(h)$.

On peut dire que les (semi-)groupes résiduellement finis s'approximent par une suite de (semi-)groupes quotients finis.

Proposition 3.2

Tout (semi-)groupe d'automate est résiduellement fini.

Démonstration. Soient un automate de Mealy $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ et $g, h \in \langle \mathcal{A} \rangle_+$ avec $g \neq h$. Comme g est différent de h, il existe un entier ℓ et un mot $\boldsymbol{v} \in \Sigma^\ell$ tels que $g.\boldsymbol{v} \neq h.\boldsymbol{v}$. Posons alors $F = T_{\Sigma^\ell}$, le semi-groupe des transformations de Σ^ℓ, et prenons $\varphi : \langle \mathcal{A} \rangle_+ \to F$ la projection naturelle. Alors $\varphi(g) \neq \varphi(h)$, on a donc le résultat annoncé. □

Cette propriété constitue, avec l'existence d'un ensemble fini de générateurs, une obstruction forte pour certains (semi-)groupes pour être des groupes d'automate. Citons par exemple les groupes de Baumslag-Solitar $BS(n, m)$ (exceptés les cas où $m = n$ ou bien si l'un des paramètres vaut 1), le monoïde bicyclique $\langle ab = \mathbb{1} \rangle_+$ (pourtant automatique) ou encore les groupes de Thompson F et T.
De plus, cette propriété nous permet d'utiliser un théorème de Zelmanov [107, 106] pour obtenir un lien entre l'ordre des éléments d'un groupe d'automate et la finitude de celui-ci.
On rappelle :

Définition 3.3 (Ordre d'un élément, torsion)

Soit G un groupe et $g \in G$. L'*ordre* de g est

$$|g| = |\langle g \rangle| = \left|\{g^i, \quad i \in \mathbb{N}\}\right| .$$

Si l'ordre est fini, alors c'est le plus petit entier strictement positif tel que :

$$g^{|g|} = \mathbb{1}_G .$$

La *torsion* de G est l'ensemble de ses éléments d'ordre fini. Le groupe est dit *sans torsion* si sa torsion se réduit à l'élément neutre. Le groupe est dit *de torsion* si tous ses éléments sont d'ordre fini.

Un théorème de Zelmanov [107, 106] affirme qu'un groupe résiduellement fini dont les ordres des éléments sont bornés par une constante est fini.
On a donc l'équivalence :

Proposition 3.4

Soit $\mathcal{A}$ un automate de Mealy inversible :

$$|\langle\mathcal{A}\rangle| = \infty \iff \begin{cases} \exists\, g \in \langle\mathcal{A}\rangle, & |g| = \infty \\ \exists\, (g_i)_i \in \langle\mathcal{A}\rangle, & \lim |g_i| = \infty\,. \end{cases} \text{ ou}$$

Cette propriété nous sera notamment utile dans la section 3.

La structure d'automate permet aussi de montrer que le *problème du mot* est toujours décidable pour les (semi-)groupes d'automate :

Problème 3.5 (Problème du mot)

Soient G un (semi-)groupe et S un ensemble générateur de G. Le *problème du mot* pour G consiste en la procédure de décision :

- **entrée :** deux mots $\boldsymbol{u}, \boldsymbol{v} \in S^*$;
- **sortie :** `oui` si et seulement si $\boldsymbol{u}$ représente le même élément que $\boldsymbol{v}$ dans G.

Proposition 3.6

Le problème du mot est décidable dans un (semi-)groupe d'automate.

Démonstration. Soient $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ et $\boldsymbol{u}, \boldsymbol{v} \in Q^*$. On remarque qu'ajouter un état isolé e induisant une transformation triviale à un automate ne change pas le (semi-)groupe engendré, on suppose donc que les deux mots sont de même longueur ℓ. On peut alors calculer les classes de Nerode de l'automate $\mathcal{A}^\ell$, et on a $\rho_{\boldsymbol{u}} = \rho_{\boldsymbol{v}} \iff [\boldsymbol{u}]_\equiv = [\boldsymbol{v}]_\equiv$. □

Ainsi, un (semi-)groupe d'automate

- est finiment engendré,
- est résiduellement fini,
- a un problème du mot décidable.

Il est naturel de se demander si tous les groupes satisfaisant de telles propriétés sont des groupes d'automate. La question est posée pour les groupes de tresses par Sushchanskiı̆ [74, Problem 16.84] et plus généralement :

Question 3.7 ([25])

Existe-il des groupes finiment engendrés, résiduellement finis et avec un problème du mot décidable mais qui ne sont pas des groupes d'automate ?

Dans le cadre des semi-groupes, Brough et Cain ont montré qu'aucun sous-semi-groupe de $(\mathbb{N}^*, +)$ n'était engendré par un automate [23]. Cependant on n'aboutit pas à une caractérisation, ni même à un contre-exemple pour les monoïdes, et cette question reste largement ouverte.

3.2 Problèmes impliquant les groupes d'automate

La première grande question et réussite où les groupes engendrés par un automate de Mealy ont joué un rôle est le problème de Burnside :

Problème de Burnside et problèmes de décision

Question 3.8 (Burnside, 1902 [24])

Un groupe (finiment engendré) de torsion peut-il être infini ?

De manière évidente, tous les éléments d'un groupe fini sont d'ordre fini, et par contraposée, si un groupe possède un élément d'ordre infini, alors il est infini.
Notons que l'on demande bien que tous les éléments soient d'ordre fini et pas seulement les générateurs (sans quoi le produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ serait un exemple facile) et que le groupe ait un nombre fini de générateurs (autrement on trouve des exemples simples comme $\bigoplus_{\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$).
Ce problème a été proéminent en théorie des groupes dans la première moitié du XX$^{\text{e}}$ siècle, mais n'a pas été résolu avant 1964 :

Théorème 3.9 (Golod-Shafarevich 1964 [47, 48])

Il existe des groupes finiment engendrés, infinis et de torsion.

On appellera désormais *groupe de Burnside* un groupe finiment engendré et de torsion.
Peu après, des groupes de Burnside infinis encore plus contraints ont été découverts :

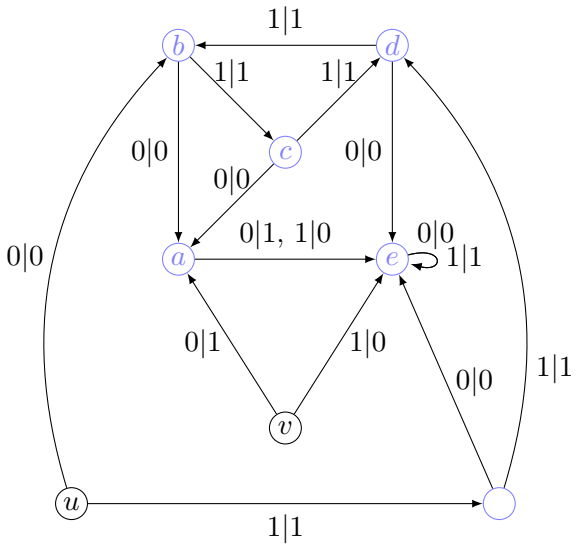


FIGURE I.22 – L'automate d'Alešin. Le groupe $\langle u, v \rangle$ est un groupe infini de Burnside.

Théorème 3.10 (Adian-Novikov 1968 [81])

Il existe des groupes finiment engendrés, infinis et dont tous les éléments sont d'ordre fini inférieur à une constante N.

L'étude de ce problème a continué de susciter de nombreux travaux importants. En particulier Zelmanov a reçu en 1994 une médaille Fields pour ses travaux sur le problème de Burnside restreint, c'est-à-dire où l'on considère les groupes ayant les ordres uniformément bornés et un nombre fixé de générateurs.

Les théorèmes précédents font néanmoins appel à des notions complexes de théorie des groupes, et leurs démonstrations n'offrent pas vraiment d'exemples manipulables. En revanche, en 1972, dans un article de cinq pages [2], Alešin a donné un exemple d'un groupe de Burnside infini sous la forme d'un sous-groupe engendré par un automate de Mealy (voir la figure I.22)

Peu après, en 1980, Grigorchuk améliore la compréhension de ce résultat en montrant que l'on peut obtenir ce résultat directement avec un groupe d'automate. Ce groupe, appelé ci-après *groupe de Grigorchuk*, ou bien *groupe de Grigorchuk-Alešin* est engendré par l'automate décrit figure I.23, et on a :

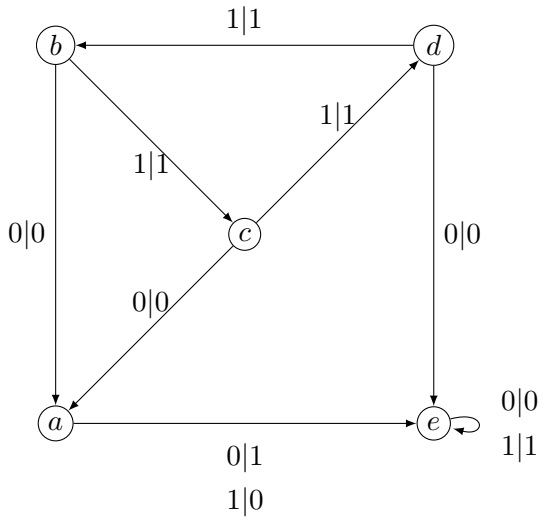


FIGURE I.23 – L'automate de Grigorchuk $\mathcal{G}$.

Théorème 3.11 (Grigorchuk 1980 [50])

Le groupe de Grigorchuk, engendré par l'automate $\mathcal{G}$ figure I.23, est un groupe de Burnside infini.

Cet exemple a été déterminant dans le développement de la théorie des groupes d'automate. Il existe des preuves admirablement élémentaires de ce théorème, et on en a adapté une dans la section 1 pour montrer que l'automate Bread-and-Butterfly engendre lui aussi un groupe infini de Burnside.

La preuve de ce théorème passe par la réponse à deux questions : "le groupe engendré est-il infini ?" et "tous les éléments sont-ils d'ordre fini ?". On peut poser ces questions pour n'importe quel (semi-)groupe d'automate :

Problème 3.12 (Problème de la finitude)

Soit $\mathcal{A}$ un automate. Le semi-groupe $\langle\mathcal{A}\rangle_+$ est-il fini ?

Problème 3.13 (Problèmes de l'ordre)

Soient $\mathcal{A}$ un automate inversible et $g \in \langle\mathcal{A}\rangle$: g est-il d'ordre fini ? Le groupe $\langle\mathcal{A}\rangle$ est-il de Burnside ?

Pour le groupe de Grigorchuk, le problème de la finitude est réglé de manière explicite. Cependant on aimerait savoir si la réponse peut nous être fournie par un algorithme, en d'autres termes si ce problème est *décidable* pour un automate inversible $\mathcal{A}$ donné. Ce problème est difficile, et en effet, dans le cadre des semi-groupes d'automate, on a:

Théorème 3.14 (Gillibert 2014 [41])

Le problème de finitude pour la classe des semi-groupes d'automate est indécidable.

Néanmoins la démonstration ne couvre pas le cas des groupes d'automate, pour lesquels le problème reste pour l'instant ouvert.
La situation est néanmoins différente pour certaines sous-classes d'automates. Parmi elles citons :

Théorème 3.15 (Antonenko 2008 [3], Russyev 2010 [86])

Le (semi-)groupe engendré par automate de Mealy appartenant à la classe des automates avec cycles sans échappatoire est fini.

Cette classe est intéressante car elle est en quelque sorte maximale. On a en effet :

Théorème 3.16 ([3, 66])

Soit (Q, Σ, δ) un automate qui n'est pas à cycles sans échappatoire. Alors il existe un choix de fonctions de production ρ tel que $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ engendre un (semi-)groupe infini.

Le comportement inverse est aussi possible :

Théorème 3.17 ([1])

Tout groupe engendré par un automate inversible, réversible mais non biréversible est infini.

Malgré leur structure très rigide, les automates biréversibles engendrent une grande variété de groupes : tous les groupes finis, mais aussi les groupes libres [42, 100, 101], des produits

libres [78] ou encore des groupes de type allumeur de réverbères [21].
Le problème de la finitude reste ouvert si l'on se restreint à cet classe d'automate.

Problème 3.18

Peut-on décider si le groupe engendré par un automate de Mealy est fini ? Même question e considérant un automate biréversible ?

Il existe tout de même un sous-cas où l'on sait répondre :

Théorème 3.19 (Klimann 2013 [63])

Le problème de finitude est décidable pour les automates biréversibles à deux lettres (ou deux états).

La démonstration de ce résultat est basée sur la $\mathfrak{md}$-réduction. Plus précisément, Klimann montre que, dans le cas des automates à deux états (le cas deux lettres s'y réduit par dualisation) un groupe est fini si et seulement si le minimisé du dual du minimisé de son dual est trivial (*i.e.* $|\langle\mathcal{A}\rangle| < \infty \iff \mathfrak{dmdm}\mathcal{A}$ est trivial).

Pour le problème de l'ordre, une classe se distingue, celle des automates à activité bornée. Bondarenko, Bondarenko, Sidki et Zapata ont montré :

Théorème 3.20 ([19])

Le problème de l'ordre est décidable pour les groupes d'automate à activité bornée.

Ils prouvent également que le problème de conjugaison (étant donnés deux éléments $g, h \in \langle\mathcal{A}\rangle$, existe-il $c \in \langle\mathcal{A}\rangle$, satisfaisant $cgc^{-1} = h$) est décidable pour g et h représentable par un automate contractant à activité bornée (et cela même en imposant que c soit lui aussi représentable par un automate à activité bornée).

En dehors de cette classe en revanche, on a :

Théorème 3.21 ([98])

Il existe des groupes d'automate pour lesquels le problème de conjugaison est indécidable.

Ce comportement où un problème est indécidable pour l'ensemble des (semi-)groupes d'automate mais décidable dans une sous-classe "naturelle" semble assez répandu. Il est intéressant de se demander quelles propriétés structurelles (structure en cycle, reversibilité) permetent d'obtenir des classes de groupes où un certain problème devient décidable voir trivial (ordre, Burnside).

On peut citer le problème d'*Engel* : notons $[g,h] = g^{-1}h^{-1}gh$ le *commutateur* de deux éléments g et h.

Problème 3.22 (Problème d'Engel)

Soient $\mathcal{A}$ un automate inversible et $g, h \in \langle\mathcal{A}\rangle$. Est-ce qu'il existe $\ell \in \mathbb{N}^*$ tel que

$$\underbrace{[\dots[[g,h]\,h]\dots h]}_{\ell} = \mathbb{1}\,?$$

Bartholdi donne dans [5] un algorithme qui est assuré de terminer sur des automates satisfaisant des conditions strictes de contraction. Il fournit également une réponse sur des exemples classiques ne satisfaisant pas ces conditions, notamment pour le groupe de Grigorchuk et le groupe de Gupta-Sidki. Il serait intéressant de connaître une condition décidable directement sur l'automate qui rendrait ce problème décidable.

Un autre problème de décision pouvant être étudié dans le cadre des automates de Mealy est le problème du sac à dos :

Problème 3.23 (Problème du sac à dos)

Soit G un groupe. Le *problème du sac à dos* consiste en la procédure de décision :
- **entrée :** $(g_1, \dots g_\ell, g) \in G^{\ell+1}$;
- **sortie :** `oui` si et seulement s'il existe $\alpha_1, \dots \alpha_\ell \in \mathbb{Z}$ tels que $g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_\ell^{\alpha_\ell} = g$.

Ce problème, qui est une généralisation de plusieurs problèmes classiques dont le problème de l'ordre, se révèle indécidable dans la classe des groupes d'automate. En effet, il a été prouvé

dans [69], et indépendamment dans [38], que le problème du sac à dos est indécidable pour un groupe formé de suffisamment de copies du groupe d'Heisenberg défini par :

$$H_3(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} ; \, a, b, c \in \mathbb{Z} \right\} .$$

Il se trouve que Bondarenko et Kravshenko ont prouvé [18]:

Proposition 3.24 (Bondarenko-Kavshenko [18])

L'automate $\mathcal{H}$ de la figure I.24 satisfait $\langle \mathcal{H} \rangle = H_3(\mathbb{Z})$.

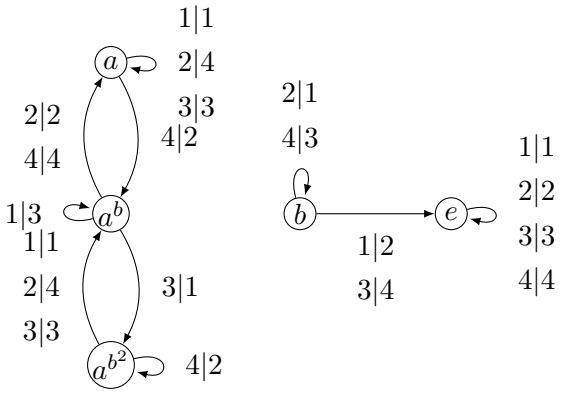


FIGURE I.24 – L'automate de Mealy $\mathcal{H}$ engendrant le groupe d'Heisenberg $H_3(\mathbb{Z})$.

Ainsi, comme le produit direct de groupes d'automate est un groupe d'automate, on déduit :

Proposition 3.25

Le problème du sac à dos est indécidable pour la classe des groupes d'automate.

On peut donc se demander s'il y a une classe d'automates (non triviale) pour laquelle ce problème est décidable.

On peut ainsi spécialiser tout problème de décision de la théorie des groupes aux groupes d'automate. On peut aussi se placer dans le cadre des semi-groupes d'automate et poser des questions analogues.

Croissance des (semi-)groupes

Le deuxième problème pour lequel les automates de Mealy se sont illustrés est le problème de la croissance des groupes [73].

Définition 3.26 (Graphe de Cayley)

Soient G un groupe finiment engendré et un ensemble générateur $S = \{s_1, \dots, s_\ell\}$ satisfaisant $S = S^{-1}$. Le *graphe de Cayley* de G pour S est le graphe $\Gamma_{G,S}$ ayant comme sommets les éléments de G et comme arêtes :

$$g \xrightarrow{s} h, \text{ avec } s \in S \text{ et } gs = h\,.$$

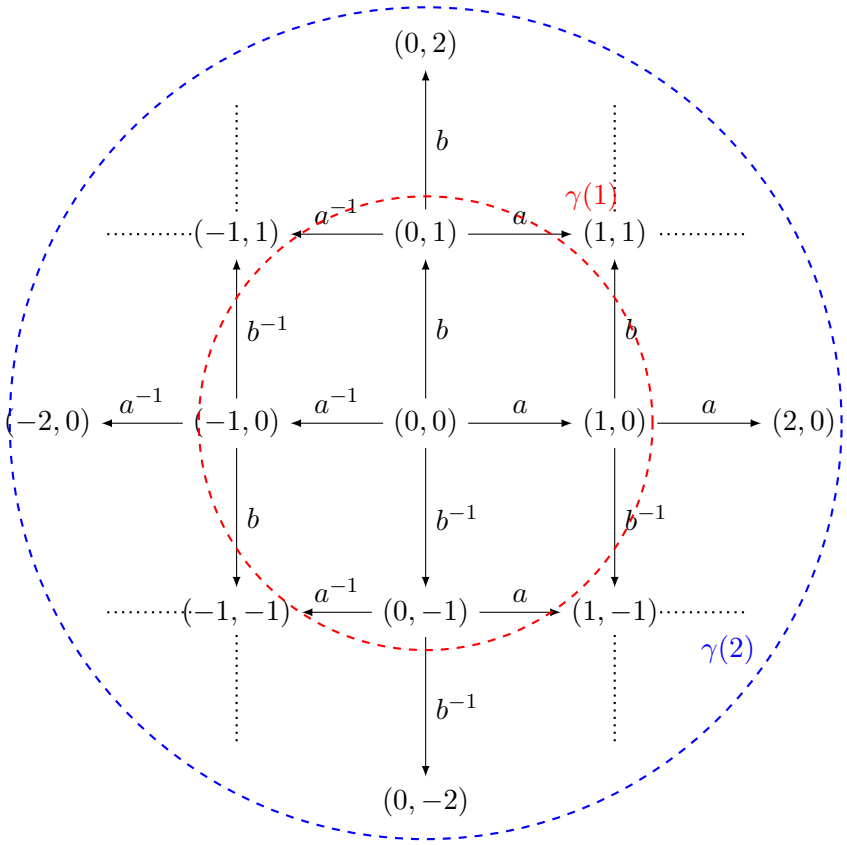


FIGURE I.25 – Le graphe de Cayley de $\mathbb{Z}^2$ et les boules de rayons 1 et 2.

Par exemple, le graphe de Cayley de $\mathbb{Z}^2$ associé au système générateur $\{(0, \pm 1), (\pm 1, 0)\}$ est représenté figure I.25.

On peut compter les éléments qui peuvent être représentés par un mot sur S de longueur au plus ℓ : il s'agit du nombre d'éléments du graphe de Cayley contenus dans une boule de rayon ℓ centrée en l'élément neutre du groupe.

Définition 3.27 (Fonction de croissance)

Soient G un groupe finiment engendré et $S = \{s_1, \dots, s_\ell\}$ un ensemble de générateurs de G, satisfaisant $S = S^{-1}$. La *fonction de croissance* de G selon S est la fonction $\gamma_{G,S} : \mathbb{N} \to \mathbb{N}$ définie par :

$$\gamma_{G,S}(\ell) = |\{g \in G,\ \exists i \leq \ell, \exists s_1, \dots s_i \in S, g = s_1 s_2 \cdots s_i\}|$$

Cette fonction est croissante et dépend de S. En revanche deux fonctions de croissance d'un même groupe sont bilipschitz équivalentes (c'est à dire que si γ et γ' sont deux fonctions de croissance d'un même groupe, il existe trois entiers positifs a, b, c tels que $\forall n \in \mathbb{N}, a\gamma'(n) \leq \gamma(n) \leq b\gamma'(n) \leq c\gamma(n)$). On peut donc étudier la fonction de croissance d'un groupe pour un ensemble de générateurs et obtenir des conclusions générales. De plus, si f et g sont deux fonctions, on dira que $f \precsim g$ s'il existe une constante positive a telle que pour tout entier n $f(n) \leq g(an)$ Par exemple on a :

Remarque 3.28 (Folklore)

Un groupe est fini si et seulement si sa fonction de croissance est ultimement constante (pour tout ensemble générateur du groupe).

Dans la suite on omettra donc souvent l'ensemble générateur dans nos notations.
On peut aussi étudier des exemples particuliers. On a :

— $\gamma_{\mathbb{Z}^d}$ est un polynôme de degré d,
— γ_{F_d} est une fonction exponentielle de paramètre d (F_d est le groupe libre à d générateurs) [2].

Cette croissance peut donc être bornée (quand G est fini) ; polynomiale, et ce, par un théorème de Gromov, si et seulement si le groupe est virtuellement nilpotent [3] [56] (en particulier, si le groupe est abélien (commutatif) alors la croissance est au plus polynomiale) ; ou bien encore exponentielle, par exemple dans le cas des groupes libres. En 1968, Milnor demande si

2. On en déduit que la fonction de croissance n'est pas monotone pour la relation de sous-groupe : par le théorème de Nielsen-Schreier, F_2 contient tous les F_d comme sous-groupes, et en particulier $\gamma_{F_3} > \gamma_{F_2}$.
3. C'est-à-dire qu'il admet un sous-groupe d'indice fini nilpotent

cette classification est complète, c'est-à-dire s'il existe des groupes où la fonction de croissance est supérieure à n'importe quel polynôme, mais toutefois sous-exponentielle. On parle alors de croissance intermédiaire.

En 1984, Grigorchuk montre :

Théorème 3.29 (Grigorchuk 1984 [49], Bartholdi 1998-2001 [8, 7])

Le groupe de Grigorchuk est à croissance intermédiaire et sa croissance est bornée par :

$$\exp 0.5157\ell \precsim \gamma_{\langle \mathcal{G} \rangle}(\ell) \precsim \exp 0.767\ell \,.$$

Grigorchuk obtient ainsi le premier exemple de groupe à croissance intermédiaire, qui reste le modèle de base pour l'étude de ces groupes, y compris pour la création de nouveaux types de croissance [62]. D'autre groupes d'automate à croissance intermédiaire ont été construits [36], il semble cependant difficile de donner une estimation exacte de la croissance.

Cette notion de croissance intermédiaire peut aussi s'étendre aux semi-groupes, où des exemples de semi-groupes à croissance intermédiaire ont été trouvés dès 1977 [15]. Là aussi les automates de Mealy fournissent d'intéressants exemples [9].

Les groupes d'automate servent également à contredire une autre conjecture sur la croissance de groupes. Gromov a demandé en 1981 si un groupe à croissance exponentielle a toujours un taux de croissance uniforme, *i.e.* si $\inf_S \lim_\ell \sqrt[\ell]{\gamma_{G,S}(\ell)} > 1$. Or on a :

Théorème 3.30 (Wilson 2004 [105])

Il existe un groupe (d'automate) G et une suite $(S_\Lambda)_\Lambda$ d'ensembles de générateurs de G tels que :

$$\inf_{S_\Lambda} \lim_\ell \sqrt[\ell]{\gamma_{G,S_\Lambda}(\ell)} = 1$$

Là aussi, l'étude de sous-classes spécifiques permet d'obtenir des caractérisations de la croissance :

Théorème 3.31 (Klimann 2016 [64])

Un automate inversible, réversible et dont toutes le puissances sont connexes [4]croît de manière exponentielle.

3.3 Dynamique de l'action

D'autres problèmes concernant les groupes d'automate proviennent de l'étude de l'action du groupe sur l'arbre enraciné $|\Sigma|$-aire. Il est possible d'identifier l'ensemble Σ^ℓ des mots de longueur ℓ avec un arbre $|\Sigma|$ régulier enraciné en le mot vide : chaque sommet au niveau i est étiqueté par un mot de longueur i et pour l'étiquette chacun de ses enfants on ajoute une lettre de Σ à l'étiquette de ce nœud (de manière à ce que tous ces enfants aient une étiquette différente).
On peut facilement munir cet arbre, ainsi que sa frontière (isomorphe à Σ^ω), d'une topologie et d'une mesure.

On dit que l'automate inversible $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ agit *transitivement par niveau* si l'action de $\langle \mathcal{A} \rangle$ est transitive pour chaque niveau ℓ :

$$\forall \ell \geq 0, \quad \forall \boldsymbol{v}, \boldsymbol{v'} \in \Sigma^\ell, \exists g \in \langle \mathcal{A} \rangle, g.\boldsymbol{v} = \boldsymbol{v'} .$$

Grigorchuk, Nekrashevich et Sushchanskii ont demandé dans [52] :

Question 3.32

Existe-t-il un algorithme qui, étant donné un automate de Mealy inversible, détermine si l'action est transitive par niveau ?

Steinberg [96] pointe que la réponse est positive dans le cas d'un automate à deux lettres mais laisse ouverte la question générale.

On peut remarquer que, si $\mathcal{A}$ agit transitivement par niveau, alors de manière équivalente les automates $(\mathfrak{d}\mathcal{A})^\ell$ sont tous (fortement) connexes (au sens de la théorie des graphes). On utilisera plus en détail cette remarque dans la section 1.

L'action de l'automate est aussi liée à la notion de *graphe de Schreier*.

4. dans la section suivante on verra que l'on peut alors dire que le dual agit transitivement par niveau.

Définition 3.33 (Graphe de Schreier)

Soient G un groupe, S un ensemble générateur symétrique fini de G et X un ensemble sur lequel G agit (on note $g \cdot x$ l'action de $g \in G$ sur $x \in X$). Le *graphe de Schreier* associé à G, S et X est le graphe $\mathrm{Sch}_{G,S}(X)$ dont les sommets sont les éléments de X et les arêtes sont données par :

$$x \xrightarrow{s} s.x \ .$$

Clairement, le graphe de Cayley d'un groupe est le graphe de Schreier pour l'action (à droite) du groupe sur lui-même.
On peut étudier les graphes de Schreier $\mathrm{Sch}_{\langle\mathcal{A}\rangle,Q}(\Sigma^\ell)$, mais aussi $\mathrm{Sch}_{\langle\mathcal{A}\rangle,Q}(\Sigma^\omega)$. On obtient alors une quantité indénombrable de graphes, et on peut s'intéresser à leurs propriétés.
En particulier, Vorobets [102] s'est intéressé à la fonction

$$F : \Sigma^\omega \to \mathrm{Sch}_{\langle\mathcal{G}\rangle,Q}(\Sigma^\omega)$$

pour le groupe $\langle\mathcal{G}\rangle$ de Grigorchuk et a montré (entre autres) que cette fonction F est continue en dehors d'une quantité dénombrable de points, et que les graphes de Schreier de ces points particuliers étaient isolés. On généralise cette approche et ces résultats dans le chapitre III, via la notion de *stabilisateurs* : soit un mot infini $\boldsymbol{\xi} \in \Sigma^\omega$, le stabilisateur de $\boldsymbol{\xi}$ dans $\langle\mathcal{A}\rangle$ est le sous-groupe $\mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi}) = \{g \in \langle\mathcal{A}\rangle, g.\boldsymbol{\xi} = \boldsymbol{\xi}\}$. On peut alors, via une topologie sur l'ensemble des sous-groupes de $\langle\mathcal{A}\rangle$ et une autre sur Σ^ω, définir la continuité de cette fonction F et se pencher sur ses points de discontinuité. Plus précisément, pour un sous-ensemble fini $E \subset \langle\mathcal{A}\rangle$, le E-voisinage d'un sous-groupe $H \leq \langle\mathcal{A}\rangle$ est l'ensemble des sous-groupes $K \leq \langle\mathcal{A}\rangle$ tels que $H \cap E = K \cap E$ (cela correspond à la topologie produit standard sur $\langle\mathcal{A}\rangle$). Du côté de Σ^ω, on dira que deux mots sont proches s'ils partagent un long préfixe.

3.4 Transfert des propriétés structurelles de l'automate au groupe

On a vu dans ce qui précède que se placer dans une sous-classe spécifique permet souvent de résoudre des problèmes dont le cas général nous est inaccessible mais peut aussi mener à des comportements propres à cette classe (par exemple ne donner que des groupes (in)finis ou ayant un problème de conjugaison décidable). Il est en fait naturel de se demander dans quelle mesure se limiter à une sous-classe d'automates restreint l'ensemble des groupes que l'on engendre. On a vu que certaines propriétés structurelles entraînent des restrictions fortes, par exemple les automates avec cycles sans échappatoires n'engendrent que des groupes finis, tandis que les automates inversibles, réversibles mais non biréversibles ne produisent que des groupes infinis (théorèmes 3.15 et 3.17).

Parmi les observations liées à la structure, il est frappant de noter qu'aucun des automates (forcément inversibles) connus engendrant un groupe de Burnside infini n'est réversible. Cela a été remarqué par Klimann, Picantin et Savchuk qui ont successivement prouvé les blocages structurels suivants :

Théorème 3.34 (Klimann 2013 [63])

Un automate inversible et réversible à deux états ne peut pas engendrer un groupe de Burnside infini.

Théorème 3.35 (Klimann, Picantin, Savchuk 2016 [67])

Un automate inversible, réversible et connexe à trois états ne peut pas engendrer un groupe de Burnside infini.

Dans cette thèse, on étend ces résultats, comme présenté dans le chapitre II.

Dans un travail avec Klimann et Picantin, on a montré :

Théorème 3.36 ([46])

Un automate inversible, réversible et non biréversible ne peut pas engendrer un groupe de Burnside infini.

Puis, en collaboration avec Klimann, on a prouvé :

Théorème 3.37 ([45])

Un automate inversible, réversible et connexe ayant un nombre premier d'états ne peut pas engendrer un groupe de Burnside infini.

Nous conjecturons que :

Conjecture 3.38

Un automate de Mealy (inversible et) réversible ne peut pas engendrer un groupe de Burnside infini.

Chapitre II

Automates de Mealy et le problème de Burnside

Les automates de Mealy ont été utilisés depuis 1972 et l'exemple d'Alešin [2] pour fournir des exemples élégants de groupes de Burnside infinis. Après Alešin, de nombreux auteurs ont proposé des exemples de (sous-)groupes d'automate de Burnside infinis, le plus célèbre étant le groupe de Grigorchuk [50], mais on peut aussi citer les groupes de Gupta-Sidki [57], les groupes spinaux de Bartholdi et Sunic [10] ou bien le groupe décrit dans l'introduction, section 1.
Tous les automates engendrant ces groupes se trouvent être *non-réversibles*, c'est-à-dire que les fonctions de transition de l'automate ne sont pas toutes des permutations des états. Dans cette partie on cherche donc à savoir si un automate inversible et réversible peut engendrer un groupe de Burnside infini.
Dans un premier temps, dans la section 1, on décrit l'*arbre lexicographique de Schreier*, un outil introduit par Klimann, Picantin et Savchuk dans [67] pour montrer qu'un automate de Mealy réversible connexe à trois états n'engendre jamais un groupe infini de Burnside, et qui généralise des idées introduites par Klimann dans [63], pour montrer ce même résultat pour les automates de Mealy réversibles à deux états. On étudie cette construction et on prouve quelques propriétés utiles pour le problème de Burnside et le problème de finitude.
Grâce à cet objet, on montre ensuite que si l'automate est inversible, réversible, mais pas coréversible, alors il engendre un semi-groupe sans torsion, et donc en particulier il n'engendre pas un groupe de Burnside. Ce travail, réalisé avec Ines Klimann et Matthieu Picantin, a fait l'objet d'une publication dans LATA 2015 [46].
On considère ensuite le cas, généralisant l'article [67], où l'automate est réversible, connexe, et

a un nombre premier d'états. On arrive alors à la même conclusion en montrant que l'automate n'engendre pas un groupe de Burnside infini. Cette étude a abouti à une publication avec Ines Klimann dans la conférence MFCS 2016 [45].

Dans tout ce chapitre on considère des automates de Mealy réversibles.

1 L'arbre lexicographique de Schreier

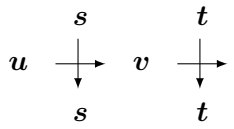
Dans l'introduction, on a décrit le *produit* d'automate. Une suite naturelle que l'on peut associer à un automate est alors la suite $\left(\mathcal{A}^\ell\right)_{\ell\geq 0}$ des puissances de cet automate. Il est possible qu'au cours de cette procédure, l'automate se scinde en plusieurs composantes connexes (voir figure II.1). On remarque alors que la prochaine puissance revient à considérer chaque composante connexe séparément. On obtient alors non plus simplement une suite linéaire de puissances mais un arbre de composantes connexes (chaque composante étant elle-même un automate de Mealy).

Une première propriété des composantes connexes d'un automate réversible est que ces composantes sont fortement connexes. Une deuxième est :

Proposition 1.1 ([67][28])

Si un mot d'état d'une composante connexe d'une puissance d'un automate de Mealy réversible induit l'identité, alors il en va de même pour tous les mots de cette composante (fortement) connexe.

Démonstration. Soient $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy réversible et $\boldsymbol{u} \in Q^*$ avec $\rho_{\boldsymbol{u}} = \mathbb{1}$, et soit $\boldsymbol{v}$ dans la composante connexe de $\boldsymbol{u}$. Par forte connexité, il existe $\boldsymbol{s} \in \Sigma^*$ tel que $\delta_{\boldsymbol{s}}(\boldsymbol{u}) = \boldsymbol{v}$. On a alors, pour tout mot $\boldsymbol{t} \in \Sigma^*$:



car $\rho_{\boldsymbol{u}}(\boldsymbol{st}) = \boldsymbol{st}$, et donc $\rho_{\boldsymbol{v}}(\boldsymbol{t}) = \boldsymbol{t}$. Comme la propriété vaut pour tout $\boldsymbol{t}$, on obtient le résultat. □

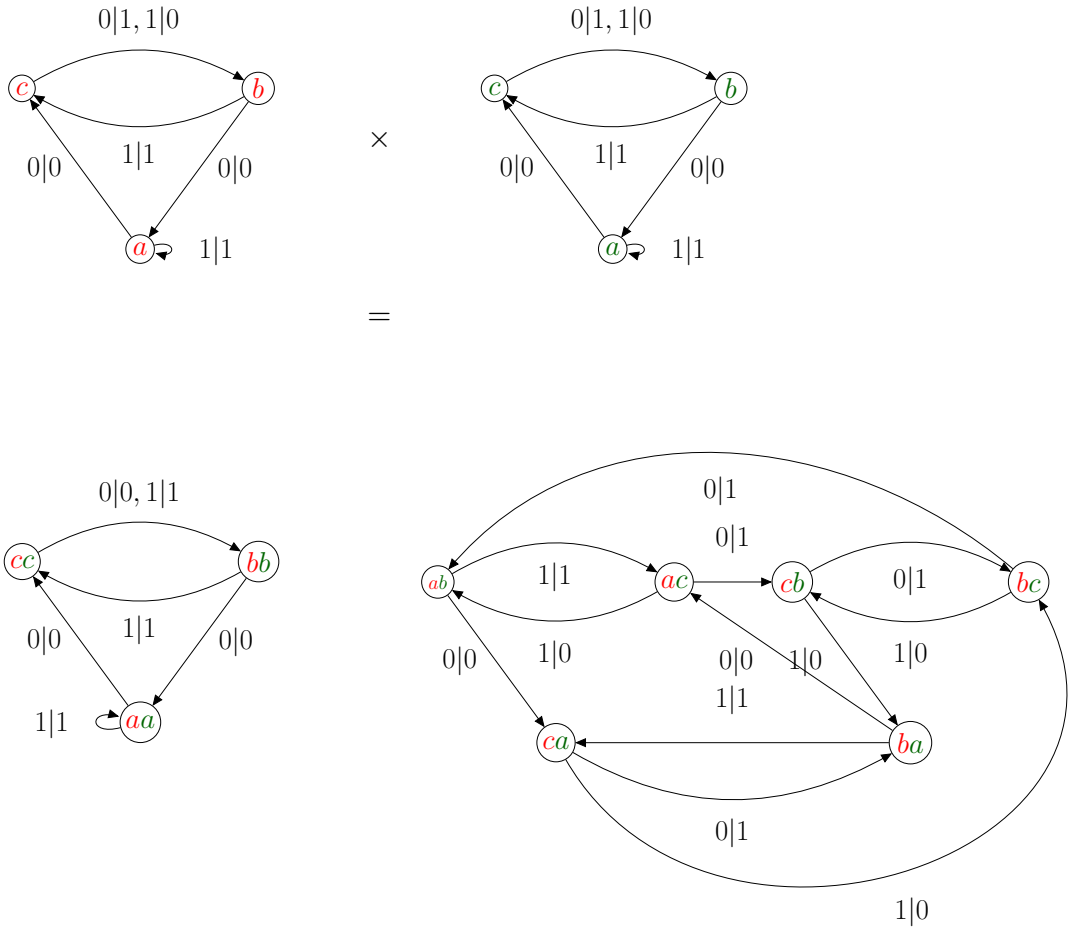


FIGURE II.1 – Le carré de l'automate Bellaterra $\mathcal{B}$.

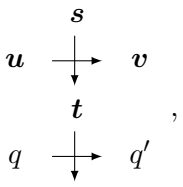
Quand l'automate est réversible, un phénomène combinatoire apparaît entre les tailles des composantes connexes.

Lemme 1.2 ([67])

Soient $\mathcal{A}$ un automate de Mealy réversible et $\ell > 0$ un entier. Si $\mathcal{C}$ est une composante connexe de $\mathcal{A}^\ell$ et $\mathcal{D}$ une composante connexe de $\mathcal{A}^{\ell+1}$ contenant l'état $\boldsymbol{u}q$, avec $\boldsymbol{u} \in \mathcal{C}$ et $q \in Q$. Alors le ratio des tailles $|\mathcal{D}| \,/\, |\mathcal{C}|$ est un entier.

Démonstration. Soit $\boldsymbol{u} \in Q^\ell$ un mot dans $\mathcal{C}$ et soit $Q_{\boldsymbol{u}} \subset Q$ l'ensemble des états tels que $\boldsymbol{u}q \in \mathcal{D}$.

On montre que $|Q_{\boldsymbol{v}}|$ pour $\boldsymbol{v} \in \mathcal{C}$ est plus grand que $|Q_{\boldsymbol{u}}|$. On a pour $q \in Q_{\boldsymbol{v}}$:



,

car, comme $\boldsymbol{u}$ et $\boldsymbol{v}$ sont dans la même composante connexe, il existe un mot $\boldsymbol{s}$ sur Σ^* avec $\delta_{\boldsymbol{s}}(\boldsymbol{u}) = \boldsymbol{v}$, et comme l'automate est complet et déterministe, $\boldsymbol{t} = \rho_{\boldsymbol{u}}(\boldsymbol{s})$ est défini de manière unique. Comme l'automate est réversible, $\boldsymbol{t}$ induit une permutation de Q, donc chaque $q' = \delta_{\boldsymbol{t}(q)}$ est différent et vérifie $\boldsymbol{v}q' \in \mathcal{D}$. Par symétrie, on obtient que $|Q_{\boldsymbol{u}}| = |Q_{\boldsymbol{v}}|$ et on en déduit le résultat. □

On remarque que la composante connexe de $\boldsymbol{u}$ dans $\mathcal{A}^\ell$ correspond à l'orbite de $\boldsymbol{u}$ sous l'action de $\langle \mathfrak{d}\mathcal{A}\rangle_+$: on a une arête $\boldsymbol{u} \in Q^\ell$ et $\boldsymbol{v} \in Q^\ell$ si le mot $\boldsymbol{u}$ est transformé en $\boldsymbol{v}$ par l'action d'un élément du système générateur Σ. C'est exactement la définition du graphe orbital pour les semi-groupes, et (dans le cas d'un automate inversible et réversible) du graphe du Schreier de $\boldsymbol{u}$ selon $\langle \mathfrak{d}\mathcal{A}\rangle$ et Σ.

On définit alors l'*arbre lexicographique de Schreier*[1] d'un automate :

Définition 1.3 (arbre lexicographique de Schreier, [67])

Soit $\mathcal{A}$ un automate de Mealy. L'arbre lexicographique de Schreier $\mathfrak{t}(\mathcal{A})$ est l'arbre enraciné en l'automate trivial sur l'alphabet de $\mathcal{A}$, noté $\mathcal{A}^0$, dont les sommets sont les composantes connexes des $\mathcal{A}^\ell$, $\ell \in \mathbb{N}$, et les arêtes sont données par

$$\mathcal{C} \xrightarrow{r} \mathcal{D}, \text{ s'il existe un mot } \boldsymbol{u} \in \mathcal{C}, \text{ et un état } q \in Q, \text{ tels que } \boldsymbol{u}q \in \mathcal{D} \text{ , et } r = \frac{|\mathcal{D}|}{|\mathcal{C}|} .$$

1. Dans les articles [67, 68, 46] et [45] on parle d'arbre des orbites (orbit tree).

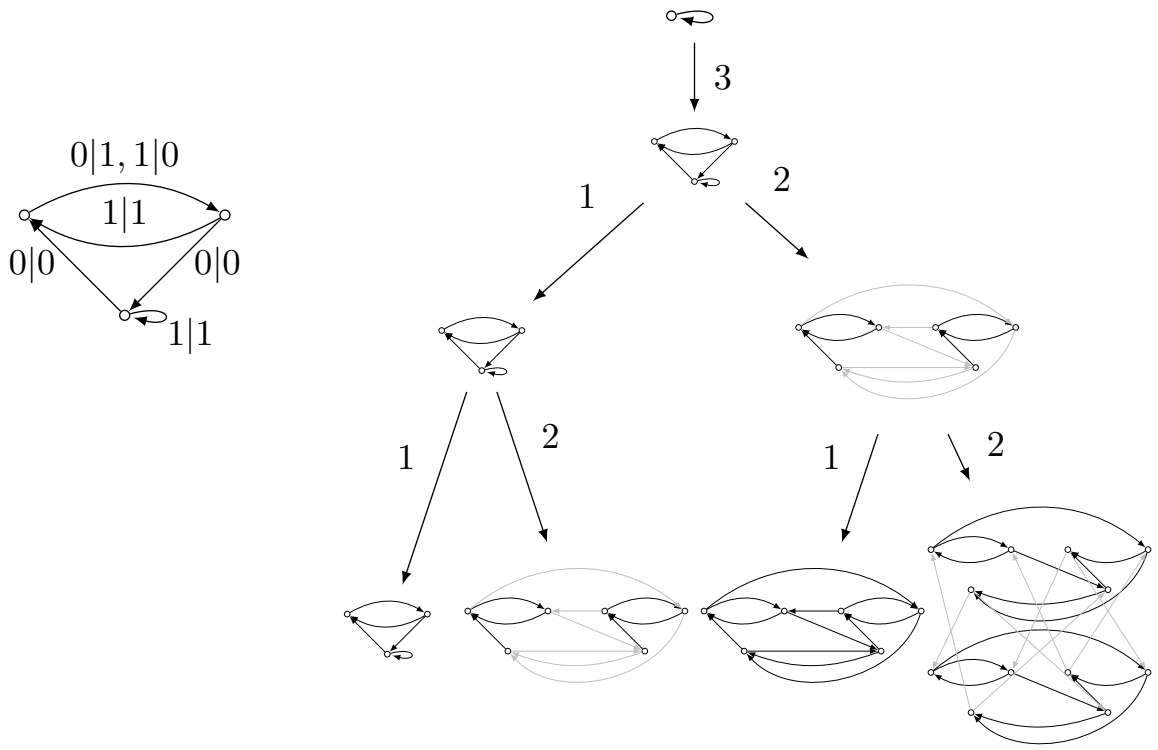


FIGURE II.2 – L'automate $\mathcal{B}$ de Bellaterra et les 4 premiers niveaux de l'arbre lexicographique de Schreier $\mathfrak{t}(\mathcal{B})$.

Dans la suite de la thèse, dans un souci de légèreté et en l'absence d'ambiguïté, on omettra le mot "lexicographique" et on parlera de l'arbre de Schreier d'un automate. Fixons un peu de vocabulaire sur les arbres. Nos arbres sont enracinés, c'est-à-dire qu'ils possèdent un sommet particulier appelé la *racine*. On visualise nos arbres de la manière classique en informatique, *i.e.* grandissant vers le bas depuis la racine. Un *chemin* est une suite (éventuellement infinie) d'arêtes adjacentes dans laquelle on ne revient pas en arrière. On dit qu'un chemin est *initial* s'il débute en la racine de l'arbre. Une *branche* est un chemin initial infini. Le premier sommet d'un chemin $\boldsymbol{e}$ est noté $\top(\boldsymbol{e})$, et, sous réserve que le chemin soit fini, son dernier est noté $\bot(\boldsymbol{e})$. Le *niveau* d'un sommet est sa distance à la racine et le niveau d'un chemin est celui de son sommet initial.
Si les arêtes d'un arbre sont étiquetées, alors l'étiquette d'un chemin est la suite ordonnée des étiquettes de ses arêtes. On étend aussi la notion de parent et enfant aux chemins et aux arêtes. Enfin, dans le cadre des arbres de Schreier, on dit que le *chemin du mot* $\boldsymbol{u} \in Q^*$ est le chemin $\boldsymbol{e}$ (initial) passant par les composantes connexes des préfixes de $\boldsymbol{u}$ (on dira aussi que $\boldsymbol{e}$ est représenté par $\boldsymbol{u}$ ou que $\boldsymbol{u}$ est un représentant du chemin $\boldsymbol{e}$).

Cet arbre de Schreier est particulièrement adapté à l'étude du problème de Burnside pour les automates réversibles. En effet, on a les liens suivants entre ordre et arbre de Schreier :

Proposition 1.4 ([67, 28])

Un automate de Mealy (inversible et) réversible engendre un (semi-)groupe fini si et seulement si les tailles des composantes connexes de ses puissances sont uniformément bornées.

Démonstration. On prouve le résultat pour les groupes, la démonstration pour les semi-groupes est semblable. Supposons que les tailles des composantes connexes des puissances d'un automate inversible et réversible $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ soient bornées. Alors, comme il n'existe qu'un nombre fini d'automates ayant une taille et un alphabet fixés, il n'existe qu'un nombre fini de fonctions de production $\{\rho_{\boldsymbol{u}},\ \boldsymbol{u} \in Q^*\}$. Donc par définition du groupe, $\langle \mathcal{A} \rangle$ est fini.
Si maintenant $\langle \mathcal{A} \rangle$ est fini, alors $\langle \mathfrak{d}\mathcal{A} \rangle$ est lui aussi fini (voir [78, 1] ou le théorème 2.7). Mais alors les orbites selon $\langle \mathfrak{d}\mathcal{A} \rangle$ sont finies de tailles bornées par $|\langle \mathfrak{d}\mathcal{A} \rangle|$. Comme les composantes connexes de $\mathcal{A}^\ell$ sont des orbites selon $\langle \mathfrak{d}\mathcal{A} \rangle$, on a que les composantes connexes sont uniformément bornées. □

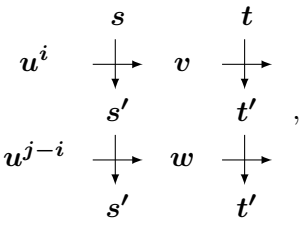
Ainsi on peut savoir, en connaissant les étiquettes de l'arbre de Schreier, si le groupe engendré par l'automate est fini : *le groupe engendré par un automate est fini si et seulement si, pour tout chemin de son arbre de Schreier, la suite des étiquettes sur le chemin est ultimement stationnaire à* 1.

Si le groupe dual $\langle \mathfrak{d}\mathcal{A} \rangle$ est transitif par niveau (et donc que toutes les puissances de $\mathcal{A}$ sont connexes), on obtient le corollaire sur les semi-groupes.

Corollaire 1.5

Si le dual un automate de Mealy réversible agit transitivement par niveau, alors le semi-groupe engendré par l'automate est sans torsion.

Démonstration. Posons $\mathcal{A} = (Q, \Sigma, \delta, \rho)$. Par la proposition 1.4, $\mathcal{A}$ engendre un semi-groupe infini. Supposons par l'absurde que $\boldsymbol{u} \in Q^+$ induit une action d'ordre fini, disons $\rho_{\boldsymbol{u}^i} = \rho_{\boldsymbol{u}^j}$ avec $i < j$. Par réversibilité de $\mathcal{A}$, tout état de $\mathcal{A}^j$ est équivalent à un état de $\mathcal{A}^i$; en effet, comme pour la proposition 1.1 on a :



et $\boldsymbol{vw}$ agit comme $\boldsymbol{v}$. Ainsi $\mathcal{A}$ engendre un semi-groupe fini, contradiction. □

Ce corollaire s'applique, entre autres, au semi-groupe engendré par l'automate $\mathcal{L}$ de l'allumeur de réverbères dessiné figure II.3.

On retrouve ce lien pour l'ordre des éléments.

Proposition 1.6 ([67][28])

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy inversible et réversible, et soit $\boldsymbol{u} \in Q^*$. Les propositions suivantes sont équivalentes :

(i) l'élément $\rho_{\boldsymbol{u}} \in \langle \mathcal{A} \rangle$ est d'ordre fini ;

(ii) la suite indexée par ℓ des tailles des composantes connexes contenant $\boldsymbol{u}^\ell$ est bornée ;

(iii) il existe un mot $\boldsymbol{v} \in Q^*$ tel que la suite indexée par ℓ des tailles des composantes connexes contenant $\boldsymbol{vu}^\ell$ est bornée ;

(iv) pour tout mot $\boldsymbol{v} \in Q^*$, la suite indexée par ℓ des tailles des composantes connexes contenant $\boldsymbol{vu}^\ell$ est bornée.

Démonstration. Les implications (ii) ⇒ (iii), (iv) ⇒ (ii) et (iv) ⇒ (iii) sont immédiates.
Montrons (i) ⇒ (ii) : il existe $c \geq 1$ tel que $\rho_{\boldsymbol{u}^c} = \mathbb{1}$. Alors tous les mots de la composante connexe de $\boldsymbol{u}^c$ induisent l'identité. Donc l'automate $\mathcal{C}(\boldsymbol{u}^c)$ (la composante connexe de $\boldsymbol{u}^c$) engendre un groupe fini (trivial), donc d'après la proposition 1.4, les tailles des composantes connexes des $\boldsymbol{u}^{c\ell}$ sont uniformément bornées. Comme le ratio entre une composante connexe et son parent dans l'arbre est un entier supérieur ou égal à 1, la suite des tailles des composantes connexes des $\boldsymbol{u}^{\boldsymbol{\ell}}$ est croissante (au sens large). On en déduit le résultat.
Montrons (iii) ⇒ (i) : comme la suite est bornée, il existe une taille de composante connexe qui apparaît infiniment souvent. Comme il n'y a qu'un nombre fini d'automates de taille fixée, il existe $i < j$ tels que $\rho_{\boldsymbol{vu}^i} = \rho_{\boldsymbol{vu}^j}$. Et donc $\rho_{\boldsymbol{u}}$ est d'ordre fini.
Montrons finalement (ii) ⇒ (iv) : la taille d'une composante connexe contenant $\boldsymbol{vu}^\ell$ ne peut pas être supérieure à $\Sigma^{|\boldsymbol{v}|}\,|\mathcal{C}(\boldsymbol{u}^{\boldsymbol{c}})|$. □

Cette proposition se comprend dans l'arbre de Schreier comme *l'ordre d'un élément* $\rho_{\boldsymbol{u}}, \boldsymbol{u} \in Q^*$ *est fini si et seulement si la suite des étiquettes sur le chemin des composantes connexes de l'automate contenant les puissances de* $\boldsymbol{u}$ *est ultimement stationnaire à* 1.

On voit que, si on connaissait parfaitement les étiquettes de l'arbre de Schreier d'un automate, alors on saurait dire si le groupe que l'automate engendre est fini et quels sont les éléments d'ordre infini, et donc si le groupe est un groupe infini de Burnside. Néanmoins le comportement de ces étiquettes est complexe, et, par exemple, il apparaît difficile de savoir si la suite des étiquettes d'un chemin est décroissante ou même ultimement constante égale à 1.
Pour surmonter cette difficulté, Klimann, Picantin et Savchuk se sont intéressés à des chemins particuliers de l'arbre de Schreier.

Définition 1.7 (arête superposable)

Soient e et f deux arêtes dans l'arbre de Schreier d'un automate de Mealy. On dit que f est *superposable* sur e si tout mot de $\perp(f)$ (sur les états $\mathcal{A}$) admet un mot d'état de $\perp(e)$ (sur les états $\mathcal{A}$) comme suffixe.

Clairement, si f est superposable sur e, alors e est plus proche de la racine que f dans l'arbre de Schreier. La condition de superposition est en fait, pour les automates réversibles, équivalente à une condition plus faible:

Lemme 1.8

Soient $\mathcal{A}$ un automate de Mealy réversible, et e et f deux arêtes dans l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$. S'il existe un mot dans $\perp(f)$ qui admet un mot dans $\perp(e)$ comme suffixe, alors f est superposable sur e.

Démonstration. Supposons $\boldsymbol{u} = \boldsymbol{vw} \in \perp(f)$ avec $\boldsymbol{w} \in \perp(e)$. Alors tout mot $\boldsymbol{u'} \in \perp(f)$ est suffixé par un mot de $\perp(e)$, car on a $\boldsymbol{u'} = \delta_{\boldsymbol{s}}(\boldsymbol{u}) = \delta_{\boldsymbol{s}}(\boldsymbol{vw}) = \delta_{\boldsymbol{s}}(\boldsymbol{v})\delta_{\rho_{\boldsymbol{v}}(\boldsymbol{s})}(\boldsymbol{w})$ et $\delta_{\rho_{\boldsymbol{v}}(\boldsymbol{s})}(\boldsymbol{w}) \in \perp(e)$. □

Un des intérêts des arêtes superposables est que si f est superposable sur e, alors comme on retrouve tous les suffixes de $\perp(f)$ dans $\perp(e)$, les manières de compléter un mot de $\top(f)$ en un mot de $\perp(f)$ fonctionnent également depuis $\top(e)$. De ce fait on a pour les étiquettes (la preuve est similaire à celle du lemme 1.8) :

Lemme 1.9

Soient e et f deux arêtes d'un arbre de Schreier. Si f est superposable sur e, alors l'étiquette de f est plus petite de celle de e.

Cette notion de superposition peut être étendue aux chemins :

Définition 1.10

Soient $\boldsymbol{e} = (e_i)_{i\in I}$ et $\boldsymbol{f} = (f_i)_{i\in I}$ deux chemins de même longueur (éventuellement infinie) d'un arbre de Schreier. Le chemin $\boldsymbol{f}$ est *superposable* sur le chemin $\boldsymbol{e}$ si, pour tout $i \in I$, l'arête f_i est superposable sur l'arête e_i.

Il est intéressant de relier les notions de superposabilité et de filiation :

Définition 1.11

Soient e et f deux arêtes d'un arbre de Schreier $\mathfrak{t}(\mathcal{A})$. On dit que f est un *enfant légitime* de e si e est son parent et que f est superposable sur e.

Définition 1.12 (Chemin auto-repliant)

Soient $\mathcal{A}$ un automate de Mealy réversible et $\mathfrak{s}$ un chemin ou sous-arbre (éventuellement infini) de $\mathfrak{t}(\mathcal{A})$. Pour $\ell > 0$, on dit que, $\mathfrak{s}$ est *ℓ-auto-repliable* si tout chemin de $\mathfrak{s}$ commençant au niveau $i + \ell$ est superposable sur un chemin de $\mathfrak{s}$ commençant au niveau i, pour tout $i \geq 0$. Un chemin ou sous-arbre est *auto-repliable* s'il est ℓ-auto-repliable pour un certain $\ell > 0$.

Ces chemins auto-repliants existent bel et bien : pour tout $\boldsymbol{u} \in Q^\ell$, le chemin représenté par $\boldsymbol{u}^\omega$ est ℓ-auto-repliant. En particulier, pour tout état $q \in Q$, la branche représentée par q^ω est un exemple de branche 1-auto-repliable.

Finalement, on donne un nom aux chemins dont les composantes connexes grossissent sans cesse.

Définition 1.13

Une branche dont l'étiquette n'est pas suffixée par 1^ω est dite *active*.

Le vocabulaire étant introduit, on peut réexprimer en partie la proposition 1.6 :

Théorème 1.14 ([67])

Le semi-groupe engendré par un automate inversible et réversible $\mathcal{A}$ possède un élément d'ordre infini si et seulement si l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$ admet une branche auto-repliante active.

Dans la suite on utilise cet arbre de Schreier pour prouver que certaines classes d'automates réversibles ne contiennent aucun automate engendrant un groupe de Burnside infini.D'autre part, l'arbre de Schreier est aussi utilisé dans [68], en addition d'une structure semblable, l'automate des orbites, pour étudier la torsion d'exemples spécifiques de groupes d'automate qui n'étaient pas traités dans [27] faute de moyens techniques.

2 Cas des automates non biréversibles

On se concentre dans cette section sur les automates de Mealy inversibles, réversibles mais non coréversibles. On sait que ces automates n'engendrent que des groupes infinis [1]. On montre qu'en plus, ces groupes possèdent des éléments d'ordre infini, et que ce ne sont donc pas des groupes de Burnside. Plus précisément, on prouve que, si l'automate est non-coréversible et connexe, alors tous les éléments du semi-groupe engendré sont d'ordre infini. Notons que les automates non-coréversibles constituent, à mesure que la taille de l'alphabet et/ou l'ensemble des états grandissent, la grande majorité des automates inversibles et réversibles. On obtient comme corollaire que, *génériquement*, les automates de Mealy inversibles et réversibles n'engendrent pas de groupes de Burnside infinis.

On utilise l'arbre de Schreier décrit dans la section précédente. On a besoin pour nos démonstrations des résultats suivants :

Lemme 2.1

Soient $\mathcal{A}$ et $\mathcal{B}$ deux automates de Mealy sur le même alphabet, et tels que $\mathcal{A}$ est connexe et réversible. Alors, pour toute composante connexe $\mathcal{C}$ de $\mathcal{A} \times \mathcal{B}$, tout état de $\mathcal{A}$ apparaît comme préfixe d'un élément de $\mathcal{C}$.

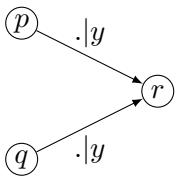
Démonstration. Prenons $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ et $\mathcal{C}$ une composante connexe de $\mathcal{A} \times \mathcal{B}$. Soient $pp' \in \mathcal{C}$ avec p un état de $\mathcal{A}$, p' un état de $\mathcal{B}$, et $q \in Q$ un état de $\mathcal{A}$. Comme $\mathcal{A}$ est connexe et réversible, il existe $\boldsymbol{s} \in \Sigma^*$ tel que $q = \delta_{\boldsymbol{s}}(p)$, donc q est un préfixe du mot $\delta_{\boldsymbol{s}}(pp')$ de $\mathcal{C}$. □

Ainsi la non-coréversibilité est conservée par produit :

Proposition 2.2

Soient $\mathcal{A}$ et $\mathcal{B}$ deux automates de Mealy réversibles sur le même alphabet. Si $\mathcal{A}$ est connexe et non-coréversible alors toutes les composantes connexes de $\mathcal{A} \times \mathcal{B}$ sont réversibles et non-coréversibles.

Démonstration. Soient Q l'ensemble des états de $\mathcal{A}$ et $\mathcal{C}$ une composante connexe de $\mathcal{A} \times \mathcal{B}$. Comme $\mathcal{A}$ et $\mathcal{B}$ sont réversibles, $\mathcal{C}$ l'est aussi (on compose juste les fonctions de production). Comme $\mathcal{A}$ n'est pas coréversible, il existe dans Q deux états distincts p et q qui mènent au même état $r \in Q$, en produisant la même lettre y :

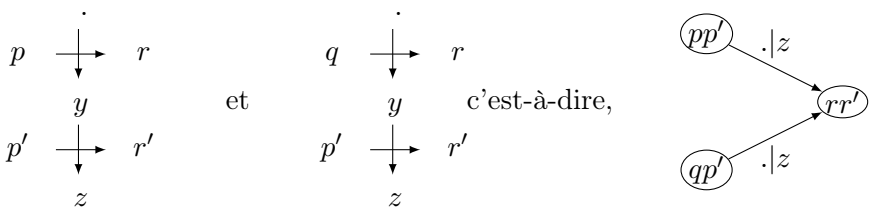


c'est-à-dire, $p \xrightarrow{y} r$ et $q \xrightarrow{y} r$.

Par le lemme 2.1, $\mathcal{C}$ contient un mot préfixé par p, disons pp'. Soit

$$p' \xrightarrow{y} r'$$

une transition de l'automate $\mathcal{B}$. Alors la configuration suivante apparaît dans $\mathcal{C}$:



ce qui témoigne de la non-coréversibilité de $\mathcal{C}$. □

Cette proposition est illustrée pour l'allumeur de réverbères figure II.3.

Pour l'arbre de Schreier on va utiliser :

Corollaire 2.3

Si un automate est (inversible) réversible et si toutes ses composantes connexes sont non-coréversibles, alors les composantes connexes de ses puissances sont toutes (inversibles) réversibles et non-coréversibles.

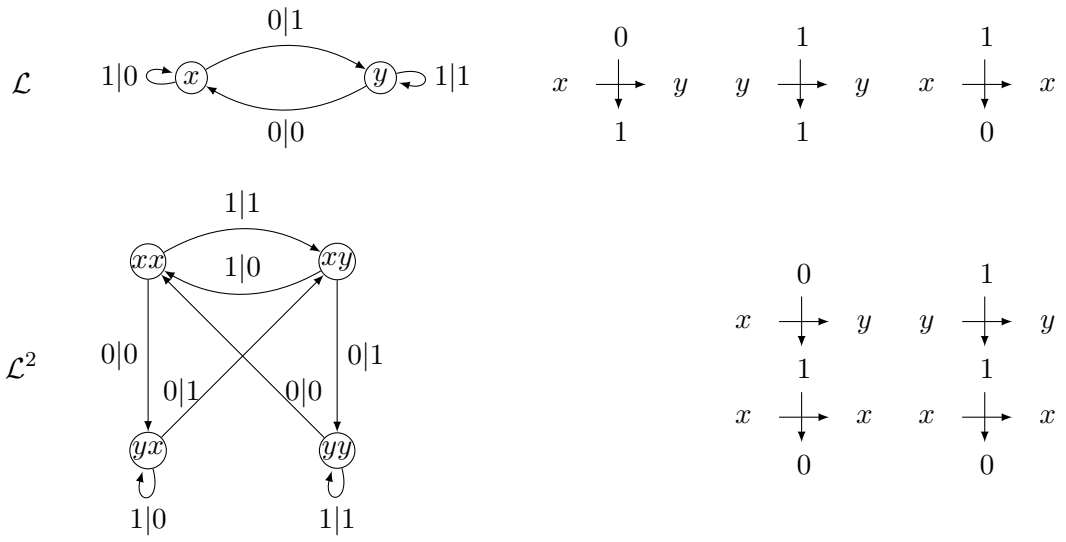


FIGURE II.3 – Un automate de l'allumeur de réverbères $\mathcal{L}$ inversible, réversible et non-coréversible et son carré, qui n'est pas non plus coréversible.

On peut maintenant montrer la proposition décisive pour cette section :

Proposition 2.4

Soit $\mathcal{A}$ un automate de Mealy connexe, inversible, réversible et non-coréversible. Un chemin 1-auto-repliant de l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$ ne peut pas contenir une arête étiquetée par 1.

Démonstration. Posons $\mathcal{A} = (Q, \Sigma, \delta, \rho)$, $\boldsymbol{e}$ un chemin 1-auto-repliant de $\mathfrak{t}(\mathcal{A})$ et e une arête de $\boldsymbol{e}$. Soit T (*resp.* L) l'ensemble des mots de $\top(e)$ (*resp.* de $\bot(e)$). Pour tout mot $\boldsymbol{w}$, $L_{\boldsymbol{w}} = \{\boldsymbol{u} \mid \boldsymbol{wu} \in L\}$ est le *quotient à gauche* de L par $\boldsymbol{w}$ (voir par exemple [87]).

Comme $\mathcal{A}$ est connexe et réversible, on peut appliquer le lemme 2.1, et, pour tout $p \in Q$, le quotient à gauche L_p est non-vide. On a donc

$$L = \bigsqcup_{p \in Q} pL_p \quad \text{(union disjointe).}$$

Comme $\boldsymbol{e}$ est 1-auto-repliable et $\mathcal{A}$ est inversible, on peut écrire

$$T = \bigcup_{p \in Q} L_p.$$

En effet, pour $p\boldsymbol{u} \in L$ avec $p \in Q$ (et $\boldsymbol{u} \in T$ par 1-auto-repliabilité) et $\boldsymbol{v} \in T$. Par réversibilité, il existe $\boldsymbol{s} \in \Sigma^*$ vérifiant $\delta_{\boldsymbol{s}}(\boldsymbol{u}) = \boldsymbol{v}$. Alors, par inversibilité, il existe $\boldsymbol{t} \in \Sigma^*$ avec $\rho_p(\boldsymbol{t}) = \boldsymbol{s}$:

$$\begin{array}{ccc} & \boldsymbol{t} & \\ p & \longrightarrow & \delta_{\boldsymbol{t}}(p) = p' \\ & \boldsymbol{s} & \\ \boldsymbol{u} & \longrightarrow & \delta_{\boldsymbol{s}}(\boldsymbol{u}) = \boldsymbol{v} \\ & \rho_{\boldsymbol{u}}(\boldsymbol{s}). & \end{array}$$

Ainsi, $\boldsymbol{v}$ est un suffixe de $\delta_{\boldsymbol{t}}(p\boldsymbol{u})$, donc $\boldsymbol{v} \in L_{p'}$ pour $p' = \delta_{\boldsymbol{t}}(x) \in Q$.

Comme $\mathcal{A}$ n'est pas coréversible, il existe $q, q', r \in Q$, $\quad q \neq q'$ et $x, y, z \in \Sigma^*$ qui satisfont

$$\begin{array}{ccc} & x & \\ q & \longrightarrow & r \\ & z & \end{array} \quad \text{et} \quad \begin{array}{ccc} & y & \\ q' & \longrightarrow & r \\ & z & \end{array} .$$

Donc, dans la composante connexe $\bot(e)$, on a

$$\delta_x(qL_q) = rL_r \quad \text{et} \quad \delta_y(q'L_{q'}) = rL_r.$$

De par la réversibilité de $\mathcal{A}$, δ_z est injective et on déduit $L_q = L_{q'}$. Comme $T = \bigcup_{q \in Q} L_q$ n'est pas une union disjointe $|T| < |L|$, ce qui signifie que l'étiquette de l'arête e, est strictement plus grande que 1. □

Comme chaque générateur $q \in Q$ définit une branche 1-auto-repliante q^ω en invoquant la proposition 1.6, on déduit immédiatement :

Proposition 2.5

Soit $\mathcal{A}$ un automate de Mealy connexe, inversible, réversible et non coréversible. Alors tout état de l'automate $\mathcal{A}$ induit une action d'ordre infini.

On peut d'ores et déjà montrer qu'on ne peut pas engendrer un groupe de Burnside, puisque le groupe contient des éléments d'ordre infini.

Théorème 2.6

Soit $\mathcal{A}$ un automate de Mealy connexe, inversible, réversible et non coréversible. Alors le groupe $\langle \mathcal{A} \rangle$ engendré par l'automate est infini mais n'est pas un groupe de Burnside.

Démonstration. Comme $\mathcal{A}$ n'est pas coréversible, il contient une composante connexe non-coréversible. On applique la proposition 2.5 à cette composante connexe (qui peut être vue comme un automate de Mealy connexe, inversible, réversible et non-coréversible), et on obtient que les états de cette composante sont d'ordre infini, ce qui implique l'infinitude du groupe et contredit la définition de groupe de Burnside. □

De plus, dans le semi-groupe, on peut montrer que si aucune composante n'est biréversible, alors aucun élément du semi-groupe n'est d'ordre fini :

Théorème 2.7

Soit $\mathcal{A}$ un automate de Mealy connexe, inversible, réversible et sans composante coréversible. Alors le semi-groupe $\langle \mathcal{A} \rangle_+$ engendré par l'automate est sans torsion.

Démonstration. Soit $\boldsymbol{u}$ un état de $\mathcal{A}^\ell$. On applique la proposition 2.5 à la composante connexe qui contient cet état et peut être vue comme un automate de Mealy connexe, inversible, réversible et non-coréversible de par le corollaire 2.3, et on conclut que $\rho_{\boldsymbol{u}}$ est d'ordre infini. □

D'autre part, toujours sur le semi-groupe, la proposition 2.4 permet d'obtenir :

Corollaire 2.8

Soit un automate de Mealy $\mathcal{A}$ à 2 ou 3 états, connexe, inversible, réversible et non-coréversible. Alors le groupe $\langle \mathfrak{d}\mathcal{A} \rangle$ agit transitivement par niveau.

Démonstration. Supposons au contraire qu'une puissance de $\mathcal{A}$ soit non connexe, et prenons ℓ le plus grand entier tel que $\mathcal{A}^\ell$ soit connexe. Alors, comme $|Q|$ une arête au moins de l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$ est étiquetée par 1 entre les niveaux ℓ et $\ell+1$ (voir la figure II.4). Cette arête se superpose sur la précédente, car $\mathcal{A}^\ell$ est connexe et contient donc tous les mots de taille ℓ. On a donc une arête sur un chemin 1-auto-repliant étiquetée par un 1, ce qui contredit la proposition 2.4. □

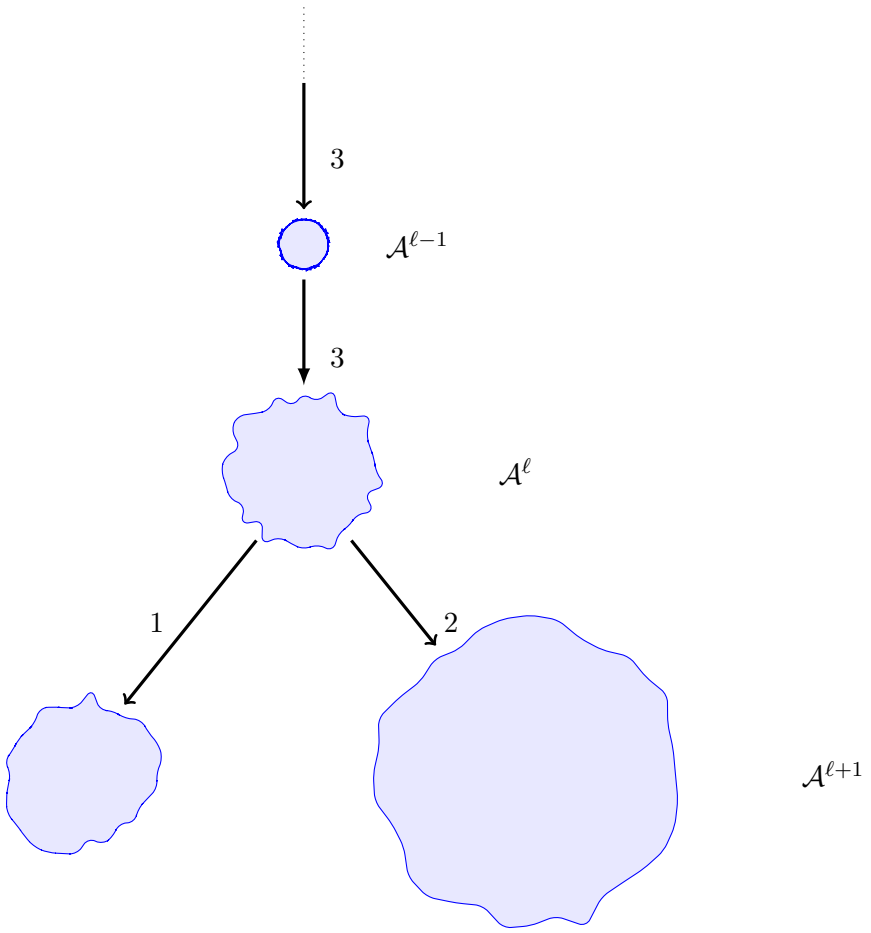


FIGURE II.4 – Un automate connexe, inversible, réversible et non-coreversible à trois états agit transitivement par niveau, sinon on trouverai un 1 dans l'arbre de Schreier.

On déduit de cela et de [63, Proposition 14] :

Corollaire 2.9

Un automate de Mealy à 2 ou 3 états, connexe, inversible, réversible et non-coréversible engendre un semi-groupe libre.

Par exemple, pour l'automate de Mealy $\mathcal{L}$ de la figure II.3, engendrant le groupe de l'allumeur de réverbères, le semi-groupe engendré $\langle\mathcal{L}\rangle_+$ est le monoïde libre de rang 2 (de base $\{x, y\}$).

Pour finir cette section, on va montrer que, génériquement, un automate inversible et réversible n'est pas biréversible, ce qui nous donnera de propriétés génériques sur les groupes engendrés par un automate inversible et réversible.

Pour cela, remarquons tout d'abord que si un automate inversible et réversible est biréversible, alors

$$\forall r \in Q, \forall i \neq j \in \Sigma,\ \rho_{\delta_i^{-1}(r)}(i) \neq \rho_{\delta_j^{-1}(r)}(j)\ .$$

En effet, chaque lettre de sortie ne peut arriver qu'une seule fois dans l'état r, voir figure II.5. Notons que l'on peut inverser δ par réversibilité de l'automate. De plus on peut effectuer le même raisonnement dans le dual et obtenir :

$$\forall i \in \Sigma, \forall p \neq q \in Q,\ \delta_{\rho_p^{-1}(i)}(p) \neq \delta_{\rho_q^{-1}(i)}(q)\ .$$

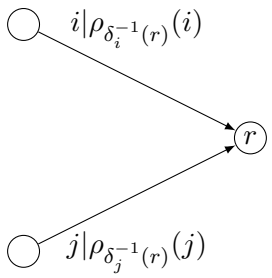


FIGURE II.5 – Dans un automate biréversible, pour tout état r et toutes lettres $i \neq j$, $\rho_{\delta_i^{-1}(r)}(i) \neq \rho_{\delta_j^{-1}(r)}(j)$.

On peut noter que le résultat du théorème 2.7 ne peut pas donner d'information supplémentaire quant à l'absence de torsion dans le groupe. Par exemple, prenons l'automate de Mealy $\mathcal{L}$ de la figure II.3 : l'action induite par yx^{-1} est d'ordre 2, et donc le groupe possède de la torsion.

À partir des voisins de r, on construit un tableau synthétisant les arêtes menant vers r, selon la lettre de sortie et l'état de provenance. La case p, j du tableau est cochée si $p \xrightarrow{i|j} r \in \mathcal{A}$ pour

une certaine lettre i. Des exemples de tels tableaux sont donnés figure II.6, pour l'automate représenté figure I.11.

lettre de sortie \ préd. de a	c	d	e
1			×
2		×	
3	×		

lettre de sortie \ préd. de b	a	c	f
1		×	×
2			
3	×		

FIGURE II.6 – Le tableau associé à l'état a (à gauche) et b (à droite) de l'automate non-biréversible de la figure I.11. On voit que pour l'état a il n'y a pas d'obstruction à la biréversibilité mais que pour l'état b la lettre (en sortie) 1 ne peut pas être un permutation de l'ensemble des états.

On voit que, pour que l'automate soit biréversible, chaque tableau associé à un état doit avoir exactement une case cochée par ligne. On dira alors que le tableau est *bien formé*. On va maintenant utiliser ce formalisme pour montrer :

Proposition 2.10

La probabilité qu'un automate inversible et réversible à k lettres et n états soit biréversible est majorée par

$$\frac{1}{n^{k-1}} + \frac{1}{k}$$

Démonstration. Fixons un état r, choisi uniformément dans l'automate. Notons T_r l'événement "le tableau associé à r est bien formé", et convenons que "prédécesseur de r" (abrégé "préd.") signifie "état admettant une transition menant vers r". On a :

$$\begin{aligned}\Pr(\mathcal{A} \in \mathrm{BIR}) &= \Pr(\mathcal{A} \in \bigcap_{r \in Q} T_r) \\ &\leq \Pr(T_r)\end{aligned}$$

D'après la formule des probabilités totales on a :

$$\begin{aligned}\Pr(\mathcal{A} \in \mathrm{BIR}) \leq{}& \Pr(T_r \mid r \text{ a 1 unique préd. }) \Pr(r \text{ a 1 unique préd.}) \quad + \\ & \Pr(T_r \mid r \text{ a au moins 2 préd.}) \Pr(r \text{ a au moins 2 préd.}) \\ \leq{}& \Pr(r \text{ a 1 unique préd.}) + \Pr(T_r \mid r \text{ a au moins 2 préd.})\end{aligned}$$

La probabilité que r ait exactement 1 prédécesseur revient à fixer un des $\delta_i^{-1}(r)$ pour une certaine lettre $i \in \Sigma$ et demander que les $k-1$ autres $\delta_j^{-1}(r)$, $j \in \Sigma \setminus \{i\}$ soient égaux à $\delta_i^{-1}(r)$, donc :

$$\Pr(\mathcal{A} \in \text{BIR}) \leq \frac{1}{n^{k-1}} + \Pr(T_r \mid \ r \text{ a au moins 2 préd.})$$

Fixons maintenant un prédécesseur p de r et posons λ le nombre de lettres menant de p vers r. Ce nombre λ est au plus $k-1$ et au moins 1. Il faut alors que les cases cochées dans la colonne de p soient compatibles (c'est-à-dire ne pas entrer en collision) avec celles des autres colonnes (événement noté C_p). Les autres colonnes doivent elles-mêmes ne pas présenter de collision (événement noté R_p). On peut encore une fois appliquer la formule des probabilité totales, en notant que $\Pr\left((T_r \mid \ r \text{ a au moins 2 préd.}) \mid R_p\right) = \Pr\left(C_p \mid R_p\right)$ et $\Pr\left((T_r \mid \ r \text{ a au moins 2 préd.}) \mid \overline{R_p}\right) = 0$

$$\begin{aligned}\Pr(\mathcal{A} \in \text{BIR}) &\leq \frac{1}{n^{k-1}} + \Pr(C_p \mid R_p)\Pr(R_p) \\ &\leq \frac{1}{n^{k-1}} + \Pr(C_p \mid R_p)\end{aligned}$$

Il faut donc que les $\lambda \geq 1$ lignes libres du tableau soient correctement remplies dans la colonne associée à p. On remarque que le "choix" des lignes correspond à l'image de lettres d'entrée $i_1, \dots i_\lambda$ selon ρ_p. Comme ρ_p est supposée être une permutation aléatoire, on peut oublier les lettres exactes et donc C_p revient à choisir l'unique configuration acceptable au sein des λ parmi k configuration possibles, d'où :

$$\begin{aligned}\Pr(\mathcal{A} \in \text{BIR}) &\leq \frac{1}{n^{k-1}} + \binom{\lambda}{k}^{-1} \\ &\leq \frac{1}{n^{k-1}} + \frac{1}{k}\,.\end{aligned}$$

□

La borne tend vers 0 quand k tend vers l'infini mais ne nous donne pas d'information quand le nombre de lettres k est fixé. Cependant on remarque que l'on peut faire le même raisonnement dans l'automate dual, ce qui échange le rôle des lettres et des états, et on obtient donc :

Théorème 2.11

La proportion d'automates de Mealy biréversibles parmi les inversibles réversibles tend vers 0 quand le nombre de lettres ou le nombre d'états tend vers l'infini.

On en déduit pour le problème de Burnside :

Corollaire 2.12

La probabilité qu'un automate de Mealy inversible et réversible engendre un groupe infini tend vers 1 quand le nombre d'états ou de lettre tend vers l'infini. La probabilité qu'un tel automate engendre un groupe de Burnside tend elle vers 0.

3 Cas des automates biréversibles, connexes et ayant un nombre premier d'états

On se penche maintenant sur le cas des automates biréversibles. Pour ces automates, Klimann, puis Klimann, Picantin et Savchuk ont montré respectivement que, si l'automate avait deux états [63] ou avait trois états et était connexe [67], alors le groupe engendré n'était jamais un groupe de Burnside infini. Dans cette section on généralise ce résultat au cas des automates connexes ayant un nombre *premier* d'états. On utilise là aussi l'arbre de Schreier, en mettant en place une mécanique permettant d'exprimer l'action induite par n'importe quel élément du groupe comme l'action induite par un mot appartenant à un sous-arbre connu. Cette boîte à outils est assez générale, et l'hypothèse de primalité n'intervient qu'au dernier pas de la démonstration, ce qui laisse espérer que les objets développés seront utiles pour montrer le cas général.

Dans cette section, on suppose que notre automate de Mealy est biréversible, connexe et n'a pas de branche auto-repliante active dans son arbre de Schreier (sinon on sait par le théorème 1.14 que le groupe engendré n'est pas de Burnside). On montre que, si cet automate a un nombre premier d'états, alors le groupe qu'il engendre est fini.

3.1 Arbres de la jungle, tiges et lianes

Pour arriver à nos fins, on s'intéresse aux chemins auto-repliants de l'arbre de Schreier, mais aussi de manière un peu plus générale à des sous-arbres auto-repliants :

Définition 3.1

Soit $\boldsymbol{e}$ un chemin fini 1-auto-repliant initial de $\mathfrak{t}(\mathcal{A})$ tel que
- $\perp(\boldsymbol{e})$ a au moins deux enfants légitimes ;
- tous les enfants légitimes de $\perp(\boldsymbol{e})$ ont 1 pour étiquette.

L'*arbre de la jungle* $\mathfrak{J}(\boldsymbol{e})$ de $\boldsymbol{e}$ est le sous-arbre de $\mathfrak{t}(\mathcal{A})$ construit comme suit :
- $\mathfrak{J}(\boldsymbol{e})$ contient le chemin $\boldsymbol{e}$ — son *tronc* ;
- $\mathfrak{J}(\boldsymbol{e})$ contient l'arbre régulier enraciné en $\perp(\boldsymbol{e})$ formé de toutes les arêtes descendantes de $\perp(\boldsymbol{e})$ qui sont superposables sur la dernière arête de $\boldsymbol{e}$.

L'*arité* de cet arbre est le nombre d'enfants légitimes de $\perp(\boldsymbol{e})$. Comme tous les enfants légitimes ont pour étiquette 1 et que $\boldsymbol{e}$ est 1-auto-repliant, cette arité est aussi égale à la dernière étiquette de $\boldsymbol{e}$.
Les mots de $\perp(\boldsymbol{e})$ sont appelés *tiges*. Ils ont tous la même longueur, qui est la longueur du tronc de $\mathfrak{J}(\boldsymbol{e})$.
Un arbre est un *arbre de la jungle* si c'est l'arbre de la jungle d'un chemin 1-auto-repliant fini initial.

On remarque que l'existence de tels arbres est assurée par l'existence d'un nombre fini non nul de chemins initiaux 1-auto-repliants (lemme 4.1) et l'hypothèse faite sur l'absence de branche active : il existe donc un chemin actif qui fini par se scinder en branches auto-repliantes non actives. De plus, par le même lemme 4.1, on obtient qu'il n'existe qu'un nombre fini d'arbre de la jungle.

Un arbre de la jungle se présente comme un chemin initial qui débouche finalement sur un arbre régulier dont toutes les étiquettes valent 1. De plus, tout arbre de la jungle est 1-auto-repliant, ce qui signifie entre autres que si on "remonte" l'arbre en oubliant la première lettre, on obtient encore un arbre de la jungle.

Définition 3.2

Soient $\mathcal{A}$ un automate de Mealy réversible et $\mathfrak{T}$ un sous-arbre de l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$ incluant la racine. Un $\mathfrak{T}$-*mot* est un mot dans $Q^* \sqcup Q^\omega$ représentant un chemin initial de $\mathfrak{T}$. Un $\mathfrak{T}$-*mot cyclique* est un mot dans Q^* dont toutes les puissances sont des $\mathfrak{T}$-mots.

On considère maintenant un arbre de la jungle $\mathfrak{J}$ de $\mathcal{A}$, dont le tronc est de longueur λ. Remarquons que, grâce à la propriété d'1-auto-repliabilité de $\mathfrak{J}$, tout facteur d'un $\mathfrak{J}$-mot est lui-

même un $\mathfrak{J}$-mot. De plus, par construction, toutes les tiges appartiennent à la même composante connexe.

Dans cet arbre, les $\mathfrak{J}$-mots cycliques induisent des actions d'ordres finis, car l'arbre ne contient que des 1 à partir d'un certain niveau par la proposition 1.4, mais on peut surtout borner cet ordre par une constante ne dépendant que de $\mathfrak{J}$:

Lemme 3.3

Tout $\mathfrak{J}$-mot cyclique induit une action d'ordre fini dans le groupe. De plus, cet ordre est inférieur à $|Q|^{\lambda|\Sigma|^{|\Sigma|}}$.

Démonstration. Comme $\mathfrak{J}$ n'a que des étiquettes 1 après le niveau λ, toutes les composantes connexes de $\mathfrak{J}$ en-dessous de ce niveau sont de même taille. Cette taille est au plus $|Q|^{\lambda}$, et on a donc au maximum $|Q|^{\lambda|\Sigma|^{|\Sigma|}}$ automates différents dans $\mathfrak{J}$ après le niveau λ. Pour tout $\mathfrak{J}$-mot $\boldsymbol{u}$ cyclique, il existe un exposant $\ell \leq |Q|^{\lambda|\Sigma|^{|\Sigma|}}$ tel que $\rho_{\boldsymbol{u}} = \rho_{\boldsymbol{u}^\ell}$, donc $\rho_{\boldsymbol{u}}$ est d'ordre fini, borné par $|Q|^{\lambda|\Sigma|^{|\Sigma|}}$. □

L'intérêt des $\mathfrak{J}$-mots est que l'on peut facilement en comprendre la structure après le niveau λ :

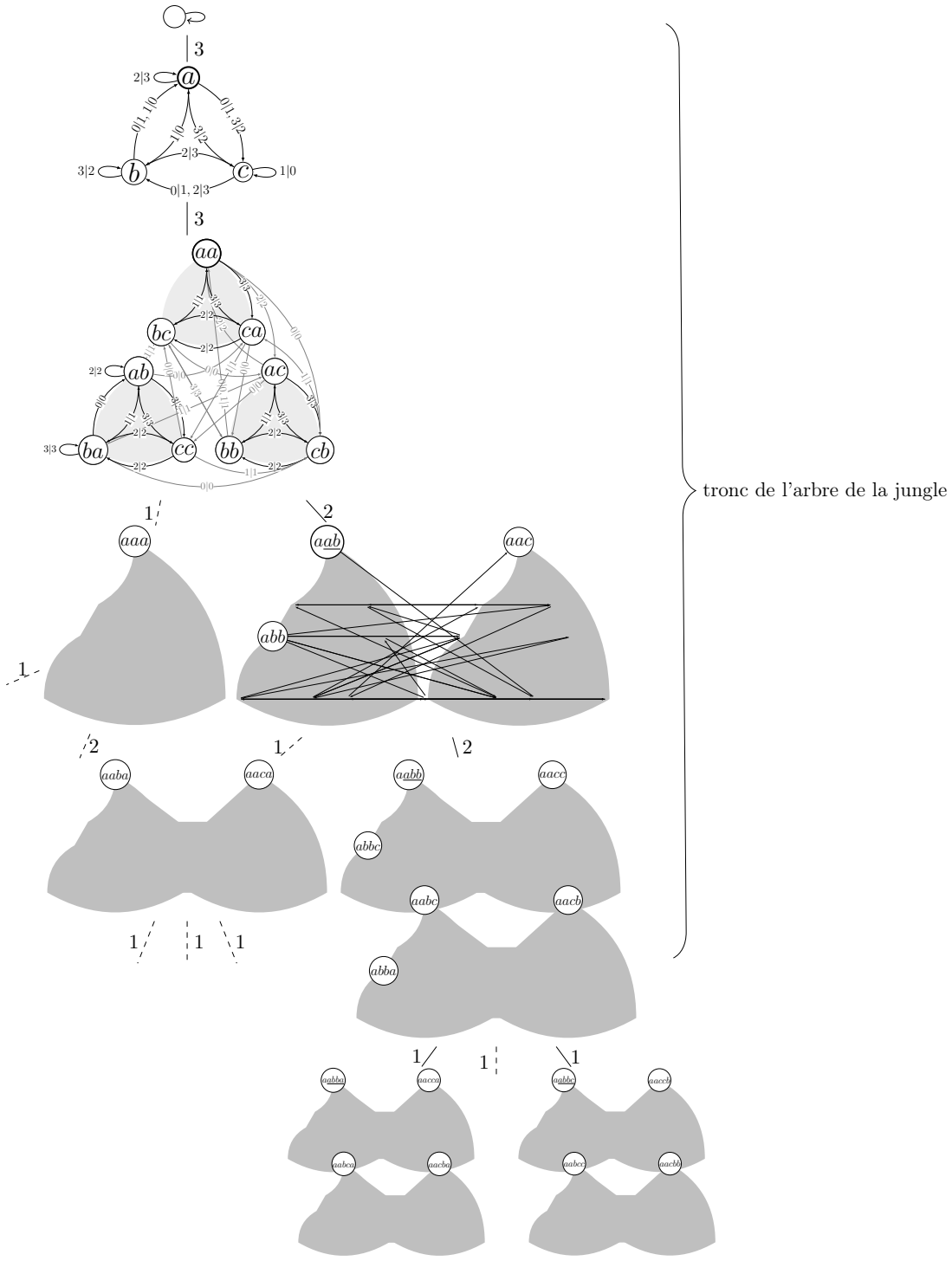


FIGURE II.7 – Un exemple des premiers niveaux de l'arbre de Schreier (tous les sommets et arêtes) dont on extrait un arbre de la jungle (arêtes pleines). Ici $\lambda = 4$ et l'arité vaut 2.

Lemme 3.4

Soit $\boldsymbol{uv}$ un $\mathfrak{J}$-mot, avec $|\boldsymbol{v}| \geq \lambda$, alors les mots $\boldsymbol{w} \in Q^*$ tels que $\boldsymbol{uvw}$ est un $\mathfrak{J}$-mot ne dépendent que de $\boldsymbol{v}$, *i.e.*

$$\{\boldsymbol{w} \mid \boldsymbol{uvw} \text{ est un } \mathfrak{J}\text{-mot}\} = \{\boldsymbol{w} \mid \boldsymbol{vw} \text{ est un } \mathfrak{J}\text{-mot}\}\,.$$

Remarquons aussi que l'existence de $\mathfrak{J}$-mots cyclique est assurée. En effet si l'on prend un $\mathfrak{J}$-mot $\boldsymbol{u}$ de taille $\lambda\,|Q|^\lambda + \lambda$, c'est-à-dire la concaténation de $|Q|^\lambda + 1$ mots de taille λ, alors on est sûr qu'un mot $\boldsymbol{v}$ de taille λ y est répété. On a $\boldsymbol{u} = \boldsymbol{w}_p\boldsymbol{vwvw}_s$, et d'après le lemme 3.4, $(\boldsymbol{vw})^\omega$ est un $\mathfrak{J}$-mot, et donc $\boldsymbol{vw}$ est un $\mathfrak{J}$-mot cyclique.

Attachons-nous maintenant à décrire les mots qu'on peut lire dans l'arbre de la jungle une fois que l'on a fixé un représentant du tronc.

Définition 3.5

Soit $\mathfrak{J}$ un arbre de la jungle dont le tronc est de taille λ. Une *liane couvrant* $\mathfrak{J}$ est un langage de $\mathfrak{J}$-mots de la forme $\boldsymbol{w}L_{\boldsymbol{w}}$, où $\boldsymbol{w} \in Q^\lambda$ est une tige et $L_{\boldsymbol{w}} \subseteq Q^* \sqcup Q^\omega$ est un langage stable par préfixe qui, vu comme un arbre, a la même arité que $\mathfrak{J}$.
Chaque sommet de $\mathfrak{J}$ possède exactement un représentant dans $\boldsymbol{w}L_{\boldsymbol{w}}$, et pour chaque tige $\boldsymbol{w}$, il y a exactement un langage $L_{\boldsymbol{w}}$ qui satisfait ces propriétés.

Remarque 3.6

Soit $\boldsymbol{w}L_{\boldsymbol{w}}$ une liane couvrant un arbre de la jungle $\mathfrak{J}$ et soit $\boldsymbol{uv}$ un $\mathfrak{J}$-mot fini, avec $|\boldsymbol{v}| = \lambda$. Si $L_{\boldsymbol{v}}$ est le langage maximal tel que $\boldsymbol{uv}L_{\boldsymbol{v}} \subseteq \boldsymbol{w}L_{\boldsymbol{w}}$, alors $\boldsymbol{v}L_{\boldsymbol{v}}$ est aussi une liane couvrant $\mathfrak{J}$.

Une des propriétés des lianes qui est centrale dans la suite est que, si $\boldsymbol{uv} \in Q^*$ est un facteur dans une liane $\boldsymbol{q}L_{\boldsymbol{q}}$, alors $\boldsymbol{u}$ se retrouve plus loin dans $\boldsymbol{q}L_{\boldsymbol{q}}$.

Théorème 3.7

Soient $\boldsymbol{q} \in Q^*$ un chemin auto-repliant initial et $\boldsymbol{u}$ un facteur dans $\boldsymbol{q}L_{\boldsymbol{q}}$. Alors $\boldsymbol{u}$ a la propriété suivante :

Si $\boldsymbol{puv} \in \boldsymbol{q}L_{\boldsymbol{q}}$, alors il existe $\boldsymbol{w} \in Q^*$ tel que $\boldsymbol{puvwu} \in \boldsymbol{q}L_{\boldsymbol{q}}$. (**Ubiquité**)

Démonstration. Tout d'abord, rappelons que, si $\boldsymbol{u}$ est une tige (*i.e.* $\boldsymbol{u}$ est un facteur de $\boldsymbol{q}L_{\boldsymbol{q}}$ de taille λ), ce qui peut suivre $\boldsymbol{u}$ (dans $\boldsymbol{q}L_{\boldsymbol{q}}$) ne dépend ni de la liane, ni de la localisation de $\boldsymbol{u}$ dans cette liane. Il est donc suffisant de prouver le théorème uniquement pour les mots de longueur λ.

On commence par montrer qu'il existe une tige $\boldsymbol{u}_0$ qui satisfait la propriété (**Ubiquité**). Pour cela, on se déplace le long de la liane $\boldsymbol{q}L_{\boldsymbol{q}}$ comme suit : on part de $\boldsymbol{u}_0 = \boldsymbol{q}$

- si $\boldsymbol{u}_0$ satisfait la propriété (**Ubiquité**), on s'arrête là ;
- sinon, après la tige $\boldsymbol{u}_0$, on suit un chemin fini tel que $\boldsymbol{u}_0$ n'existe plus jamais après ce chemin ; on remplace alors $\boldsymbol{u}_0$ par le mot de taille λ suivant dans la liane $\boldsymbol{q}L_{\boldsymbol{q}}$, et on itère le processus.

Comme $\boldsymbol{q}L_{\boldsymbol{q}}$ est infinie mais ne contient qu'un nombre fini de facteurs de taille λ, l'algorithme renvoie bien une tige $\boldsymbol{u}_0$ qui satisfait la propriété (**Ubiquité**). De par la remarque 3.6, l'arbre de la jungle $\mathfrak{J}$ est couvert par une liane de la forme $\boldsymbol{u}_0 L_{\boldsymbol{u}_0}$.

Montrons à présent que toutes les tiges satisfont la propriété (**Ubiquité**).

Soit $\boldsymbol{uv}$ un facteur dans la liane, avec $|\boldsymbol{u}| = \lambda$. Comme $\boldsymbol{u}$ est une tige, $\boldsymbol{u}_0$ et $\boldsymbol{u}$ sont dans la même composante connexe, et il existe un chemin de $\boldsymbol{u}_0$ vers $\boldsymbol{u}$, par exemple par l'action induite par $\boldsymbol{s} \in \Sigma^*$. Comme l'automate est réversible, $\boldsymbol{v}$ est l'image d'un certain $\boldsymbol{v}_0 \in Q^{|\boldsymbol{v}|}$ par $\boldsymbol{t} = \delta_{\boldsymbol{u}_0}(\boldsymbol{s})$.

Mais alors, on sait que, dans la partie gauche de la figure II.8, on peut retrouver $\boldsymbol{u}_0$, après avoir lu un certain mot $\boldsymbol{w}_0$ (car $\boldsymbol{u}_0$ possède la propriété (**Ubiquité**)). Or, par inversibilité de l'automate, il existe une certaine puissance $(\boldsymbol{u}_0\boldsymbol{v}_0\boldsymbol{w}_0)^\alpha$ dont l'action stabilise $\boldsymbol{s}$ (voir encore la figure II.8).

Ainsi $\boldsymbol{u}$ peut être revu car $\rho_{\boldsymbol{u}_0\boldsymbol{v}_0\boldsymbol{w}_0)^\alpha}(\boldsymbol{s}) = \boldsymbol{s}$ et donc $\delta_{\boldsymbol{s}}\left((\boldsymbol{u}_0\boldsymbol{v}_0\boldsymbol{w}_0)^\alpha \boldsymbol{u}_0\right) = \delta_{\boldsymbol{s}}(\boldsymbol{u}_0) = \boldsymbol{u}$. De plus, le mot sur la droite de la figure II.8 est bien un $\mathfrak{J}$-mot, car il est dans la même composante que le $\mathfrak{J}$-mot $(\boldsymbol{u}_0\boldsymbol{v}_0\boldsymbol{w}_0)^\alpha$, sur la gauche de cette figure. La tige $\boldsymbol{u}$ satisfait donc bien la propriété (**Ubiquité**). □

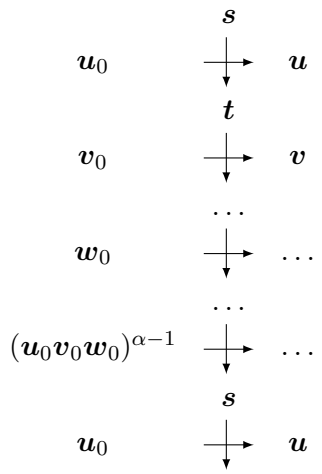


FIGURE II.8 – Extension de la propriété (**Ubiquité**) à n'importe quelle tige.

3.2 Équivalences et combinatoire sur les tiges

On définit maintenant des équivalences sur les tiges, qui permettent de construire, à partir d'un mot d'états quelconque, un mot de la jungle ayant la même action sur Σ^*.

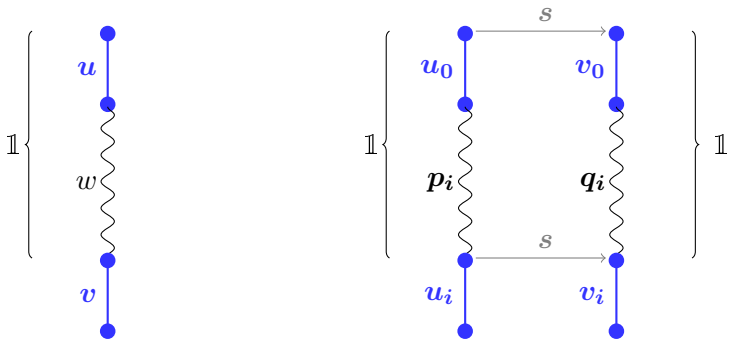
Définition 3.8

La relation $\sim$ sur l'ensemble des tiges d'un arbre de la jungle $\mathfrak{J}$ est définie par :
$\boldsymbol{u} \sim \boldsymbol{v}$ s'il existe $\boldsymbol{w} \in Q^*$ tel que $\boldsymbol{uwv}$ est un $\mathfrak{J}$-mot et $\rho_{\boldsymbol{uw}}$ agit comme l'identité sur Σ^*.

On a :

Lemme 3.9

La relation $\sim$ est une relation d'équivalence sur l'ensemble des tiges d'un arbre de la jungle $\mathfrak{J}$.



(A) Tiges équivalentes $u \sim v$.

(B) Les classes d'équivalence selon $\sim$ ont la même taille.

FIGURE II.9 – Equivalence $\sim$ sur l'ensemble des tiges d'un arbre de la jungle.

Démonstration. Soient u et v deux tiges de $\mathfrak{J}$.

transitivité Supposons $u \sim v$ et $v \sim w$. Il existe $p, q \in Q^*$ tels que upv et vqw sont des $\mathfrak{J}$-mots, et ρ_{up} et ρ_{vq} agissent comme l'identité. Comme v est une tige, on obtient par le lemme 3.4 que $upvqw$ est un $\mathfrak{J}$-mot, et ρ_{upvq} agit comme l'identité, d'où $u \sim w$.

réflexivité D'après le théorème 3.7, il existe $w \in Q^*$ tel que uwu est un $\mathfrak{J}$-mot. Comme u est une tige, $uwuw$ est aussi un $\mathfrak{J}$-mot, de même que toutes les puissances de uw. Or, de par les hypothèses et le théorème 1.14, uw induit une action d'ordre fini, disons α: $u(wu)^{\alpha-1}wu$ est un $\mathfrak{J}$-mot et $\rho_{u(wu)^{\alpha-1}w} = \rho_{(uw)^\alpha}$ agit comme l'identité.

symétrie Supposons que $u \sim v$: il existe $w \in Q^*$ tel que uwv est un $\mathfrak{J}$-mot et ρ_{uw} agit comme l'identité. Par la réflexivité de $\sim$, il existe $q \in Q^*$ tel que $uwvqu$ est un $\mathfrak{J}$-mot et ρ_{uwvq} agit comme l'identité. Alors $\rho_{vq} = \rho_{uw}^{-1}\rho_{uwvq}$ agit comme l'identité et vqu est un $\mathfrak{J}$-mot, ce que achève la preuve.

□

Remarquons que, grâce à la réflexivité de $\sim$ et le théorème 3.7, si u et v sont des tiges $\sim$-équivalentes et uw est un $\mathfrak{J}$-mot, pour un certain $w \in Q^*$, alors il existe $q \in Q^*$ tel que $uwqv$ est un $\mathfrak{J}$-mot et ρ_{uwq} agit comme l'identité. Ainsi, non seulement v *peut être atteint depuis* u *tout en produisant l'identité dans le groupe*, mais même en descendant dans l'arbre de la jungle $\mathfrak{J}$ après avoir lu le mot u, on peut encore atteindre le mot v en produisant l'identité.

On étudie les classes d'équivalences selon $\sim$. On cherche à montrer que, pour tout état $q \in Q$ et pour toute classe selon $\sim$, il existe dans la classe une tige préfixée par q. On y parvient dans le cas où l'automate a un nombre premier d'états.

Proposition 3.10

Toutes les $\sim$-classes de tiges d'un arbre de la jungle $\mathfrak{J}$ sont de même taille.

Démonstration. Cette démonstration est illustrée figure II.9B. Soient $\boldsymbol{u}_0$ et $\boldsymbol{v}_0$ deux tiges de $\mathfrak{J}$: ce sont des éléments de la même composante connexe, et il existe donc $\boldsymbol{s} \in \Sigma^*$ tel que $\delta_{\boldsymbol{s}}(\boldsymbol{u}_0) = \boldsymbol{v}_0$. Notons $\{\boldsymbol{u}_0, \dots, \boldsymbol{u}_k\}$ la $\sim$-classe de $\boldsymbol{u}_0$. Pour $1 \leq i \leq k$, il existe $\boldsymbol{p}_i \in Q^*$ tel que $\boldsymbol{u}_0\boldsymbol{p}_i\boldsymbol{u}_i$ est un $\mathfrak{J}$-mot et $\rho_{\boldsymbol{u}_0\boldsymbol{p}_i}$ agit comme l'identité. Soient $\boldsymbol{v}_i \in Q^{|\boldsymbol{u}_i|}$ et $\boldsymbol{q}_i \in Q^{|\boldsymbol{p}_i|}$ définis de la manière suivante : $\delta_{\boldsymbol{s}}(\boldsymbol{u}_0\boldsymbol{p}_i\boldsymbol{u}_i) = \boldsymbol{v}_0\boldsymbol{q}_i\boldsymbol{v}_i$. Notons que $\boldsymbol{v}_0\boldsymbol{q}_i\boldsymbol{v}_i$ est également un $\mathfrak{J}$-mot car c'est l'image d'un $\mathfrak{J}$-mot. Notons maintenant que $\rho_{\boldsymbol{v}_0\boldsymbol{q}_i}$ agit comme l'identité, par la réversibilité de $\mathcal{A}$, et donc $\boldsymbol{v}_i$ est $\sim$-équivalente à $\boldsymbol{v}_0$. De plus, comme $\rho_{\boldsymbol{u}_0\boldsymbol{p}_i}$ agit comme l'identité, on a $\boldsymbol{v}_i = \delta_{\boldsymbol{s}}(\boldsymbol{u}_i)$, et comme $\delta_{\boldsymbol{s}}$ est une permutation, les $\boldsymbol{v}_i$ sont 2 à 2 distincts. □

Fixons un arbre de la jungle $\mathfrak{J}$ et supposons que les étiquettes du tronc de $\mathfrak{J}$ sont $n_1, n_2, \dots, n_\lambda$ (numérotées depuis la racine vers le bas). Notons que, si l'automate est connexe, alors $n_1 = |Q|$, et que par construction de l'arbre de la jungle, $n_\lambda \geq 2$. Par exemple, pour l'arbre de la figure II.7, on a $\lambda = 4$, $n_1 = n_2 = 3$, et $n_3 = n_4 = 2$.

Dans un premier temps, on peut compter les tiges ayant un préfixe donné, sans plus de restriction :

Lemme 3.11

Le nombre de tiges ayant un préfixe donné ne dépend que de la taille i de ce préfixe et des étiquettes $n_{i+1}, n_{i+2}, \dots, n_{\lambda-1}$ et n_λ dans l'arbre de la jungle.

Démonstration. Par définition des étiquettes, n_{i+1} est le nombre de façons de compléter un mot dans une composante connexe. L'indépendance vis-à-vis du choix de la classe vient de la réversibilité, comme dans le lemme 1.2. □

Soit $\boldsymbol{u}$ un $\mathfrak{J}$-mot de taille strictement inférieure à λ. On peut aussi se poser deux questions en quelque sorte duales.
Premièrement, si $\boldsymbol{u}$ est vu comme le préfixe de tiges dans une $\sim$-classe, de combien de façons $\boldsymbol{u}$ peut-il être complété en une tige de cette classe d'équivalence (proposition 3.12) ?
Deuxièmement, dans combien de $\sim$-classes $\boldsymbol{u}$ est-il le préfixe d'une tige (corollaire 3.18) ?

Proposition 3.12

Soit $\boldsymbol{u}$ un $\mathfrak{J}$-mot de taille inférieure à λ. Fixons une $\sim$-classe γ qui contient une tige préfixée par $\boldsymbol{u}$, et un entier i tel que $|\boldsymbol{u}| + i \leq \lambda$. Alors le nombre de mots $\boldsymbol{v} \in Q^i$ tels que $\boldsymbol{uv}$ soit le préfixe d'une tige de γ ne dépend que de $|\boldsymbol{u}|$ et i.

Démonstration. Par les mêmes arguments que la proposition 3.10. □

Soit $\boldsymbol{u} \in Q^*$ le préfixe d'une tige dans une $\sim$-classe γ donnée. On note $\mathcal{S}_{|\boldsymbol{u}|+1}$ le cardinal de l'ensemble $\{q \in Q \mid \boldsymbol{u}q$ est le préfixe d'une tige dans $\gamma\}$ (de par la proposition proposition 3.12, ceci ne dépend que de $|\boldsymbol{u}|$ et pas de γ).

Pour obtenir une borne sur la taille de ces $\sim$-classes, on introduit une nouvelle relation d'équivalence sur les tiges, dont on prouvera (lemme 3.14) qu'elle est plus fine que la relation $\sim$.

Définition 3.13

La relation $\wedge_0$ sur l'ensemble des tiges d'un arbre de la jungle $\mathfrak{J}$ est définie par :

$\boldsymbol{u} \wedge_0 \boldsymbol{v}$ s'il existe une tige $\boldsymbol{w}$ telle que $\boldsymbol{wu}$ et $\boldsymbol{wv}$ sont des $\mathfrak{J}$-mots.

On définit la relation d'équivalence $\wedge$ comme la clôture transitive de $\wedge_0$.

Cette relation est illustrée figure II.10.

Par construction de l'arbre de la jungle, le nombre de tiges en $\wedge_0$-relation avec une tige $\boldsymbol{u}$ fixée est n_λ^λ, où $n_\lambda \geq 2$ est l'arité de l'arbre de la jungle.

Lemme 3.14

La relation $\wedge$ est plus fine que la relation $\sim$: $\boldsymbol{u} \wedge \boldsymbol{v} \Rightarrow \boldsymbol{u} \sim \boldsymbol{v}$.

Démonstration. Par transitivité, il nous suffit de montrer que $\boldsymbol{u} \wedge_0 \boldsymbol{v} \Rightarrow \boldsymbol{u} \sim \boldsymbol{v}$. Soient $\boldsymbol{u}$ et $\boldsymbol{v}$ deux tiges avec $\boldsymbol{u} \wedge_0 \boldsymbol{v}$: il existe une tige $\boldsymbol{w}$ telle que $\boldsymbol{wu}$ and $\boldsymbol{wv}$ sont des $\mathfrak{J}$-mots. Par le théorème 3.7, il existe un mot $\boldsymbol{q} \in Q^*$ tel que $\boldsymbol{uqw}$ est un $\mathfrak{J}$-mot. Comme $\boldsymbol{u}$ et $\boldsymbol{w}$ sont des tiges, et que $\boldsymbol{wu}$ est un $\mathfrak{J}$-mot, $(\boldsymbol{uqw})^2$ est aussi un $\mathfrak{J}$-mot, par le lemme 3.4, ainsi que toutes les puissances de $\boldsymbol{uqw}$. Alors, par le théorème 1.14, le mot $\boldsymbol{uqw}$ induit une action d'ordre fini, disons α : $(\boldsymbol{uqw})^\alpha \boldsymbol{v}$ est donc un $\mathfrak{J}$-mot et $\rho_{(\boldsymbol{uqw})^\alpha}$ agit comme l'identité, on a donc $\boldsymbol{u} \sim \boldsymbol{v}$. □

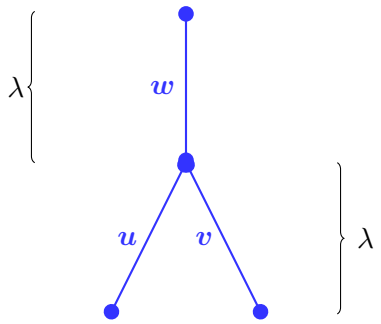


FIGURE II.10 – Tiges satisfaisant la relation $\boldsymbol{u} \wedge_0 \boldsymbol{v}$

Par conséquent :

Lemme 3.15

Pour tout i, on a $\mathcal{S}_i \geq 2$.

Démonstration. Pour une tige $\boldsymbol{u}$, l'ensemble des tiges en $\wedge_0$-relation avec $\boldsymbol{u}$, vu comme un arbre, a la même arité que l'arbre de la jungle $\mathfrak{J}$; Donc, par le lemme 3.14, pour tout i, $\mathcal{S}_i$ est supérieur à l'arité de $\mathfrak{J}$. □

Il est possible de se montrer plus précis :

Proposition 3.16

La suite $(\mathcal{S}_i)_i$ est décroissante et minorée par n_λ, l'étiquette de la dernière arête du tronc de l'arbre de la jungle.

Démonstration. Montrons que $\mathcal{S}_i \geq \mathcal{S}_{i+1}$. Considérons $p\boldsymbol{u}$ un mot de la jungle, avec $p \in Q$ et $\boldsymbol{u} \in Q^{i-1}$. Il existe $\mathcal{S}_{i+1}$ états q_j tels que les $p\boldsymbol{u}q_j$ soient des mots de la jungle équivalents. Donc pour chaque j, il existe v_j tel que les $p\boldsymbol{u}q_j\boldsymbol{v}_j$ soient des tiges $\sim$-équivalentes. Soit r_ℓ un état tel que $p\boldsymbol{u}q_\ell\boldsymbol{v}_\ell r_\ell$ soit un $\mathfrak{J}$-mot (il en existe au moins un par construction de l'arbre de la jungle). Par la réflexivité de l'équivalence $\sim$ et le théorème 3.7, il existe $\boldsymbol{w}_{j,\ell} \in Q^*$ tel que $p\boldsymbol{u}q_j\boldsymbol{v}_j r_j \boldsymbol{w}_{j,\ell} p\boldsymbol{u}q_\ell\boldsymbol{v}_\ell$ soit un $\mathfrak{J}$-mot et $\rho_{p\boldsymbol{u}q_j\boldsymbol{v}_j r_j \boldsymbol{w}_{j,\ell}} = \mathbb{1}$. Alors, comme $p\boldsymbol{u}q_\ell\boldsymbol{v}_\ell$ est une tige, $p\boldsymbol{u}q_j\boldsymbol{v}_j r_j \boldsymbol{w}_{j,\ell} p\boldsymbol{u}q_\ell\boldsymbol{v}_\ell r_\ell$ est un $\mathfrak{J}$-mot et $\rho_{\boldsymbol{u}q_j\boldsymbol{v}_j r_j \boldsymbol{w}_{j,\ell} p} = \mathbb{1}$, et donc $\boldsymbol{u}q_j v_j r_j \sim \boldsymbol{u}q_\ell v_\ell r_\ell$, pour tout j, et le cardinal de l'ensemble $\{q \in Q \mid \boldsymbol{u}q$ est le préfixe d'une tige dans la $\sim$classe de $\boldsymbol{u}q_\ell v_\ell r_\ell\}$ est supérieur à $\mathcal{S}_{i+1}$.
Comme $\mathcal{S}$ ne dépend pas du choix du préfixe ni de la classe d'équivalence, on conclut $\mathcal{S}_i \geq \mathcal{S}_{i+1}$. □

On considère maintenant la deuxième question :

Proposition 3.17

Soit $\boldsymbol{u}$ un $\mathfrak{J}$-mot de longueur inférieure à λ. Le nombre des tiges préfixées par $\boldsymbol{u}$ dans une $\sim$-classe est 0 ou ne dépend que $|\boldsymbol{u}|$.

Démonstration. On utilise les même arguments que dans la proposition 3.10. □

Des propositions 3.12 et 3.17 on obtient :

Corollaire 3.18

Soit $\boldsymbol{u}$ un $\mathfrak{J}$-mot de longueur inférieure à λ. Le nombre de $\sim$-classes contenant une tige préfixée par $\boldsymbol{u}$ dépend seulement de $|\boldsymbol{u}|$.

On note $\mathcal{P}_{|\boldsymbol{u}|+1}$ le nombre de $\sim$-classes contenant une tige préfixée par $\boldsymbol{u}$ (qui ne dépend que de $|\boldsymbol{u}|$ d'après le corollaire 3.18).

On peut maintenant démontrer :

Théorème 3.19

Soit $\mathcal{A}$ un automate connexe et biréversible ayant un nombre premier d'états et sans branche auto-repliante active dans son arbre de Schreier $\mathfrak{t}(\mathcal{A})$. Alors, si on fixe une $\sim$-classe, l'ensemble des états qui apparaissent comme la première lettre d'une tige dans cette classe est égal à l'ensemble des états.

$$\text{Pour toute tige } \boldsymbol{u}, \{q \in Q, \exists \boldsymbol{v} \text{ une tige préfixée par } q \text{ et } \boldsymbol{u} \sim \boldsymbol{v}\} = Q\,.$$

Démonstration. Posons $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ avec $|Q| = p$ premier. Soit $\mathfrak{J}$ un arbre de la jungle dans $\mathfrak{t}(\mathcal{A})$ dont le tronc $\boldsymbol{e}$ est de taille λ, et est étiqueté par $n_1, \ldots, n_\lambda$ (du haut vers le bas). L'automate étant connexe, on a $n_1 = p$.
Soient γ une $\sim$-classe sur l'ensemble des tiges de $\mathfrak{J}$ et $\boldsymbol{u} \in Q^i$ le préfixe d'une tige de γ ($i \leq \lambda$). Considérons toutes les tiges de γ ayant pour préfixe $\boldsymbol{u}$. Par le lemme 3.11, leur nombre vaut exactement $n_{i+1} \times n_{i+2} \times \cdots \times n_\lambda$. C'est aussi le nombre de tiges préfixées par $\boldsymbol{u}$ dans une $\sim$-classe

γ multiplié par le nombre de $\sim$-classes de γ qui ont $\boldsymbol{u}$ comme préfixe. Ainsi, par double-comptage et pour tout i, on a

$$n_{i+1} \times n_{i+2} \times \cdots \times n_\lambda = \mathcal{S}_{i+1} \times \mathcal{P}_{i+1} \times \mathcal{S}_{i+2} \times \mathcal{P}_{i+2} \times \cdots \times \mathcal{S}_\lambda \times \mathcal{P}_\lambda \,.$$

Il en découle que $n_\lambda = \mathcal{P}_\lambda \times \mathcal{S}_\lambda$ et que, par induction, $\mathcal{P}_\ell \times \mathcal{S}_\ell = n_\ell$ pour tout ℓ. En particulier, pour $\ell = 1$, on obtient que $\mathcal{S}_1$ divise n_1. De $n_1 = p$ et $\mathcal{S}_1 \geq 2$ (lemme 3.15), on obtient $\mathcal{S}_1 = p$. □

De la démonstration précédente on tire aussi :

Corollaire 3.20

Soit $\mathcal{A}$ un automate biréversible connexe. Alors $\mathcal{S}_i$ divise l'étiquette de l'arête au niveau $i-1$ de l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$.

Corollaire 3.21

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy connexe, biréversible, ayant un nombre premier d'états et pas de branche auto-repliante active dans son arbre de Schreier $\mathfrak{t}(\mathcal{A})$. Soient $\mathfrak{J}$ un arbre de la jungle de $\mathfrak{t}(\mathcal{A})$ et $\boldsymbol{u}$ un $\mathfrak{J}$-mot. Alors, pour tout état $q \in Q$, il existe $\boldsymbol{w} \in Q^*$ tel que $\boldsymbol{uw}q$ est un $\mathfrak{J}$-mot et $\rho_{\boldsymbol{w}}$ agit comme l'identité sur Σ^*.

Démonstration. Soit $\boldsymbol{v}$ une tige telle que $\boldsymbol{uv}$ soit un $\mathfrak{J}$-mot. D'après le théorème 3.19, il existe dans la $\sim$-classe de $\boldsymbol{v}$ un mot $\boldsymbol{q}$ dont la première lettre est q, *i.e.* il existe $\boldsymbol{w} \in Q^*$ tel que $\boldsymbol{vwq}$ est un $\mathfrak{J}$-mot et $\rho_{\boldsymbol{vw}}$ agit comme l'identité sur Σ^*. □

On notera que dans le corollaire précédent, rien n'empêche $\boldsymbol{u}$ d'être le mot vide.

3.3 Application au problème de Burnside

On montre maintenant :

Théorème 3.22

Un automate de Mealy connexe, inversible et réversible ayant un nombre premier d'états ne peut pas engendrer un groupe de Burnside infini.

Démonstration. Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un tel automate. Si $\mathcal{A}$ n'est pas biréversible, on peut appliquer le théorème 2.6 et obtenir que $\langle \mathcal{A} \rangle$ contient un élément d'ordre infini, et donc n'est pas un groupe de Burnside (voir aussi [1, 46]).

Si $\mathcal{A}$ est biréversible et si $\mathfrak{t}(\mathcal{A})$ admet une branche 1-auto-repliante active, alors là aussi $\langle \mathcal{A} \rangle$ admet un élément d'ordre infini par le théorème 1.14.

On suppose donc que $\mathcal{A}$ est biréversible et que $\mathfrak{t}(\mathcal{A})$ n'a pas de branche 1-auto-repliante active. Montrons que $\langle \mathcal{A} \rangle$ est fini. Soit $\mathfrak{J}$ un arbre de la jungle de $\mathfrak{t}(\mathcal{A})$. Comme dans [67], on prouve que tout mot $\boldsymbol{u} \in Q^*$ possède une puissance uniformément bornée qui agit comme un $\mathfrak{J}$-mot cyclique.

Soit $\boldsymbol{u} \in Q^*$. On prouve par induction que tout préfixe de $\boldsymbol{u}$ induit la même action qu'un $\mathfrak{J}$-mot. C'est vrai de manière triviale pour le préfixe vide. Fixons maintenant $i < |\boldsymbol{u}|$ et supposons que le préfixe de longueur i de $\boldsymbol{u}$, noté $\boldsymbol{v}$, induit la même action qu'un $\mathfrak{J}$-mot $\boldsymbol{v}_{\mathfrak{J}}$. Soit $q \in Q$ la $(i+1)$-ème lettre de $\boldsymbol{u}$. Par le corollaire 3.21, il existe un $\mathfrak{J}$-mot $\boldsymbol{w}$ induisant l'identité, tel que $\boldsymbol{v}_{\mathfrak{J}}\boldsymbol{w}q$ soit un $\mathfrak{J}$-mot. Mais alors, $\boldsymbol{v}q$ and $\boldsymbol{v}_{\mathfrak{J}}\boldsymbol{w}q$ induisent la même action, et le résultat suit. Ainsi, on construit un $\mathfrak{J}$-mot $\boldsymbol{u}^{(1)}$ induisant la même action que $\boldsymbol{u}$.

Par le même procédé, on peut construire, pour tout $i \in \mathbb{N}$, un $\mathfrak{J}$-mot $\boldsymbol{u}^{(i)}$ induisant la même action que $\boldsymbol{u}$, et tel que $\boldsymbol{u}^{(1)}\boldsymbol{u}^{(2)} \dots \boldsymbol{u}^{(i)}$ est un $\mathfrak{J}$-mot. Comme l'ensemble des tiges est fini, il existe deux entiers i et j satisfaisant $i < j$ et $j - i \leq |Q|^\lambda$, et tels que $\boldsymbol{u}^{(i)}$ et $\boldsymbol{u}^{(j)}$ ont le même préfixe de longueur λ. Prenons alors $\boldsymbol{u}_c = \boldsymbol{u}^{(i)}\boldsymbol{u}^{(i+1)} \dots \boldsymbol{u}^{(j-1)}$: $\boldsymbol{u}_c$ est un $\mathfrak{J}$-mot cyclique et induit la même action que $\boldsymbol{u}^{j-i}$. Par le lemme 3.3, l'ordre de $\rho_{\boldsymbol{u}_c}$ est borné par une constante ne dépendant que de l'arbre de la jungle $\mathfrak{J}$, et donc il en va de même pour $\rho_{\boldsymbol{u}}$ (avec une constante différente, mais qui ne dépend toujours que de $\mathfrak{J}$). Ainsi, tous les éléments de $\langle \mathcal{A} \rangle$ sont d'ordre fini, et cet ordre est uniformément borné par une constante. Comme $\langle \mathcal{A} \rangle$ est résiduellement fini, on peut appliquer un théorème de Zelmanov [107, 106]: si un groupe est résiduellement fini et si les ordres de ses éléments sont bornés par une même constante, alors le groupe est fini. On peut donc conclure que $\langle \mathcal{A} \rangle$ est fini. □

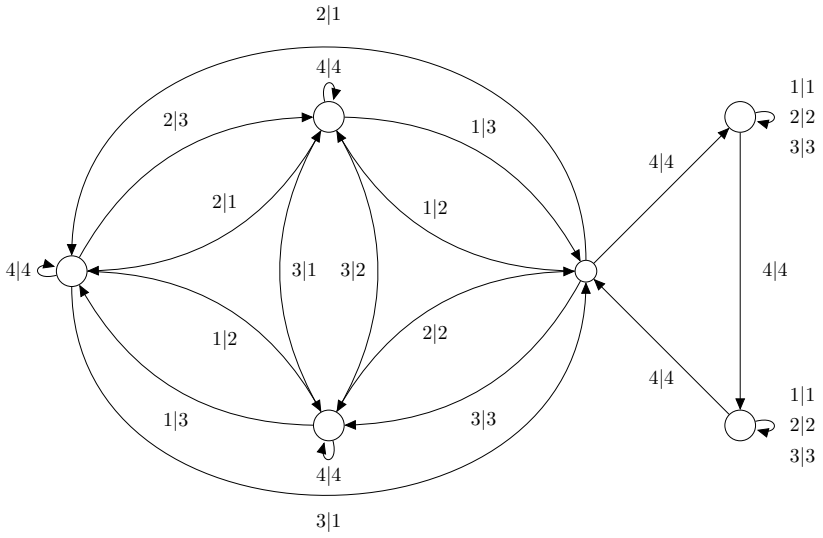


FIGURE II.11 – Un exemple d'automate avec un nombre d'états non-premier, pour lequel un analogue du théorème 3.22 peut être appliqué.

.

On note que l'hypothèse de primalité de l'ensemble des états est faite tardivement, au théorème 3.19, et que les outils restent assez généraux par ailleurs. On peut même parfois appliquer des analogues au théorème 3.22 dans des cas particuliers.

Prenons par exemple l'automate dessiné figure II.11. Il a 6 états, et on ne peut donc pas conclure directement. En revanche, il existe un chemin auto-repliant commençant par les étiquette $6, 5, 5, 5, 5, 5$ (voir la figure II.12). En appliquant le même raisonnement que dans la preuve du théorème 3.19, on trouve que, dans un arbre de la jungle débutant par ce chemin, que $\mathcal{S}_1 \geq 2$ et $\mathcal{S}_1$ divise $n_1 = 6$ mais aussi que $\mathcal{S}_2 \geq 2$ et $\mathcal{S}_2$ divise $n_2 = 5$,et donc $\mathcal{S}_2 = 5$. Mais alors, par la proposition 3.16, $\mathcal{S}_1 \geq \mathcal{S}_2 = 5$ et $\mathcal{S}_1$ divise 6 et on peut donc trouver, dans chaque $\sim$-classe, chaque état comme préfixe d'une tige.

On obtient la dichotomie suivante :

— soit $\mathfrak{t}(\mathcal{A})$ admet (au moins) une branche 1-auto-repliante active, et par la proposition 1.4, $\langle \mathcal{A} \rangle$ possède un élément d'ordre infini ;

— soit $\mathfrak{t}(\mathcal{A})$ n'admet pas de branche 1-auto-repliante active, et on peut construire un arbre de la jungle: en appliquant le raisonnement précédent, puis en raisonnant comme dans la preuve du théorème 3.22 pour construire des mots équivalents dans cet arbre de la jungle, on peut conclure que $\langle \mathcal{A} \rangle$ est fini.

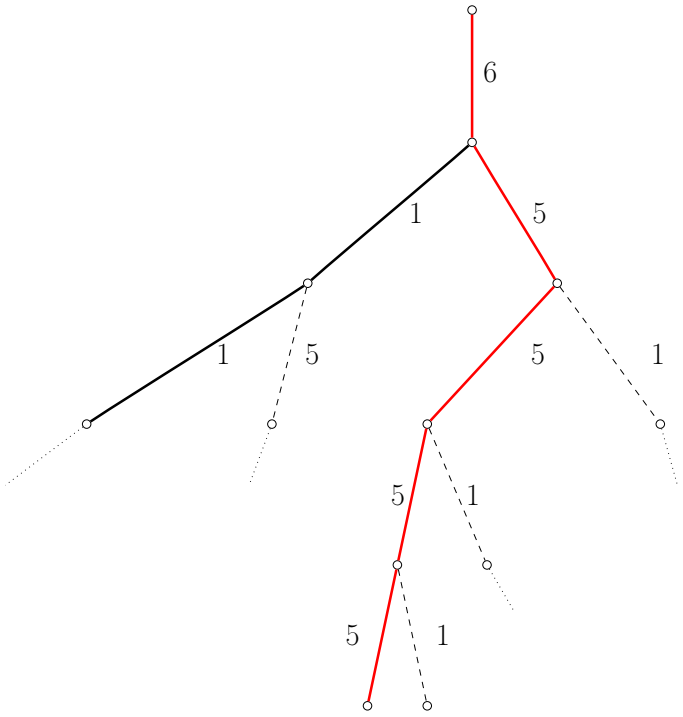


FIGURE II.12 – Les premiers niveaux de l'arbre de Schreier de l'automate figure II.11. Les chemins 1-auto-repliants sont représentés par des arêtes pleines, et le début d'un éventuel arbre de la jungle est en rouge.

Ainsi on obtient :

Proposition 3.23

Le groupe engendré par l'automate de la figure II.11 n'est pas un groupe de Burnside infini.

On peut de cette manière conclure dès que l'automate est connexe et que l'arbre de Schreier admet un chemin 1-auto-repliant de taille ℓ satisfaisant, par exemple $n_\ell > n_1/2$ et n_ℓ premier.

Ces conditions ne sont pas suffisantes pour obtenir un critère de décision, mais offrent l'avantage de permettre de conclure dans des situations assez variées, et surtout d'être très faciles à implémenter.

En revanche, ce critère ne peut pas être adapté pour conclure dans tous les cas. Il existe des exemples d'automates, tel l'automate $\mathcal{H}$ étudié dans [27, 68] et représenté figure II.13, où, dans les $\sim$-classes, deux sous-ensembles d'états alternent dans les mots, et l'on ne peut donc pas appliquer directement notre construction.

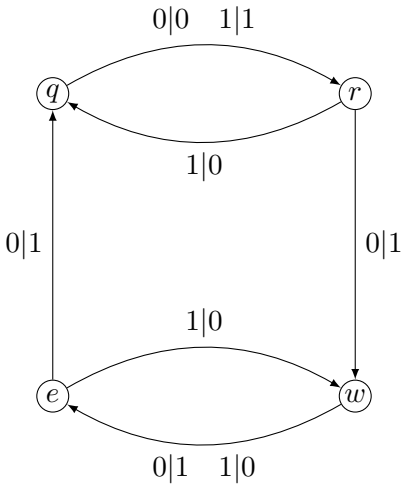


FIGURE II.13 – Automate $\mathcal{H}$ ayant un élément d'ordre infini [27, 68].

4 Remarques et conclusions

4.1 Dénombrement dans les arbres de Schreier

L'étude des chemins auto-repliants étant instructive, il semble intéressant de chercher à mieux comprendre leur structure. On peut commencer cette étude par quelques résultats de comptage.

Lemme 4.1

La somme des étiquettes des enfants légitimes d'un chemin 1-auto-repliant est égale à l'étiquette de la dernière arête de ce chemin.

Démonstration. Considérons l'arbre de Schreier $\mathfrak{t}(\mathcal{A})$ d'un automate de Mealy réversible $\mathcal{A} = (Q, \Sigma, \delta, \rho)$. Soient $\boldsymbol{e}$ un chemin 1-auto-repliant, e sa dernière arête, n_e l'étiquette e, $\boldsymbol{u}$ un mot de $\top(e)$ et q un état de Q tel que $\boldsymbol{u}q$ soit un mot de $\bot(e)$. Écrivons $\boldsymbol{u} = p\boldsymbol{w}$ pour $p \in Q$. Comme $\boldsymbol{e}$ est un chemin 1-auto-repliant et $p\boldsymbol{w}q$ est un mot de $\bot(\boldsymbol{e}) = \bot(e)$, $\boldsymbol{w}q$ est un mot de $\top(e)$. Donc, par construction de l'arbre de Schreier, il y a exactement n_e états, que nous noterons $(r_i)_{1\leq i\leq n_e}$, tels que les mots $(\boldsymbol{w}qr_i)_i$ soient tous dans $\bot(e)$. Les composantes contenant les $(p\boldsymbol{w}qr_i)_i$ sont les enfants légitimes de e, et la somme de leurs étiquettes vaut donc au moins n_e. Comme e ne peut clairement pas avoir d'autre enfant légitime, on obtient l'égalité. □

Ainsi, le nombre de chemins 1-auto-repliants est une constante, si l'on prend en compte la multiplicité :

Corollaire 4.2

Soit $\mathcal{A}$ un automate de Mealy réversible à n états. Pour tout ℓ, la somme des étiquettes des arêtes au niveau ℓ des chemins 1-auto-repliants initiaux vaut n.

Le lemme 4.1 s'étend aux chemins ℓ-auto-repliants. Si l'on appelle enfant ℓ-légitime d'un chemin $\boldsymbol{e}$ de longueur ℓ tout chemin $\boldsymbol{f}$ (de taille ℓ) tel que chaque arête de $\boldsymbol{f}$ est ℓ-superposable sur l'arête de $\boldsymbol{e}$ correspondante, alors le lemme 4.1 a un équivalent direct. Il convient seulement d'être attentif quant à la multiplicité : une arête est comptée autant de fois que son étiquette, et donc un chemin autant que le produit de ses étiquettes.

Lemme 4.3

Soient $\mathcal{A}$ un automate de Mealy réversible et $\boldsymbol{e}$ un chemin m-auto-repliant dans $\mathfrak{t}(\mathcal{A})$. Alors, si $\left(\boldsymbol{e^{(i)}}\right)_i$ avec $\boldsymbol{e^{(i)}} = e_{k+1}^{(i)}, \dots, e_{2k}^{(i)}$ sont les enfants m-légitimes partant de $\perp(\boldsymbol{e})$ on a

$$\sum_i \prod_{j\in\{m+1,\dots,2m\}} l(e_j^{(i)}) = \prod_{j\in\{1,\cdots,m\}} l(e_j)\,,$$

où $e_1, \dots, e_m$ sont les m dernières arêtes de $\boldsymbol{e}$, et $l(e)$ représente l'étiquette de l'arête e.

Démonstration. Soient $\boldsymbol{u}$ un mot de $\top(e_1)$ et $\boldsymbol{q}$ un mot d'états de $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ tel que $\boldsymbol{uq}$ soit un mot de $\perp(\boldsymbol{e}) = \perp(e_m)$. Décomposons $\boldsymbol{u}$ en $\boldsymbol{u} = \boldsymbol{pw}$, $\boldsymbol{p} \in Q^m$. Comme $\boldsymbol{e}$ est un chemin m-auto-repliant et que $\boldsymbol{pwq}$ est un état de $\perp(\boldsymbol{e}) = \perp(e_m)$, $\boldsymbol{wq}$ est un mot de $\top(e_1)$. Donc, par construction de l'arbre de Schreier, il y a exactement $n_e = \prod_{j\in\{1,\dots,m\}} l(e_j)$ mots d'états $(\boldsymbol{r_i})_{1\le i\le n_e}$ tels que $(\boldsymbol{wqr_i})_i$ soient dans $\perp(e)$. Donc les composantes contenant les $(\boldsymbol{pvqr_i})_i$ sont les enfants m-légitimes de e, et la somme de leurs étiquettes vaut donc au moins n_e. Là encore, $\boldsymbol{e}$ ne peut clairement pas avoir d'autre enfant m-légitime, et on conclut. □

On peut aussi dénombrer les chemins qui sont strictement ℓ-auto-repliants. C'est-à-dire les chemins pour lesquels il n'existe pas de $\ell' < \ell$ tel que le chemin soit ℓ'-auto-repliant.
On rappelle qu'un mot est primitif s'il ne peut pas s'écrire comme une puissance d'un mot strictement plus court (dénombrée par la suite A143324 de l'encyclopédie en ligne des suites entières [**OEIS**]).
On remarque que tout chemin ℓ-auto-repliant est aussi $k\ell$-auto-repliant pour tout $k \ge 1$.

Lemme 4.4

Soit $\mathcal{A}$ un automate de Mealy réversible à n états. Alors, pour tout ℓ, la somme des étiquettes des arêtes au niveau ℓ des chemins strictement ℓ-auto-repliants initiaux est égale au nombre de mots primitifs de longueur ℓ sur n lettres.

Démonstration. On utilise la formule d'inversion de Möbius : si f et g sont deux fonctions sur les entiers et μ est la *fonction de Möbius*, alors

$$g(k) = \sum_{d|k} f(d) \implies f(k) = \sum_{d|k} \mu(\frac{d}{k}) g(d) \,.$$

Par le corollaire 4.2, l'automate $\mathcal{A}^\ell$ possède exactement n^ℓ chemins 1-auto-repliants. On peut donc appliquer la formule d'inversion de Möbius, avec $f(\ell)$ la somme des étiquettes à un niveau donné des chemins strictement ℓ-auto-repliants initiaux et $g(\ell) = n^\ell$ la somme des étiquettes à un niveau donné des chemins ℓ-auto-repliants initiaux :

$$f(\ell) = \sum_{d|\ell} \mu(\frac{d}{k}) n^d$$

donc

$$n^k = \sum_{d|k} f(d) \,.$$

On reconnaît alors la formule de dénombrement des mots primitifs, d'où le résultat. □

L'intérêt de ce dénombrement est chercher à trouver des éléments d'ordre infini. Un exemple peut être trouvé figure II.14.

4.2 Conclusion

Dans ce chapitre, on a vu comment des outils de théorie des automates (produit d'automates de Mealy) et de dénombrement, alliés à des théorèmes de théorie des groupes (comme le théorème de Zelmanov) peuvent permettre de mieux appréhender les propriétés des groupes d'automate et le transfert de propriétés structurelles des automates vers des propriétés de groupe. On a ainsi montré que la réversibilité de l'automate interdit dans de nombreux cas au groupe engendré d'être infini de Burnside. La continuité naturelle de ces travaux est d'étendre ce résultat à l'ensemble des automates de Mealy réversibles, c'est-à-dire résoudre :

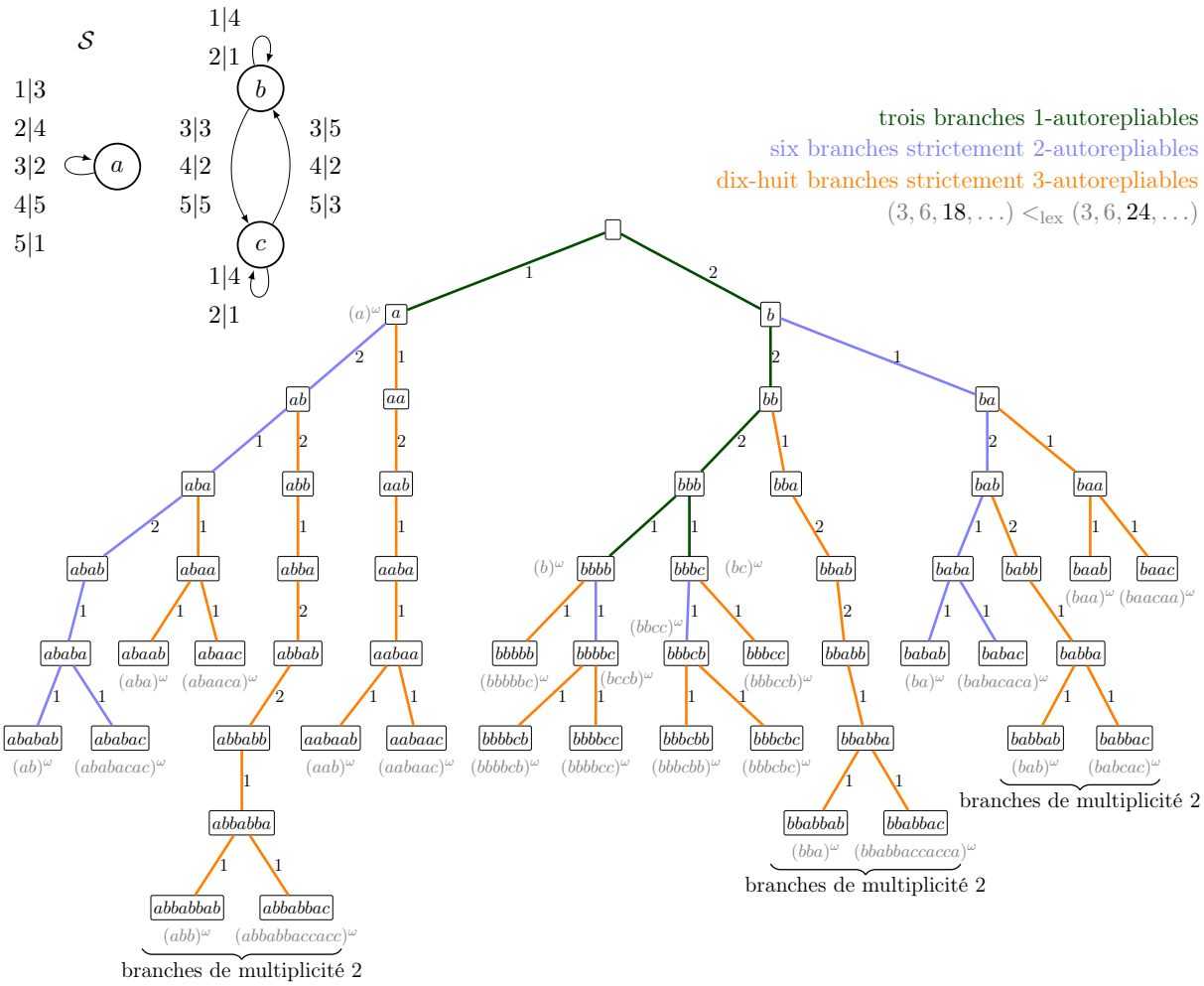


FIGURE II.14 – Dénombrement des chemins strictement auto-repliants d'un automate $\mathcal{S}$.

Conjecture 4.5

Un automate de Mealy inversible et réversible ne peut pas engendrer un groupe de Burnside infini.

Dans un esprit comparable, Klimann [64] a montré dans cette classe que, si l'action du groupe engendré par le dual de l'automate est transitive par niveau (c'est-à-dire que l'arbre de Schreier de l'automate est formé d'une unique branche), alors le groupe a une croissance exponentielle. Il semble intéressant de se demander si la réversibilité seule empêche le groupe d'être de croissance intermédiaire. En effet, comme pour les groupes de Burnside infinis, tous les exemples de groupes d'automate ayant une croissance intermédiaire proviennent d'automates non-réversibles. En fait, on ne connaît pas non plus d'automate de Mealy réversible qui engendre un groupe infini à croissance polynomiale, et on peut chercher à démontrer que, si l'automate est inversible et réversible, alors le groupe est soit fini, soit à croissance exponentielle.

Chapitre III

Dynamique de l'action du groupe d'automate sur l'arbre enraciné infini

Points singuliers, diagrammes en croix et pavage de Wang

Un groupe d'automate peut naturellement être vu comme agissant sur un arbre : on a vu que les éléments du groupe induisent une transformation des mots vers les mots. L'ensemble Σ^* des mots sur un alphabet Σ à k lettres peut être décrit comme un arbre d'arité k, dont la racine est le mot vide et les enfants de chaque sommet sont étiquetés par une lettre différente de l'alphabet. L'action de l'automate sur cet arbre est décrite récursivement : si $g = \rho_{\boldsymbol{u}}$, $\pi(\boldsymbol{u}) = \sigma \in \mathcal{S}_\Sigma$ et $\delta_i(\boldsymbol{u}) = \boldsymbol{u}_i$ alors g permute les sous-arbres du premier niveau selon σ, et on applique $\rho_{\boldsymbol{u}_i}$ au sous-arbre étiqueté par i. On a vu dans le chapitre précédent que cette action nous donne de nombreuses propriétés sur le groupe engendré par le dual de l'automate, et comment les composante connexes des puissances d'un automate s'apparentent aux *graphes de Schreier* de ce groupe dual. Il est alors naturel de passer à la limite et de considérer cette action non plus sur les mots finis—*i.e.* l'arbre régulier fini Σ^*— mais sur les *mots infinis*—*i.e.* l'arbre régulier infini Σ^ω—. Une première remarque est qu'alors le nombre d'orbites n'est plus fini, ni même dénombrable.

Cette action et ces composantes présentent de nombreuses propriétés, étudiées entre autres par [52, 51, 53]. On cherche en général à savoir si telle propriété est toujours/presque-toujours/presque-jamais/jamais vérifiée, ou bien on essaie de décrire la structure de l'action sur la frontière $\partial T = \Sigma^\omega$ [20, 53]. Une propriété remarquable de l'action du groupe sur un mot $\boldsymbol{u}$ (fini) peut être, par exemple, de laisser le mot **invariant**, c'est-à-dire $g.\boldsymbol{u} = \boldsymbol{u}$ pour tout élément g de ce groupe, ou, si l'on se place à la frontière, le fait que le mot $\boldsymbol{\xi}$ (infini) soit **stabilisé**, c'est-à-dire $g.\boldsymbol{\xi} = \boldsymbol{\xi}$ pour un certain élément non trivial g de ce groupe. On peut aussi chercher à retrouver

des informations sur l'action du groupe en regardant les graphes de Schreier des points infinis. En ce sens, Vershik [99] a introduit le concept d'action *totalement non-libre* : de manière classique, on dit que l'action d'un groupe est libre si, pour tout élément g de ce groupe, la mesure de l'ensemble $\mathrm{St}_g(X) = \{x \in X, g.x = x\}$ est nulle pour $g \neq \mathbb{1}$ (en particulier si le groupe agit sur un ensemble fini, cela signifie qu'aucun élément de cet ensemble n'est stable par l'action de g). Alors on ne peut pas extraire d'autre information des graphes de Schreier que la liberté de cette action. Vershik s'intéresse au cas en quelques sorte opposé où tous les points infinis ont des stabilisateurs distincts, et alors l'action originelle du groupe peut être presque entièrement recouvrée. Grigorchuk a montré ([51]) que, pour les groupes faiblement branchés, l'action du groupe sur Σ^ω est totalement non-libre.

Dans ce chapitre, qui se base sur un travail effectué en collaboration avec Daniele D'Angeli, Ines Klimann, Matthieu Picantin et Emanuele Rodaro [29], nous étudions les *points singuliers* de cette action, c'est-à-dire les points de discontinuité de la fonction qui, à un mot infini dans l'arbre associe son groupe des stabilisateurs. On adoptera souvent la vision "action sur l'arbre". Cette vision est décrite plus en détail dans l'introduction, ainsi que les notions topologiques qui lui sont associées.
Pour commencer, on cherche de nouveau à utiliser des outils de théorie des automates et la structure des automates sous-jacents pour étudier ces points singuliers. Cette approche se révèle fructueuse car on peut ainsi retrouver par des méthodes élémentaires la caractérisation des points singuliers de l'action du groupe de Grigorchuk donnée par Vorobets [102] et, en général, aboutir à une caractérisation exacte des points singuliers de l'action de groupes engendrés par des automates ayant de bonnes propriétés structurelles. On trouve aussi des propriétés de mesure de ces points singuliers, ainsi que des liens avec le produit d'automate et les graphes de Schreier. Dans un deuxième temps, on cherche à exhiber des points singuliers spécifiques de l'action. Pour cela on utilise le graphe en hélice de l'automate, et on met en exergue le lien entre automate de Mealy et pavage de Wang. En utilisant ce lien, on montre que l'existence de certains couples lettre-état, liée à l'existence de points singuliers, est indécidable.

1 Points singuliers

Définissons la fonction St qui, à un mot infini sur Σ, associe ses stabilisateurs :

$$\begin{aligned} \mathrm{St}\colon \Sigma^\omega &\longrightarrow \text{Sous-groupes}(\langle \mathcal{A} \rangle) \\ \boldsymbol{\xi} &\longmapsto \mathrm{St}_{\langle \mathcal{A} \rangle}(\boldsymbol{\xi}). \end{aligned}$$

De plus on définit le stabilisateur du voisinage $\mathrm{St}^0_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$ d'un mot infini $\boldsymbol{\xi}$ comme l'ensemble des éléments $g \in \langle\mathcal{A}\rangle$ qui stabilisent $\boldsymbol{\xi}$, ainsi qu'un voisinage de $\boldsymbol{\xi}$ (qui peut dépendre de g): soit $\xi \in \Sigma^\omega$,

$$\mathrm{St}^0_{\langle A\rangle}(\xi) = \{g \in \langle A\rangle, \exists k_g \in \mathbb{N}, \forall \zeta \in \Sigma^\omega, g.\xi[:k_g]\zeta = \xi[:g]\zeta\}\,.$$

On remarque que c'est un sous-groupe distingué dans $\mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$.

Le lemme suivant, dû à Vorobets, relie la continuité de St avec le stabilisateur du voisinage. Fixons la topologie sur l'ensemble des sous-groupes d'un groupe dénombrable G : prenons une numérotation $G = \{g_1, g2, \ldots\}$, alors la distance entre deux sous-groupes H_1 et H_2 de G vaut 0 si $H_1 = H_2$ et 2^{-n} où n est le premier indice tel que g_n appartienne à la différence symétrique entre H_1 et H_2.

Lemme 1.1 ([102, Lemma 5.4])

La fonction St est continue en $\boldsymbol{\xi} \in \Sigma^\omega$ si et seulement si $\mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi}) = \mathrm{St}^0_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$.

Définition 1.2

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy inversible. Un point $\boldsymbol{\xi} \in \Sigma^\omega$ est dit *singulier* si la fonction St n'est pas continue en ce point.
On note κ l'ensemble des points singuliers.

Le lemme suivant traduit la singularité en terme de dynamique sur l'automate :

Lemme 1.3

Soit $\mathcal{A}$ un automate inversible et $\boldsymbol{\xi} \in \Sigma^\omega$. Les propositions suivantes sont équivalentes :

(i) $\boldsymbol{\xi}$ n'est pas singulier ;

(ii) St est continue en $\boldsymbol{\xi}$;

(iii) pour tout $g \in \mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$, il existe ℓ satisfaisant $g.\boldsymbol{\xi}[:\ell] = \mathbb{1}$.

Démonstration. (i)$\Longleftrightarrow$(ii) et (iii)$\Rightarrow$(ii), suivent directement des définitions.
Pour prouver (ii)$\Rightarrow$(iii), nous raisonnons par contraposée : soit $\boldsymbol{\xi}$ tel qu'il existe $g \in \mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$ avec pour tout ℓ, $g_{|\boldsymbol{\xi}[:\ell]} \neq \mathbb{1}$. Alors pour tout ℓ , il existe une lettre x_ℓ vérifiant $g_{|\boldsymbol{\xi}[:\ell]}.x_\ell \neq x_\ell$. Ainsi, en considérant les mots $\boldsymbol{\xi}[:\ell](x_\ell)^\omega$, on construit une suite convergeant vers $\boldsymbol{\xi}$ dont les éléments

ne sont pas stables par $\mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$, donc $\mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi}) \neq \mathrm{St}^0_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi})$, et par le lemme 1.1, la fonction St n'est pas continue en $\boldsymbol{\xi}$. □

On peut s'intéresser à des points particuliers de Σ^ω : les mots ultimement périodiques. Malgré leur forme spécifique, l'existence de points singuliers est équivalente à l'existence de points singuliers ultimement périodiques :

Lemme 1.4

Un automate de Mealy inversible admet des points singuliers si et seulement s'il admet des points singuliers périodiques.

Démonstration. Le sens réciproque est immédiat. On prouve le sens direct par contraposée : soit $\boldsymbol{\xi} \in \Sigma^\omega$ un point singulier. D'après le lemme 1.3, il existe $g \in \mathrm{St}_{\langle\mathcal{A}\rangle}(\boldsymbol{\xi}) \setminus \{\mathbb{1}\}, \forall \ell \in \mathbb{N}, g_{|\boldsymbol{\xi}[:\ell]} = \mathbb{1}$. Comme l'ensemble $\{g_{|\boldsymbol{\xi}[:i]}\}_i$ est fini, il existe deux indices i et j qui vérifient $g_{|\boldsymbol{\xi}[:i]} = g_{|\boldsymbol{\xi}[:j]}$. Mais alors $g_i := g_{|\xi[:i]}$ stabilise le mot ultimement périodique $\boldsymbol{\zeta} = (\boldsymbol{\xi}[i:j])^\omega$, et pour tout ℓ, $g_{i|\boldsymbol{\zeta}[:\ell]} \neq \mathbb{1}$, donc $\boldsymbol{\zeta}$ est singulier. □

Dans [102], il est prouvé que l'ensemble κ des points singuliers est *maigre*, c'est-à-dire union dénombrable d'ensembles fermés d'intérieur vide (aussi appelés espaces nulle part denses). De manière générale, un tel ensemble n'est pas forcément de mesure nulle pour la mesure de Bernoulli μ sur l'arbre Σ^ω, c'est cependant le cas ici :

Théorème 1.5

Soit un automate inversible. L'ensemble κ de ses points singuliers est de mesure nulle.

Démonstration. La preuve s'appuie fortement sur des idées provenant de la proposition 4.1 et du théorème 4.2 de [60].
Soit un mot d'états $\boldsymbol{u}$, posons $\mathrm{Fix}(\boldsymbol{u}) = \{\boldsymbol{\xi} \in \Sigma^\omega, \rho_{\boldsymbol{u}}(\boldsymbol{\xi}) = \boldsymbol{\xi}\}$ l'ensemble des mots infinis fixés par $\boldsymbol{u}$, et $\mathrm{Fix}(\boldsymbol{u})_k$ l'ensemble des mots de longueur k fixés par $\boldsymbol{u}$.
Pour $\boldsymbol{u} \in \widetilde{Q}^*$ et $k \geq 1$, considérons les ensembles suivants :

$$\chi(\boldsymbol{u}) = \{\boldsymbol{\xi} \in \Sigma^\omega : \boldsymbol{\xi} \in \mathrm{Fix}(\boldsymbol{u}) \text{ et } \delta_{\boldsymbol{\xi}[:j]}(u) \neq \mathbb{1} \quad \forall j \geq 0\}$$

$$\text{et } \chi_k(\boldsymbol{u}) = \{\boldsymbol{w} \in \Sigma^k : \boldsymbol{w} \in \mathrm{Fix}(\boldsymbol{u})_k \text{ et } \delta_{\boldsymbol{w}[:j]}(\boldsymbol{u}) \neq \mathbb{1} \quad 0 \leq j \leq k\}.$$

L'ensemble des points singuliers s'écrit :

$$\kappa = \bigcup_{\boldsymbol{u}\in\widetilde{Q}^*} \chi(\boldsymbol{u}).$$

Montrons que $\mu(\chi(\boldsymbol{u})) = 0$, pour tout $\boldsymbol{u} \in \widetilde{Q}^*$. Comme une union dénombrable d'ensembles de mesure nulle est elle-même de mesure nulle, cela impliquera le théorème. On a :

$$\chi(\boldsymbol{u}) = \bigcap_{k\geq 1} (\chi_k(\boldsymbol{u})\Sigma^\omega)\,,$$

donc :

$$\mu(\chi(\boldsymbol{u})) = \lim_{k\to\infty} \mu(\chi_k(\boldsymbol{u})\Sigma^\omega) = \lim_{k\to\infty} \frac{|\chi_k(\boldsymbol{u})|}{|\Sigma|^k}\,.$$

Soit $H_i = \{\boldsymbol{v} \in \widetilde{Q}^i\,,\, \boldsymbol{v} \neq \mathbb{1}\}$. Comme l'ensemble $H_{|\boldsymbol{u}|}$ est fini, il existe un entier p tel qu'aucun élément de $H_{|\boldsymbol{u}|}$ n'induise l'identité sur Σ^p. Supposons alors par récurrence que $\left|\chi_{p(k-1)}(\boldsymbol{u})\right| \leq (|\Sigma|^p - 1)^{k-1}$. Comme $\delta_h(\boldsymbol{u}) \in H_{|\boldsymbol{u}|}$ pour tout $h \in \chi_{p(k-1)}(\boldsymbol{u})$, il existe un mot $\boldsymbol{s} \in \Sigma^p$ qui n'est pas fixé par $\delta_h(\boldsymbol{u})$. Ainsi

$$|\chi_{p\cdot k}(\boldsymbol{u})| \leq |\chi_{p(k-1)}(\boldsymbol{u})|(|\Sigma|^p - 1) \leq (|\Sigma|^p - 1)^k\,.$$

Et donc $\lim_{k\to\infty} \frac{|\chi_k(\boldsymbol{u})|}{|\Sigma|^k} = 0$, et on peut conclure que $\mu(\kappa) = 0$. □

On caractérise maintenant de manière plus précise l'ensemble des points singuliers. On suit deux approches diamétralement opposées : dans la section 2 on se restreint à une classe donnée d'automates et on utilise les propriétés de la-dite classe pour mieux décrire les points singuliers. On retrouve ainsi avec une preuve plus simple et générale d'un résultat de Vorobets [102]. Ensuite, dans la section 3, on examine les liens entre les points singuliers et la structure des graphes de Schreier de l'automate. Dans la section 4 on étudie des points spéciaux de Σ^ω et on utilise le lien entre l'action du groupe et les pavages de Wang pour obtenir des informations sur les points singuliers.

2 Points singuliers et propriétés structurelles de l'automate

Dans cette section, on s'intéresse à la description de l'ensemble κ des points singuliers dans des classes spécifiques de groupes d'automate. On se penche d'abord sur les automates *contractants*, puis sur les automates *(bi)réversibles*.

2.1 Automates contractants

Rappelons qu'un automate $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ est dit contractant s'il existe un autre automate $\mathcal{N}$ (fini) sur le même alphabet, appelé *noyau* de $\mathcal{A}$, tel que pour tout n, tout élément $\boldsymbol{q}$ de Q^n, et tout mot $\boldsymbol{\xi}$ sur Σ^ω, il existe un indice ℓ tel que, pour tout $i \geq \ell$, $\delta_{\boldsymbol{\xi}[:i]}(\boldsymbol{q})$ induit la même action sur Σ^* qu'un élément de $\mathcal{N}$.

Par cette propriété, on peut décrire partiellement les points singuliers d'un automate contractant $\mathcal{A}$: si $\boldsymbol{\xi}$ est un point singulier, alors il est stabilisé par un certain état de $\mathcal{A}^m$, $m \in \mathbb{N}$, et il admet un suffixe qui est stabilisé par un état du noyau de $\mathcal{A}$ et qui ne devient pas l'identité en lisant les préfixes de $\boldsymbol{\xi}$ (voir la figure III.1). Comme le noyau est fini, ces conditions peuvent être vérifiées directement sur le noyau.

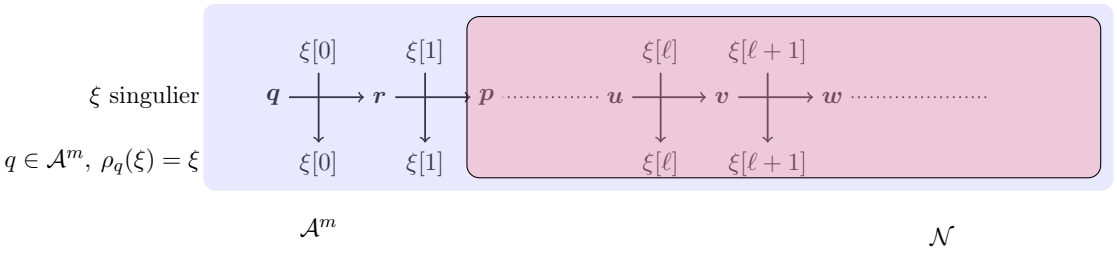


FIGURE III.1 – Si ξ est singulier, alors un de ses suffixe est stabilisé par un élément du noyau.

Soit $\mathcal{A}$ un automate. L'*automate stable* de $\mathcal{A}$, noté $\mathcal{B}(\mathcal{A})$ est l'automate de Büchi ayant le même ensemble d'états que $\mathcal{A}$ et dont les transitions sont données par :

$$q \xrightarrow{a} p \ \in \mathcal{B}(\mathcal{A}) \quad \Longleftrightarrow \quad q \xrightarrow{a|a} p \ \in \mathcal{A}\,,$$

Ses états acceptants sont les états représentant des éléments non triviaux dans le groupe $\langle \mathcal{A} \rangle$. Comme tous les états non triviaux (*i.e.* les états représentant des élément non triviaux dans le groupe) de l'automate stable sont acceptants, l'automate stable est un automate de Büchi *faible* (*weak Büchi* [83]). Il en découle que le langage reconnu par $\mathcal{B}(\mathcal{N})$ est fermé et régulier. Il est aussi clos par suffixe (infini).

On a le résultat suivant :

Théorème 2.1

Soit $\mathcal{A}$ un automate contractant et $\mathcal{N}$ son noyau. L'ensemble κ des points singuliers de cet automate est inclus dans l'ensemble des mots finissant par un mot du langage reconnu par l'automate stable de $\mathcal{N}$:

$$\kappa \subset \Sigma^* \mathcal{L}\left(\mathcal{B}\left(\mathcal{N}\right)\right) .$$

Inversement tout mot du langage reconnu par l'automate stable de $\mathcal{N}$ est singulier:

$$\mathcal{L}\left(\mathcal{B}\left(\mathcal{N}\right)\right) \subset \kappa .$$

Démonstration. Quitte à minimiser, on peut supposer que le noyau $\mathcal{N}$ ne possède qu'un seul état $\mathbb{1}$ représentant l'élément trivial dans le groupe : cet état est le seul état non acceptant de $\mathcal{B}\left(\mathcal{N}\right)$. Soit un point singulier $\boldsymbol{\xi} \in \Sigma^\omega$. D'après le lemme 1.3, il existe $\boldsymbol{u} \in Q^n$ qui stabilise $\boldsymbol{\xi}$ et tel que pour tout i, $\delta_{\boldsymbol{\xi}[:i]}(\boldsymbol{u}) \neq \mathbb{1}$. Mais alors par définition du noyau, il existe un indice ℓ tel que pour tout i, $q_i = \delta_{\boldsymbol{\xi}[:\ell+i]}(\boldsymbol{u}) \in \mathcal{N}$ (on identifie les états équivalents dans $Q^{|\boldsymbol{u}|}$ et $\mathcal{N}$). Ces états vérifient $\rho_{q_i}(\boldsymbol{\xi}[i]) = \boldsymbol{\xi}[i]$, et la transition est présente dans $\mathcal{B}\left(\mathcal{N}\right)$, donc $\boldsymbol{\xi}[\ell :]$ est un chemin infini dans $\mathcal{B}\left(\mathcal{N}\right)$ qui évite l'état $\mathbb{1}$ (par hypothèse sur les $\delta_{\boldsymbol{\xi}[:i]}(\boldsymbol{u})$). Ainsi $\boldsymbol{\xi}[: \ell] \in \mathcal{L}\left(\mathcal{B}\left(\mathcal{N}\right)\right)$ et $\boldsymbol{\xi}$ est cofinal à un mot du langage reconnu par $\mathcal{B}\left(\mathcal{N}\right)$.

Pour la réciproque partielle, il suffit de remarquer que si $\boldsymbol{\xi}$ est un chemin infini accepté par $\mathcal{B}\left(\mathcal{N}\right)$ depuis l'état q, alors il ne passe jamais par e qui est un puits, d'où $\delta\boldsymbol{\xi}[: i](q) \neq \mathbb{1}$ et que $\rho_q(\boldsymbol{\xi}) = \boldsymbol{\xi}$, par définition des transitions de $\mathcal{B}\left(\mathcal{N}\right)$. On conclut en remarquant que $\langle\mathcal{N}\rangle < \langle\mathcal{A}\rangle$. □

Ce théorème est particulièrement pertinent quand $\mathcal{L}\left(\mathcal{B}\left(\mathcal{N}\right)\right) = \emptyset$, car alors $\kappa = \emptyset$. Par exemple pour le groupe de la Basilique :

Corollaire 2.2

Le groupe de la Basilique, engendré par l'automate (contractant) figure I.17 n'admet aucun point singulier.

On remarque que si un point $\boldsymbol{\xi} \in \Sigma^\omega$ est singulier, alors tout élément de son orbite l'est aussi. En effet si $\boldsymbol{\xi}$ est singulier ($g.\boldsymbol{\xi} = \boldsymbol{\xi}$, avec $g_{|\boldsymbol{\xi}[:i]} \neq \mathbb{1}$ pour tout i) et $h.\boldsymbol{\xi}$ est un point dans l'orbite de $\boldsymbol{\xi}$, on a $hgh^{-1}.(h.\boldsymbol{\xi}) = hgh^{-1}h.\boldsymbol{\xi} = hg.\boldsymbol{\xi} = h.\boldsymbol{\xi}$, et comme un élément a même ordre que ses conjugués, ${hgh^{-1}}_{|h.\boldsymbol{\xi}[:i]} \neq \mathbb{1}$ pour tout i.

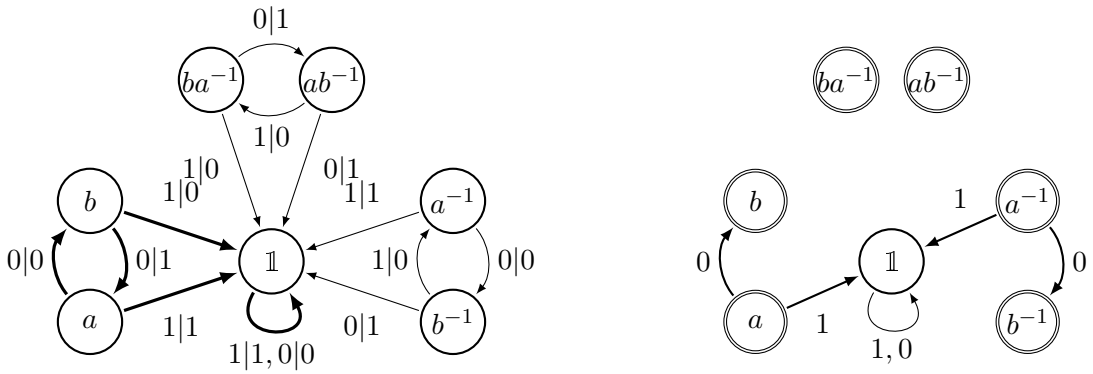


FIGURE III.2 – Le noyau (à gauche) et l'automate stable (à droite), associés à l'automate de la Basilique (figure I.17, arêtes du noyau en gras).

On peut aboutir à une caractérisation exacte dans le cas des automates *fractaux*. Pour mémoire un automate $\mathcal{A}$ est dit fractal si, pour tout mot $\boldsymbol{s} \in \Sigma^*$ et tout élément g du groupe $\langle \mathcal{A} \rangle$, il existe $h \in \mathrm{St}_{\langle \mathcal{A} \rangle}(\boldsymbol{s})$ (donc $h.\boldsymbol{s} = \boldsymbol{s}$) tel que $h_{|\boldsymbol{s}} = g$. On obtient :

Proposition 2.3

Soit $\mathcal{A}$ un automate inversible, contractant et fractal et soit $\mathcal{N}$ son noyau. Alors l'ensemble κ des points singuliers est exactement l'ensemble des points finissant par un mot du langage reconnu par l'automate $\mathcal{B}(\mathcal{N})$:

$$\kappa = \Sigma^* \mathcal{L}(\mathcal{B}(\mathcal{N})) \ .$$

Démonstration. La première inclusion provient du théorème 2.1. Pour prouver maintenant que tout mot $\boldsymbol{s}\boldsymbol{\xi}$ finissant par un mot $\boldsymbol{\xi}$ reconnu par l'automate $\mathcal{B}(\mathcal{N})$, on remarque simplement qu'il existe $g \in \langle \mathcal{A} \rangle$ stabilisant $\boldsymbol{\xi}$ et tel que $g_{|\boldsymbol{\xi}[:i]} \neq \mathbb{1}$ pour tout i (lemme 1.3). Alors comme $\langle \mathcal{A} \rangle$ est fractal il existe $h \in \langle \mathcal{A} \rangle$ tel que :

$$\begin{array}{ccccc} & \boldsymbol{s} & & \boldsymbol{\xi}[n:] & \\ h & \downarrow & h_{|\boldsymbol{s}} = g & \downarrow & \\ & \boldsymbol{s} & & \boldsymbol{\xi}[n:] & \end{array}$$

Et on a bien $h_{|\boldsymbol{s}\boldsymbol{\xi}[:i]} \neq \mathbb{1}$ pour tout i, donc par le lemme 1.3, $\boldsymbol{s}\boldsymbol{\xi}$ est singulier. □

Malgré ces hypothèses qui peuvent sembler fortes, la classe des automates fractaux et contractants est loin d'être sans intérêt : elle inclut entre autres les automates de Grigorchuk, de la Ba-

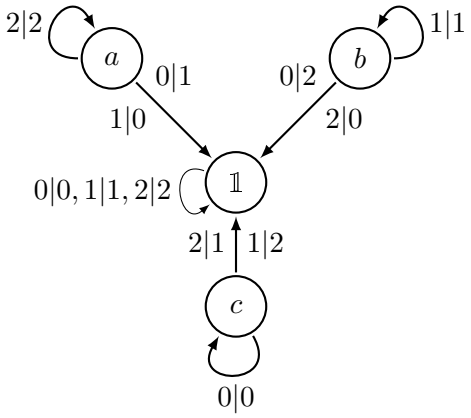


FIGURE III.3 – L'automate (contractant) engendrant le groupe des tours de Hanoï $H^{(3)}$.

silique ou des tours de Hanoï. On retrouve d'ailleurs (voir la figure III.4) le résultat de Vorobets sur le groupe de Grigorchuk [102], ainsi qu'un analogue pour d'autres groupes importants :

Corollaire 2.4 ([102])

Les points singuliers du groupe de Grigorchuk $\langle \mathcal{G} \rangle$ sont les points finissant par à 1^ω. De manière équivalente ce sont les points de l'orbite de 1^ω.

Corollaire 2.5

Les points singuliers du groupe de Hanoï H^3 sont les points cofinaux à x^ω, $x \in \{0, 1, 2\}$. De manière équivalente ce sont les points de l'orbite de x^ω, $x \in \{0, 1, 2\}$.

Regardons maintenant la taille de l'ensemble κ. On a vu avec le théorème 1.5 que cet ensemble est négligeable au sens de la mesure de Bernoulli, puis on a vu des exemples où cet ensemble est vide ou dénombrable.
Il existe aussi des automates fractaux et contractants ayant un quantité indénombrable de points singuliers, comme le montre l'exemple figure III.5, où $(000+111)^\omega \subset \kappa$. On en a également étudié un autre exemple avec l'automate Bread-and-Butterfly (Chapitre I), qui vérifie, par construction, $((\text{-}1\text{-}1\text{-}1) + (+1+1+1))^\omega \subset \kappa$.

On peut cependant constater que l'ensemble des points est dénombrable si la structure en cycles est simple.

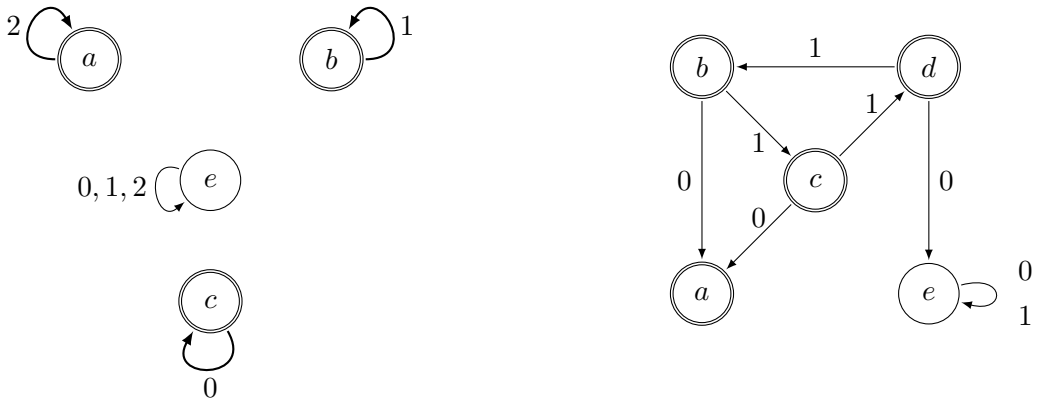


FIGURE III.4 – Les automates stables de l'automate des tours de Hanoï $\mathcal{B}\left(H^{(3)}\right)$ (à gauche) et de l'automate de Grigorchuk (à droite).

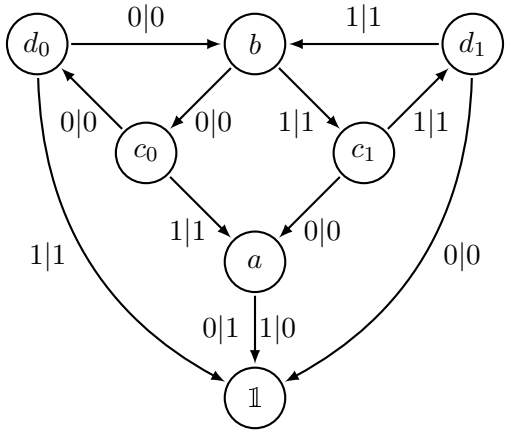


FIGURE III.5 – Une version déformée de l'automate de Grigorchuk ayant un nombre indénombrable de points singuliers. Ce groupe est fractal et contactant et vérifie $(000 + 111)^\omega \subset \kappa$.

Proposition 2.6

Un automate inversible, contractant et à activité polynomiale a un ensemble de points singuliers au plus dénombrable.

Démonstration. Comme $\mathcal{A}$ est à activité polynomiale, $\mathcal{N}$ l'est aussi et donc seul un nombre borné de cycles non triviaux sont accessibles depuis un cycle. Il en va de même dans l'automate stable, et donc le langage de l'automate stable est de la forme $\bigsqcup_{\boldsymbol{s}} \Sigma^* \boldsymbol{s}^\omega$, avec $\boldsymbol{s} \in \Sigma^*$ les mots lus sur les cycles de l'automate stable (car un mot accepté est ultimement reconnu par un cycle de

l'automate stable). Le théorème 2.1 implique alors $\kappa \subset \bigsqcup \Sigma^* \boldsymbol{v}^\omega$, qui est une union dénombrable d'ensembles dénombrables, et donc lui-même dénombrable. □

Là encore cette classe reste riche et contient des exemples majeurs d'automates de Mealy, parmi lesquels l'automate de Grigorchuk, la machine à additionner, l'automate de la Basilique ou celui des tours de Hanoï.

D'autre part, le fait d'avoir accès dans les automates contractants, à la structure de l'automate reconnaissant les suffixes des points singuliers permet de raffiner le théorème 1.5, du moins dans un cadre topologique, via la *dimension de Minkowski-Bouligand*[1].

Soit S un sous-ensemble d'un espace métrique compact (E, d). Posons $N_S(\epsilon)$ le nombre minimal de sphère de rayon ϵ dont le centre appartient à S nécessaires pour couvrir S. La dimension de Minkowski-Bouligand (aussi appelée box-counting dimension), est :

$$\dim_{\text{BOX}}(S) = \lim_{\epsilon \to 0} \frac{\log N_S(\epsilon)}{\log(1/\epsilon)} .$$

Dans notre cas, la sphère de rayon $1/k^i$ centrée en $\boldsymbol{\xi} \in \Sigma^\omega$ est tout simplement le sous-arbre k-aire situé sous le préfixe de taille i de $\boldsymbol{\xi}$.

Par exemple, pour l'automate de Grigorchuk, le langage reconnu par l'automate stable est de dimension de Minkowski-Bouligand nulle, car la sphère centrée en 1^ω suffit à couvrir tous les points singuliers. En revanche, s'il existe, comme dans l'exemple de la figure III.5, un ensemble indénombrable de mots reconnus par l'automate stable, alors la dimension de Minkowski-Bouligand est plus grande que 1 (elle vaut 2/8 si le langage est $(000+111)^\omega$). Le problème majeur de cette dimension est qu'elle n'est pas laissée invariante par l'ajout d'une quantité dénombrable de points, alors que l'on souhaite, pour les points singuliers d'un automate fractal par exemple, pouvoir ajouter n'importe préfixe. On peut alors se limiter aux points singuliers périodiques. En pratique, cela permet de se placer directement dans l'automate stable et ne change pas la valeur de la dimension pour le langage reconnu par l'automate stable.

En fait, on retrouve la notion d'*entropie d'un langage*[2]. Staiger [95] définit l'entropie d'un ω-langage L comme :

$$\mathcal{H}(L) = \limsup \frac{\log |L_\ell|}{\ell} ,$$

1. Je suis très reconnaissant à Ville Salo de m'avoir suggéré, lors de ma visite à Turku, de m'intéresser à cette dimension pour ce problème.

2. Je tiens maintenant à remercier Benjamin Hellouin de Menibus pour m'avoir fait remarquer que la box dimension correspondait à la notion d'entropie d'un langage, ainsi qu'Eugène Asarin pour les références et l'aide qu'il m'a apportées sur cette notion.

où L_ℓ est l'ensemble des préfixes de taille ℓ dans L. On remarque alors qu'un préfixe de longueur ℓ du langage représente une boule de rayon $1/|\Sigma|^\ell$ couvrant une partie du langage et donc que les deux notions coïncident (à une constante égale à la taille de l'alphabet près). On a alors un algorithme pour calculer cette entropie : il suffit de calculer la matrice d'adjacence de l'automate (vu comme un graphe) dont on a supprimé les puits, puis d'en extraire la plus grande valeur propre ρ (cette valeur propre se trouve être un nombre réel supérieur à 1, et en fait un nombre de Perron). On obtient :

$$\mathcal{H}(L) = \log \rho \,.$$

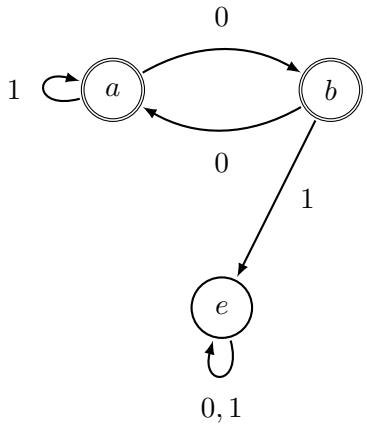


FIGURE III.6 – Un automate de Büchi dont le langage a pour entropie le logarithme du nombre d'or.

Exemple 2.7

L'automate de Büchi de la figure III.6 reconnait le langage $L = (1 + 00)^\omega$ et a pour entropie $\mathcal{H}(L) = \log \frac{1+\sqrt{5}}{2}$.

Ainsi, si $\mathcal{A}$ est un automate contractant, l'entropie de l'ensemble des points singuliers périodiques est égale à l'entropie du langage reconnu par l'automate stable. En particulier on retrouve des liens avec l'activité : un automate dont le noyau est à activité bornée est d'entropie nulle.

Il semble intéressant de continuer d'explorer ces notions de complexité (mesure, entropie, ...) de l'ensemble des points singuliers. Cette étude est facilitée par la structure de l'automate, et n'est pour l'instant possible que dans la classe des automates contractants. Cette classe est déjà riche et intéressante, comme on le voit dans la sous-section suivante.

2.2 Automates contractants, points singuliers et produit(s).

Dans cette sous-section, on s'intéresse à la notion de produit direct de groupe. Il est bien connu que la classe des groupes d'automate est close pour l'opération de produit direct d'automates (voir [26], ou l'introduction). En revanche, il n'est pas clair que les propriétés des automates (réversibilité, activité, contractibilité, ...) soient conservées par l'opération correspondant à ce produit direct, et de fait certaines constructions ne conservent pas ces propriétés. On considère dans cette sous-section un produit qui conserve les caractères contractant et fractal des automates.

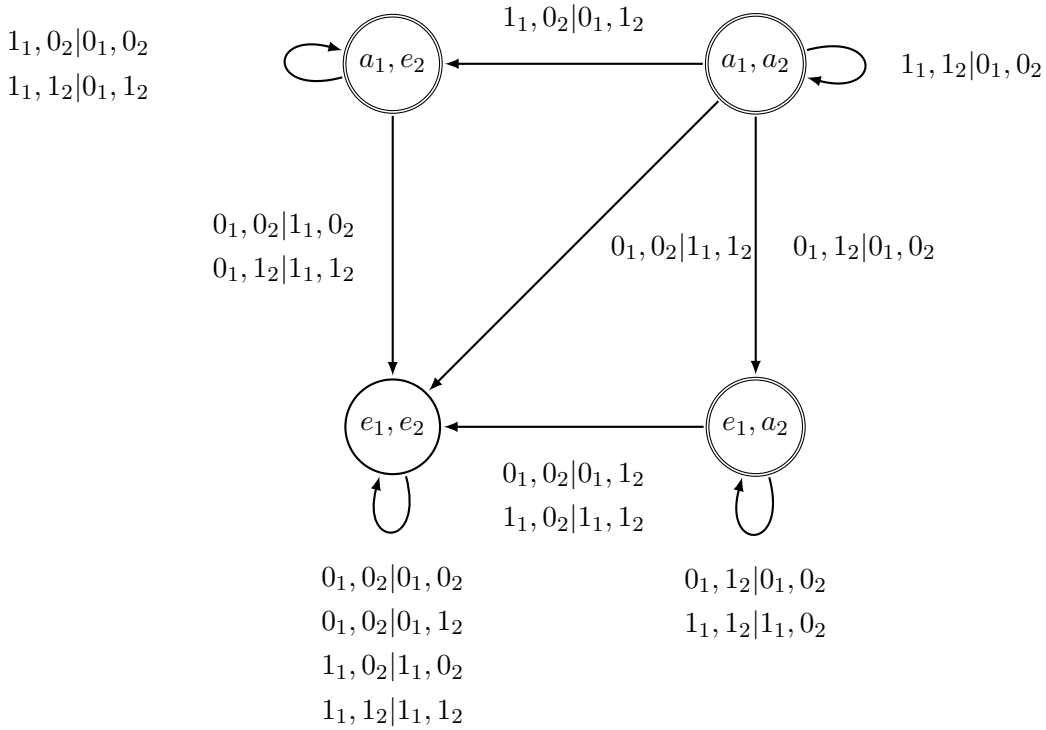


FIGURE III.7 – Construction de Cain pour $\mathbb{Z}^2$.

La construction de Cain pour le produit direct de (semi-)groupes d'automate est :

Proposition 2.8 ([26])

Soient $\mathcal{A} = (Q_1, \Sigma_1, \delta_1, \rho_1)$ et $\mathcal{B} = (Q_2, \Sigma_2, \delta_2, \rho_2)$ deux automates de Mealy inversibles. L'automate $\mathcal{A} \times_C \mathcal{B} = (Q_1 \times Q_2, \Sigma_1 \times \Sigma_2, (\delta_1, \delta_2), (\rho_1, \rho_2))$ appelé *produit direct naturel* des automates engendre le produit direct $\langle \mathcal{A} \rangle \times \langle \mathcal{B} \rangle$.

Cette construction (illustrée figure III.7) fonctionne aussi pour les automates non-inversibles, sous réserve que le produit des semi-groupes soit finiment engendré (ce qui n'est pas toujours le cas).

Pour ce produit, on a de bonnes propriétés de conservation :

Lemme 2.9

Soient $\mathcal{A}$ et $\mathcal{B}$ deux automates engendrant des groupes contractants. Alors le groupe $\langle\mathcal{A}\rangle \times \langle\mathcal{B}\rangle$ engendré par l'automate $\mathcal{A} \times_C \mathcal{B}$ est contractant et son noyau est le produit direct naturel des noyaux de $\mathcal{A}$ et $\mathcal{B}$.

Démonstration. Posons $\mathcal{A} = (Q_1, \Sigma_1, \delta_1, \rho_1)$ et $\mathcal{B} = (Q_2, \Sigma_2, \delta_2, \rho_2)$, et soient $(g, h) \in \langle\mathcal{A}\rangle \times \langle\mathcal{B}\rangle$ et $(\boldsymbol{\xi}, \boldsymbol{\zeta}) \in (\Sigma_1 \times \Sigma_2)^\omega$. Alors $(g, h)_{|(\boldsymbol{\xi},\boldsymbol{\zeta})[:n]} = (g_{|\boldsymbol{\xi}[:n]}, h_{|\boldsymbol{\zeta}[:n]})$ pour tout entier n. Maintenant, par hypothèse, $\mathcal{A}$ et $\mathcal{B}$ sont contractants, et donc pour n assez grand on se retrouve dans le produit des noyaux de ces automates. □

Lemme 2.10

Soient $\mathcal{A}$ et $\mathcal{B}$ deux automates engendrant des groupes fractaux. Alors le groupe $\langle\mathcal{A}\rangle \times \langle\mathcal{B}\rangle$ engendré par l'automate $\mathcal{A} \times_C \mathcal{B}$ est fractal.

Démonstration. Posons $\mathcal{A} = (Q_1, \Sigma_1, \delta_1, \rho_1)$ et $\mathcal{B} = (Q_2, \Sigma_2, \delta_2, \rho_2)$, et soient $(g, h) \in \langle\mathcal{A}\rangle \times \langle\mathcal{B}\rangle$ et $(\boldsymbol{s}, \boldsymbol{t}) \in (\Sigma_1 \times \Sigma_2)^*$. Alors par hypothèse, il existe $g' \in \langle\mathcal{A}\rangle$ avec $g'.\boldsymbol{s} = \boldsymbol{s}$ et $g'_{|\boldsymbol{s}} = g$ (resp. $h' \in \langle\mathcal{A}\rangle$ avec $h'.\boldsymbol{t} = \boldsymbol{t}$ et $h'_{|\boldsymbol{t}} = h$). On obtient $(g', h')_{|(\boldsymbol{s},\boldsymbol{t})} = (\boldsymbol{s}, \boldsymbol{t})$ et $(g', h')_{|(\boldsymbol{s},\boldsymbol{t})} = (g, h)$, donc $\langle\mathcal{A} \times_C \mathcal{B}\rangle$ est fractal. □

On peut maintenant utiliser les méthodes développées précédemment pour analyser les points singuliers de $\mathcal{A} \times_C \mathcal{B}$:

Proposition 2.11

Soient $\mathcal{A}$ et $\mathcal{B}$ deux automates engendrant des groupes contractants et fractaux. Alors on a

$$\kappa(\langle\mathcal{A} \times_C \mathcal{B}\rangle) = \kappa(\langle\mathcal{A}\rangle) \times \kappa(\langle\mathcal{B}\rangle)\,.$$

Ainsi on confirme encore que la classe des automates contractants et fractaux est riche et se prête bien à l'étude des points singuliers.

2.3 Automates biréversibles

On s'intéresse maintenant à une nouvelle classe, les automates biréversibles, c'est-à-dire les automates où les fonctions de transition, de production et de co-transition (les fonctions associées aux lettres en sortie des transitions) sont des permutations. Cette classe est en quelque sorte l'opposée des automates à activité polynomiale, puisque les cycles sont tous co-accessibles dans une composante connexe. Pour ces automates, on peut simplifier le lemme 1.3:

Lemme 2.12

Soit $\mathcal{A}$ un automate biréversible sur l'alphabet Σ. Tout point $\boldsymbol{\xi} \in \Sigma^\omega$ vérifie :

$$\boldsymbol{\xi} \in \kappa \Longleftrightarrow \mathrm{St}_{\langle \mathcal{A} \rangle}(\boldsymbol{\xi}) \neq \mathbb{1} \ .$$

Démonstration. Soit $g \in \mathrm{St}_{\langle \mathcal{A} \rangle}(\boldsymbol{\xi})$ et $\boldsymbol{u} \in \widetilde{Q}^n$ un mot représentant g. Soit il existe ℓ tel que $g_{|\boldsymbol{\xi}[:\ell]} = \mathbb{1}$, et alors comme $\mathcal{A}$ est biréversible, tout élément de la composante (fortement) connexe d'un élément trivial est trivial, d'où $g = \mathbb{1}$. Sinon, pour tout i, $g_{|\boldsymbol{\xi}[:i]} \neq \mathbb{1}$, et par le lemme 1.3, $\boldsymbol{\xi}$ est singulier. □

Cette caractérisation permet de retrouver un résultat de [97]. On dit que l'action de $\langle \mathcal{A} \rangle$ sur Σ^ω est *essentiellement libre* (essentially free [51]), si

$$\mu(\{x \in \Sigma^\omega : \ \mathrm{St}_{\langle \mathcal{A} \rangle}(x) \neq \{\mathbb{1}\}\}) = 0 \, .$$

Steinberg, M. Vorobets et Y. Vorobets ont prouvé dans cette classe un résultat qui peut également être déduit du lemme 2.12 et du théorème 1.5 :

Proposition 2.13 ([97],[29])

L'action d'un automate biréversible est essentiellement libre.

Dans la proposition suivante, on caractérise en terme d'orbite, dans le cas des automates biréversibles, les groupes d'automate sans points singuliers. Il est à noter que cela correspond à avoir tous les stabilisateurs de la frontière triviaux, et qu'aucun exemple d'automate biréversible engendrant une telle action n'est connu [54], d'où la question :

Question 2.14 (GrSa13)

Existe-t-il un automate de Mealy biréversible dont l'ensemble des points singuliers est vide ?

On dit que deux mots sont *cofinaux* s'il existe un indice à partir duquel leurs suffixes commençant à cet indice sont identiques.

Proposition 2.15

Pour un automate biréversible, l'ensemble κ des points singuliers est vide si et seulement si aucun mot infini n'est cofinal avec un autre mot de son orbite selon le groupe engendré par l'automate.

Démonstration. Tout d'abord, supposons que $\boldsymbol{\xi}$ soit cofinal avec $\boldsymbol{\eta} = g.\boldsymbol{\xi} \neq \boldsymbol{\xi}$ (en particulier $g \neq \mathbb{1}$). Comme $\boldsymbol{\xi}$ et $\boldsymbol{\eta}$ sont cofinaux, il existe ℓ satisfaisant $\boldsymbol{\xi}[\ell :] = \boldsymbol{\eta}[\ell :]$. Comme $\mathcal{A}$ est biréversible, on a $g_i := g.\boldsymbol{\xi}[: i] \neq \mathbb{1}$. Mais alors on a $g_\ell.\boldsymbol{\xi}[\ell :] = \boldsymbol{\eta}[\ell :] = \boldsymbol{\xi}[\ell :]$, et donc $\boldsymbol{\xi}[: \ell]$, stabilisé par $g_\ell \neq \mathbb{1}$, est singulier.
Réciproquement si $\langle\mathcal{A}\rangle$ admet un point singulier $\boldsymbol{\xi}$ alors il existe $g \neq \mathbb{1}$ avec $g.\boldsymbol{\xi} = \boldsymbol{\xi}$. Comme $\mathcal{A}$ est biréversible et g est non trivial, il existe $\boldsymbol{v} \in \Sigma^*$ et $f \in \langle\mathcal{A}\rangle$ vérifiant $f.v \neq v$ et $f_{|v} = g$. Et alors $\boldsymbol{v\xi}$ et $f.\boldsymbol{v\xi}$ sont deux mots cofinaux distincts dans la même orbite. □

3 Points singuliers et graphes de Schreier

Si l'on s'intéresse aux graphes de Schreier des points à la frontière de l'arbre Σ^*, on trouve des relations entre les points singuliers d'exemples étudiés dans la section 2 et la topologie des-dits graphes. Dans la suite, on considéra les graphes de Schreier pointés en un mot infini comme un ensemble de graphes, et l'on dira que deux graphes sont proches s'ils coïncident sur une boule de grand rayon centrée en le point marqué. On commence par la proposition suivante :

Proposition 3.1

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate inversible de Mealy. S'il existe $x \in \Sigma$ et $q \in Q$ tels que x est le seul point fixe de ρ_q et que $\delta_x(q) = q$, alors le graphe de Schreier $\mathrm{Sch}\,(x^\omega)$ est isolé dans $\mathrm{Sch}\,(\Sigma^\omega)$.

Démonstration. Soient $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy inversible et $x \in \Sigma$ tels qu'il existe $q \in Q$ avec $\delta_x(q) = q$, $\rho_q(x) = x$ et $\rho_q(y) \neq y, \forall y \in \Sigma \setminus \{x\}$. On cherche à montrer qu'il existe un rayon tel que les boules centrées en des points de $\mathrm{Sch}\,(x^\omega)$ et $\mathrm{Sch}\,(\Sigma^\omega) \setminus \mathrm{Sch}\,(x^\omega)$ ne sont pas isomorphes. Clairement $\mathrm{Sch}\,(x^\omega)$ admet une boucle étiquetée par q sur le sommet x^ω. Comme tout mot différent de x^ω contient une lettre différente de x, il n'est pas fixé par q. Donc $\mathrm{Sch}\,(x^\omega)$ est isolé car c'est le seul graphe ayant une boucle étiquetée par q.
Le même argument fonctionne avec les mots dans l'orbite de x^ω, qui sont les seuls à être à une distance finie d'une boucle étiquetée par q. □

Dans le théorème précédent, on voit que x^ω est un point singulier de $\langle \mathcal{A} \rangle$. Il est facile de voir que le théorème reste valide en remplaçant $x \in \Sigma$ par $\boldsymbol{s} \in \Sigma^*$ ou bien $q \in Q$ par $\boldsymbol{u} \in Q^*$. On peut appliquer le résultat sur l'exemple du groupe des tours de Hanoï (Figure III.3) et l'on obtient :

Corollaire 3.2

Soit $\boldsymbol{\xi}$ un point singulier du groupe de Hanoï H^3. Alors $\mathrm{Sch}\,(\xi)$ est isolé dans $\mathrm{Sch}\,(\Sigma^\omega)$.

Ce corollaire s'applique en particuliers pour les points 0^ω, 1^ω et 2^ω. Il est alors naturel de s'interroger sur le comportement de la suite des graphes de Schreier des mots finis convergeant vers x^ω, $x \in \{0, 1, 2\}$.

Pour $x \in \{0, 1, 2\}$, on considère le grapheΥ_x obtenu à partir de $\mathrm{Sch}\,(x^\omega)$ comme suit :

1. soient deux copies de $\mathrm{Sch}\,(x^\omega)$ avec $g_x \in \{a, b, c\}$ l'étiquette de la boucle sur x^ω ;
2. effacer la boucle de x^ω dans chaque copie de $\mathrm{Sch}\,(x^\omega)$;
3. relier les deux copies par une arête étiquetée par g_x entre les deux sommets x^ω et choisir l'un des sommets x^ω comme sommet marqué.

Cette construction correspond à la dynamique d'évolution des graphes de Schreier des points x^k, comme on peut le voir figure III.8.

Proposition 3.3

Soient $x \in \{0, 1, 2\}$ et $(\boldsymbol{\eta}_n)_n$ une suite d'éléments de $\Sigma^\omega \setminus \{x^\omega\}$ convergeant vers x^ω. Alors la suite $(\mathrm{Sch}\,(\boldsymbol{\eta}_n))_n$ de graphes de Schreier du groupe des tours de Hanoï $H^{(3)}$ converge vers Υ_x quand $n \to \infty$.

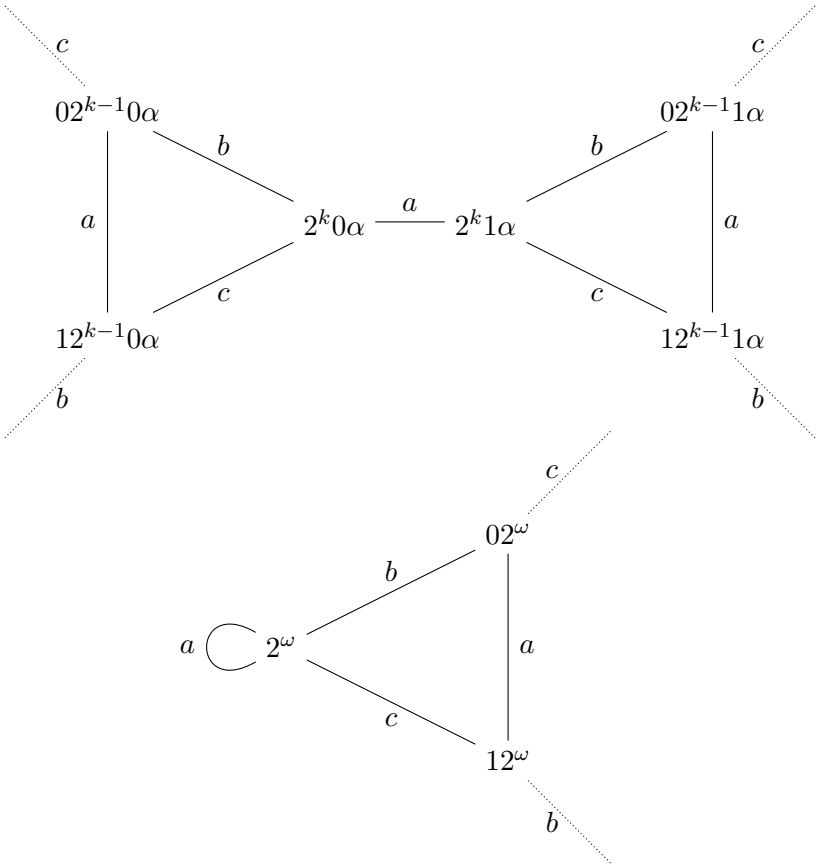


FIGURE III.8 – Une partie d'un graphe de Schreier (infini) de $2^k0\alpha, \alpha \in \Sigma^o mega$ du groupe des tours de Hanoï $H^{(3)}$ (en haut) et du graphe de Schreier (infini) de 2^ω (en bas)

Démonstration. Soit $(z_n)_{n\in\mathbb{N}}$ la suite d'entiers tels que z_n est la position de la première lettre différente de x dans $\boldsymbol{\eta}_n$. De par la structure des graphes de Schreier (finis) de $H^{(3)}$ (voir figure III.8), les boules de rayon $z_n - 1$ dans Υ_x avec x^ω comme centre, et dans $\mathrm{Sch}(\boldsymbol{\eta}_n)$ avec $\boldsymbol{\eta}_n$ comme centre, sont isomorphes. Comme z_n tend vers l'infini avec n, on a le résultat annoncé. □

On peut montrer [20] que les graphes de Schreier infinis du groupe des tours de Hanoï n'ont qu'un seul bout, c'est-à-dire que, si l'on retire une boule de rayon arbitrairement grand on obtient à la limite une unique composante connexe. Comme Υ_x admet deux composantes connexes après que l'on ait supprimé une boule de rayon fini (et a donc deux bouts), ce n'est pas un graphe (infini) de Schreier pour $H^{(3)}$. Plus exactement il n'existe pas de point $\boldsymbol{\xi} \in \Sigma^\omega$ tel que $\mathrm{Sch}(\boldsymbol{\xi})$ soit isomorphe à Υ_x.

Ce lien entre graphes de Schreier isolés (au sens large) et points singuliers semble être prometteur et reste encore largement inexploré.

4 Paires commutantes et pavages de Wang

Dans cette section, on cherche à décrire les points singuliers d'un automate en partant d'un point de vue différent : on part de points spécifiques et "presque singuliers", et on essaie de raffiner pour extraire des points singuliers. Les points "presque singuliers" que nous considérons sont les *paires commutantes* :

Définition 4.1

Une *paire commutante* est un couple $(\boldsymbol{u}, \boldsymbol{s}) \in Q^* \times \Sigma^*$ satisfaisant $\delta_{\boldsymbol{s}}(\boldsymbol{u}) = \boldsymbol{u}$ et $\rho_{\boldsymbol{u}}(\boldsymbol{s}) = \boldsymbol{s}$.

Cette définition a une traduction graphique claire, voir la figure III.9.

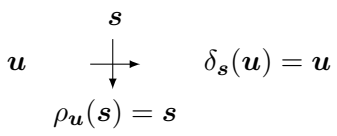


FIGURE III.9 – Une paire commutante $(\boldsymbol{u}, \boldsymbol{s})$.

On peut bien sûr étendre la définition à $\widetilde{Q}^* \times \widetilde{\Sigma}^*$ (on rappelle la notation $\widetilde{A} = A \sqcup A^{-1}$). L'intérêt de ces paires provient de leur proximité avec les points singuliers périodiques : $\boldsymbol{s}^\omega \in \Sigma^\omega$ est singulier si et seulement s'il existe $\boldsymbol{u} \in \widetilde{Q}^*$ tel que $\delta_{\boldsymbol{s}^\omega[:i]}(\boldsymbol{u}) \neq \mathbb{1}$ pour tout i. Comme l'existence de points singuliers est équivalente à l'existence de points singuliers périodiques (lemme 1.4), on peut ainsi espérer étudier les paires commutantes d'un automate et obtenir des informations sur ses points singuliers.

D'autre part, les paires commutantes sont liées aux graphes en hélice de la manière suivante :

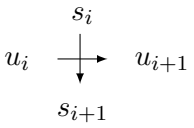
Lemme 4.2

Soit $\mathcal{A}$ un automate inversible et soit

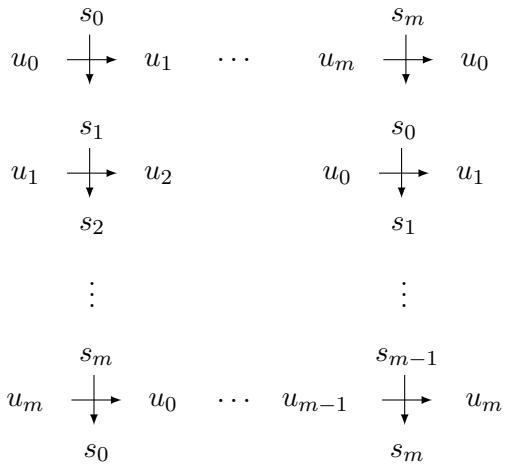
$$(u_0, s_0) \to (u_1, s_1) \to \cdots \to (u_m, s_m) \to (u_0, s_0)$$

un cycle dans son graphe en hélice $\mathcal{H}_{n,k}$ (*resp.* $\widetilde{\mathcal{H}_{n,k}}$). Alors $(u_0u_1\cdots u_m,\ s_0s_1\cdots s_m)$ est une paire commutante dans $Q^* \times \Sigma^*$ (*resp.* $\widetilde{Q}^* \times \widetilde{\Sigma}^*$).

Démonstration. On a (modulo $m+1$) le diagramme en croix :



ce qui nous permet d'écrire :



On obtient notre paire commutante en lisant les côtés de ce carré (et on voit aussi que les permutations circulaires synchrones–c'est à dire que le décalage d'indice doit être le même pour les deux mots–de cette paire de mots sont aussi des paires commutantes). □

On en déduit qu'il existe une multitude de paires commutantes.

Lemme 4.3

Tout automate de Mealy $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ admet une paire commutante dans $Q^* \times \Sigma^*$ (*resp.* $\widetilde{Q}^* \times \widetilde{\Sigma}^*$).

Démonstration. Considérons le graphe en hélice $\mathcal{H}_{n,k}$ d'ordre n, k (*resp.* le graphe en hélice étendu $\widetilde{\mathcal{H}_{n,k}}$). Ce graphe est fini et tous ses sommets sont de degré sortant 1. Il admet donc un cycle qui est, d'après le lemme 4.2, une paire commutante. □

À l'aide de ces paires commutantes on recherche des points singuliers. Pour cela on met en relation l'action de l'automate avec les *pavages de Wang*. Cette relation (plus exactement la traduction inverse) a aussi été exploitée indépendamment par Jeandel et Rao pour rechercher le plus petit ensemble de tuiles de Wang pavant le plan de manière apériodique [59], et était implicitement présente dans le travail de Glasner et Mozes [42].

Une *tuile de Wang* est un carré dont chaque coté (gauche, droite, haut, bas) porte une couleur. Le *problème du domino*, formulé par Wang en 1961 [103], consiste à décider s'il existe un pavage du plan qui n'utilise que des tuiles provenant d'un ensemble donné. Berger a montré en 1966 que ce problème est indécidable. Ce problème est ensuite devenu un classique des problèmes indécidables en informatique théorique, et a été utilisé notamment par Kari pour montrer que le problème de la nilpotence pour les automates cellulaires est indécidable [61], ou encore par Gillibert pour montrer que les problèmes de l'ordre et de la finitude sont indécidables pour les semi-groupes d'automate [41].

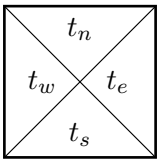


FIGURE III.10 – Une tuile de Wang.

Formellement, une *tuile de Wang* est un quadruplet $(t_w, t_s, t_e, t_n) \in \mathcal{C}^4$ où $\mathcal{C}$ un ensemble fini de couleurs. Un jeu de tuile $\mathcal{T}$ est un ensemble fini de tuiles de Wang, et l'on dit que $\mathcal{T}$ *pave* le plan s'il existe une fonction $f : Z^2 \to \mathcal{T}$ vérifiant $f(x, y)_e = f(x+1, y)_w$ et $f(x, y)_n = f(x, y+1)_s$, pour tout point (x, y) de $\mathbb{Z}^2$. On étend la fonction de pavage aux rectangles de $\mathbb{Z}^2$.

On dit qu'un *pavage* est *périodique* s'il existe un vecteur v de $\mathbb{Z}^2$ tel que, pour tout point $t \in \mathbb{Z}^2$, on a $f(t + v) = f(t)$.

Comme dans [70], nous dirons qu'un jeu de tuiles $\mathcal{T}$ est *sw-déterministe* si la donnée de t_w et de t_s détermine au plus une tuile de $\mathcal{T}$; et de même pour *se*, *ne* ou *nw*. Si un pavage est tout à la fois *sw*-, *se*-, *ne*- et *nw*-, on dit que le jeu est *4-way déterministe*.
À un automate de Mealy $\mathcal{A}$, il y a une manière naturelle d'associer un jeu $\mathcal{T}(\mathcal{A})$ de tuiles de Wang : pour chaque transition $q \xrightarrow{x|y} p$ on associe la tuile de Wang (q, x, p, y) avec les couleurs $\mathcal{C} = Q \sqcup \Sigma$.

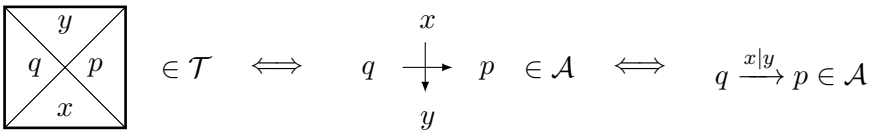


FIGURE III.11 – Le jeu de tuiles $\mathcal{T}(\mathcal{A})$ associé à l'automate $\mathcal{A}$.

Lemme 4.4

Le jeu de tuiles associé à un automate de Mealy est nécessairement *sw*-déterministe. De plus, pour un automate $\mathcal{A}$, on a :

- $\mathcal{T}(\mathcal{A})$ est également *se*-déterministe si et seulement si $\mathcal{A}$ est réversible ;
- $\mathcal{T}(\mathcal{A})$ est également *nw*-déterministe si et seulement si $\mathcal{A}$ est inversible ;
- $\mathcal{T}(\mathcal{A})$ est 4-way déterministe si et seulement si $\mathcal{A}$ est biréversible.

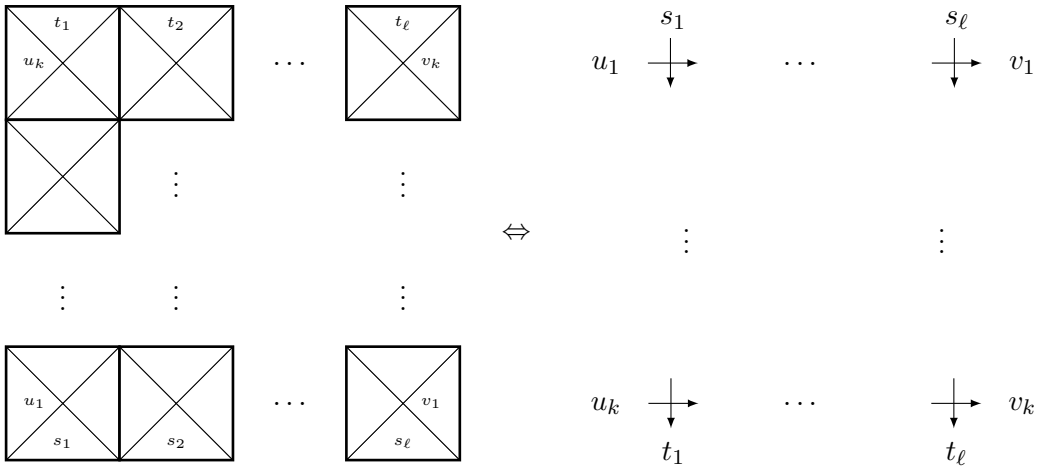
Il y a une forte correspondance entre pavages de Wang (issus d'un jeu de tuiles déterministe) et action d'un automate, ainsi que l'illustre la figure III.12. Cette correspondance s'étend aux mots infinis de manière directe.

On peut alors remarquer que l'existence d'une paire commutante dans l'automate induit l'existence d'un pavage périodique construit avec le jeu de tuiles associé :

Lemme 4.5

Soit (q, x) (*resp.* $(\boldsymbol{u}, \boldsymbol{s})$) une paire commutante de $\mathcal{A}$ dans $Q \times \Sigma$ (*resp.* $Q^n \times \Sigma^k$). Alors la tuile (*resp.* le rectangle) associée à (q, x) (*resp.* $(\boldsymbol{u}, \boldsymbol{s})$) dans $\mathcal{T}(\mathcal{A})$ pave le plan.

Démonstration. C'est une application directe de la correspondance de la figure III.12. □



$$\Leftrightarrow$$

$$\rho_{u_1 \cdots u_k}(s_1 \cdots s_\ell) = t_1 \dots t_\ell$$

$$\Leftrightarrow$$

$$\delta_{s_1 \cdots s_\ell}(u_1 \cdots u_k) = v_1 \dots v_k$$

FIGURE III.12 – Correspondance entre pavages partiels, diagrammes en croix et actions de l'automate.

De là on obtient, grâce au lemme 4.3 l'existence d'un pavage périodique pour tout jeu de tuiles associé à un automate de Mealy :

Corollaire 4.6

Le jeu de tuiles associé à un automate de Mealy permet de construire un pavage périodique du plan.

Malheureusement, rien ne garantit que ces paires commutantes $(\boldsymbol{u}, \boldsymbol{s})$ aient un réel intérêt dans le groupe engendré par l'automate : il se peut que $\boldsymbol{u}$ représente l'élément neutre du groupe, ou bien que l'on ait $\boldsymbol{u}_{|\boldsymbol{s}^\omega[:i]} = \mathbb{1}$ à partir d'un certain i.
Pour éviter cela, on peut commencer par restreindre le jeu de tuiles, et, par exemple, ne pas considérer les tuiles colorées par e quand e est un état trivial de l'automate. On définit une paire commutante restreinte à $Q' \subset Q$ comme un couple $(\boldsymbol{u}, \boldsymbol{s}) \in Q'^* \times \Sigma^*$, satisfaisant $\delta_{\boldsymbol{s}}(\boldsymbol{u}) = \boldsymbol{u}$ et $\rho_{\boldsymbol{u}}(\boldsymbol{s}) = \boldsymbol{s}$. Cela nous conduit à considérer le problème suivant :

`Paires commutantes restreintes` :

— **entrée :** $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ et $Q' \subsetneq Q$.

— **sortie :** `oui` si et seulement si $\mathcal{A}$ admet une paire commutante restreinte à Q'.

Ce problème se révèle indécidable, ce qui contraste avec la facilité à trouver une paire commutante non restreinte. Pour le montrer, on utilise la connexion entre les automates de Mealy et les pavages de Wang, et on se sert des résultats d'indécidabilité provenant de ce domaine. En particulier, même si le jeu de tuiles présente des caractéristiques de déterminisme, le problème du domino reste indécidable [61, 72, 70].

Pour obtenir ce résultat d'indécidabilité, on réduit le problème du domino pour les jeux de tuiles 4-way déterministes à un sous-problème de `Paires commutantes restreintes` . On commence par construire un automate de Mealy à partir d'un jeu de tuiles 4-way déterministe.

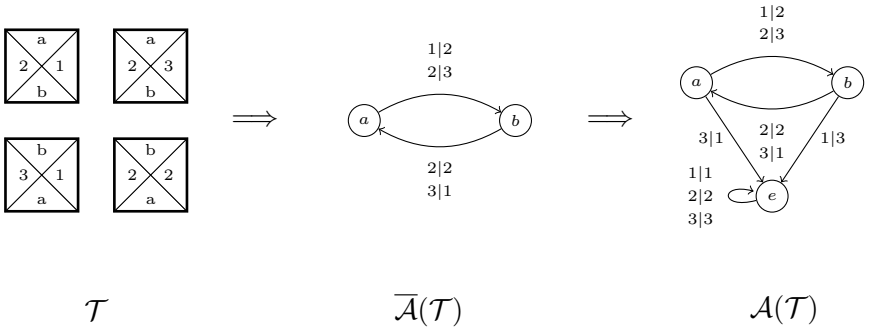


FIGURE III.13 – Construction d'un automate Mealy inversible à partir d'un jeu de tuiles 4-way déterministe.

Soit $\mathcal{T}$ un jeu de tuiles 4-way déterministe. On construit un automate $\overline{\mathcal{A}}(\mathcal{T})$ selon la procédure décrite figure III.11. Cet automate n'est pas complet en général. En revanche, comme le jeu de tuiles est 4-way déterministe, on peut compléter $\overline{\mathcal{A}}(\mathcal{T})$ en y ajoutant un état-puits e et des transitions supplémentaires vers cet état-puits, voir la figure III.13. On obtient alors un automate de Mealy inversible $\mathcal{A}(\mathcal{T})$.

Par cette construction, on a :

Théorème 4.7

Le problème `Paires commutantes restreintes` est indécidable.

Démonstration. On va montrer qu'une instance particulière de `Paires commutantes restreintes`

est indécidable. Prenons Q' l'ensemble des états privé des états induisant des actions triviales dans le groupe (cet ensemble est décidable car le problème du mot l'est).
`Paires commutantes non-élémentaires` :

— **entrée :** $\mathcal{A}$ un automate Mealy.

— **sortie :** `oui` si et seulement si $\mathcal{A}$ admet une paire commutante n'utilisant pas d'état trivial.

D'après [70], trouver un pavage *périodique* étant donné un jeu de tuiles 4-way déterministe est indécidable. Or, à partir d'un tel jeu de tuiles $\mathcal{T}$, on construit un automate de Mealy inversible $\mathcal{A}(\mathcal{T})$, et, comme toute paire commutante non élémentaire évite l'état-puits par définition, trouver une paire commutante non élémentaire permet de construire un pavage (périodique) du plan par des tuiles de $\mathcal{T}$. □

5 Conclusion

La notion de points singuliers abordée dans ce chapitre nous a mené vers deux réflexions : une analyse, présentée dans ce chapitre, qui a permis de décrire et mieux comprendre la structure des points singuliers d'un groupe d'automate à l'aide de l'automate de Mealy sous-jacent ; mais aussi à retrouver et renforcer le lien entre automates de Mealy et pavages de Wang. Ce lien avait déjà été noté par Gillibert du côté (semi-)groupes d'automate et par Kari, repris récemment par Jeandel et Rao du côté pavage, et semble extrêmement fertile.

Si on a ici utilisé les pavages comme un outil conduisant à des résultats d'indécidabilité, il est aussi possible de mener nos recherches dans l'autre sens : *est-il possible d'exhiber au moyen d'automates de Mealy et de graphes en hélice des ensemble intéressants de tuiles de Wang ?* Nous avons essayé de répondre à ce problème dans notre papier avec D'Angeli, Klimann, Picantin et Rodaro, et avons abouti à des résultats partiels pour des ensembles de tuiles présentant de nombreuses symétries, mais ces résultats préliminaires mettent en lumière l'intérêt de considérer ces notions ensemble partiels, ainsi que d'autres notions proches, telle la notion d'automate synchronisant.

Cette étude nous conduit aussi à nous interroger sur les relations que peuvent entretenir automates de Mealy et automates cellulaires. Les automates cellulaires sont en effet un domaine de l'informatique théorique proche des pavages de Wang et des sous-shifts qui possèdent des outils et des questions qui ressemblent étrangement à des problématiques que l'on trouve dans la théorie des automates de Mealy. Bien sûr, les automates de Mealy et les automates cellulaires peuvent tous les deux être étudiés dans le cadre de la dynamique symbolique, et l'on peut introduire dans la théorie des automates cellulaires des notions de groupes et semi-groupes qui en accroissent la puissance, mais de manière plus profonde on retrouve des relations dans les preuves concernant ces objets.
Gillibert [41] a utilisé des résultats venant en fait de ces automates cellulaires pour montrer l'indécidabilité du problème de finitude pour les semi-groupes d'automate. Dans un travail récent

et toujours en cours, Delacourt et Ollinger ont étendu le lien trouvé par Gillibert et réussi à relier la finitude pour les automates de Mealy inversibles à un problème de périodicité pour les automates cellulaires unidirectionnels permutifs, ce qui tend à suggérer que le problème est indécidable.
Il semble donc très naturel de continuer dans cette voie et d'essayer de lier d'autres problèmes de décision et notions de dynamique entre ces objets. Là encore la notion de transducteur jouera vraisemblablement un rôle central.

Chapitre IV

Génération aléatoire de groupes

En mathématiques discrètes, si l'on s'intéresse à une famille fixée, il est souvent pertinent de chercher un moyen de générer des éléments de cette famille de manière aléatoire, selon une distribution prédéfinie (ou tout du moins connue). C'est un moyen intéressant pour formuler des conjectures, tester leur robustesse, ou trouver des comportements inconnus ou contre-intuitifs. Par exemple, Berlinkov [16] et Nicaud [80] ont prouvé respectivement qu'un automate est génériquement [1] synchronisant et que le plus court mot synchronisant est de taille inférieure à $n^{1+\epsilon}$ (c'est-à-dire que la conjecture de Černý est génériquement vraie). À l'opposé, Erdős ([33, 32]) a été le premier dans les années 50 à utiliser la théorie des probabilités pour prouver l'existence d'objets satisfaisant une propriété donnée, en montrant que la probabilité que la-dite propriété soit satisfaite était non nulle.

Dans le cas des groupes, deux situations sont à distinguer, selon que l'on souhaite obtenir des groupes infinis ou finis.
Dans le cas infini (finiment engendré) plusieurs approches complémentaires sont possibles : on peut tirer de manière aléatoire des relations, ou bien des graphes décrivant la structure du groupe, et on obtient typiquement des résultats de la forme "si le paramètre est plus petit que α alors le groupe satisfait génériquement la propriété P_1, sinon il satisfait génériquement la propriété P_2". L'exemple historique de Gromov prend pour paramètre la densité des relations, avec $\alpha = 1/2$, et comme propriétés l'infinitude et l'hyperbolicité contre la trivialité. Pour une introduction plus complète à la génération de groupes infinis, on pourra se référer à [82], ou bien à la série d'articles [12, 14, 13, 11].

1. Dans toute la thèse, *génériquement* signifiera "avec une probabilité qui tend vers 1 à mesure que le paramètre augmente". Dans notre cas le paramètre sera le nombre de lettres de l'automate.

Dans le cas des groupes finis, une idée naturelle est de tirer aléatoirement des permutations et de regarder le groupe qu'elles engendrent. En effet, le théorème de Cayley affirme :

Théorème 0.1 (Cayley)

Soit G un groupe d'ordre k. Alors G est un sous-groupe du groupe symétrique agissant sur G, *i.e.* $G \leq S_k$.

Démonstration. Soit S_G le groupe des bijections de G dans G. Définissons, pour tout $g \in G$ la fonctions $\tau_g : G \to G, \quad x \mapsto g.x$. Clairement chaque τ_g est une bijection et $\{\tau_g \mid g \in G\}$ a une structure de sous-groupe dans S_G. De plus ce sous-groupe est isomorphe à G ; d'où le résultat. □

Cependant cette approche se heurte à un écueil majeur : les distributions qui en découlent sont dégénérées. Si l'on choisit de ne tirer qu'une permutation σ, alors le groupe engendré est $\langle\sigma\rangle = \{\sigma^i | i \in \mathbb{N}\}$, c'est-à-dire, comme σ est d'ordre fini, un groupe cyclique. On peut d'ailleurs noter que la taille de ce groupe est relativement bien connue : la distribution du logarithme de l'ordre d'une permutation aléatoire satisfait un théorème central limite :

Théorème 0.2 (Erdős-Turan 1967 [34])

Soit σ une permutation aléatoire de S_k. On a, pour tout y positif :

$$\lim_{k\to\infty} \mathbb{P}\left(\frac{\log|\sigma| - \log^2 k}{\frac{1}{\sqrt{3}\log^{3/2} k}} < y\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{\frac{-v^2}{2}} dv \,.$$

Cependant, si l'on décide de tirer plusieurs permutations et de considérer le groupe ainsi obtenu on tombe sur le théorème de Dixon (conjecturé par Netto en 1882 [79]).

Théorème 0.3 (Dixon 1969 [31])

Soient σ et τ deux éléments de S_k choisis aléatoirement. On a

$$\lim_{k\to\infty} \mathbb{P}\left(\langle\sigma,\tau\rangle = S_k \text{ or } A_k\right) = 1 \,.$$

En d'autre termes, l'idée naturelle mais naïve de tirer des permutations pour engendrer des groupes de manière variée est vouée à l'échec. Le théorème de Dixon ayant été étendu [71] à tout

groupe fini simple [2] (si l'on tire au hasard deux éléments d'un groupe fini simple alors le groupe engendré est génériquement le groupe entier), il est donc nécessaire de trouver une nouvelle approche, un nouveau paradigme, pour la génération de groupes finis.

Il est facile de voir que les automates de Mealy permettent d'engendrer tous les groupes finis. Considérons un groupe fini. D'après le théorème de Cayley, il est engendré par des permutations $\sigma_1, \dots \sigma_i$. Alors l'automate présenté figure IV.1 engendre ce groupe. En fait il est même possible,

FIGURE IV.1 – Un automate de Mealy engendrant le groupe fini $\langle \sigma_1, \dots \sigma_i \rangle$.

étant donnés deux groupes, de trouver un automate engendrant ces deux groupes. C'est la proposition 2.8 : Si G et H deux (semi-)groupes finis, il existe un automate de Mealy $\mathcal{A}$ qui engendre G et dont le dual engendre H.

Il est donc raisonnable d'essayer d'engendrer des groupes finis aléatoires en tirant non plus de simples permutations mais des automates de Mealy, avec l'espoir que la structure supplémentaire créera une plus grande diversité de groupes. Malheureusement, on ne sait pas en général si un automate donné engendre un groupe fini (c'est même indécidable pour les semi-groupes d'automate [41]), et on ne peut donc pas juste tirer aléatoirement n'importe quel automate, d'autant que les algorithmes de rejet offrent empiriquement des performances médiocres dans notre situation.
En revanche, il existe des classes n'engendrant que des groupes finis ou infinis. Par exemple, si l'automate est inversible, réversible mais pas biréversible (*i.e.* si une lettre de sortie ne définit pas une permutation des états de l'automate), alors le groupe engendré est infini [1].
Du côté des groupes finis, Antonenko et Russeiev ont indépendamment étudié les automates *avec cycles sans échappatoire* qui engendrent uniquement des groupes finis (voir [3, 86]). Graphiquement, cela signifie que l'automate est un graphe orienté sans cycle (DAG) (sans boucle sur les sommets) dont les feuilles sont des cycles sans échappatoire, d'où le nom. Un exemple d'un tel automate est présenté figure IV.2. Klimann et Picantin ont montré dans [66] que cette classe est maximale en cela que, pour tout automate $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ n'appartenant pas à cette classe, il existe un ensemble de fonctions de production inversibles ρ' tel que $\mathcal{A}' = (Q, \Sigma, \delta, \rho')$ engendre

2. Un groupe est *simple* s'il ne possède pas de sous-groupe normal non trivial. Le théorème de Jordan-Holdër affirme que tout groupe fini est construit de manière unique (à ordre et isomorphisme près) par une suite d'extensions par des groupes finis simples. On peut donc voir ces groupes comme les briques élémentaires, l'équivalent pour les groupes finis des nombres premiers.

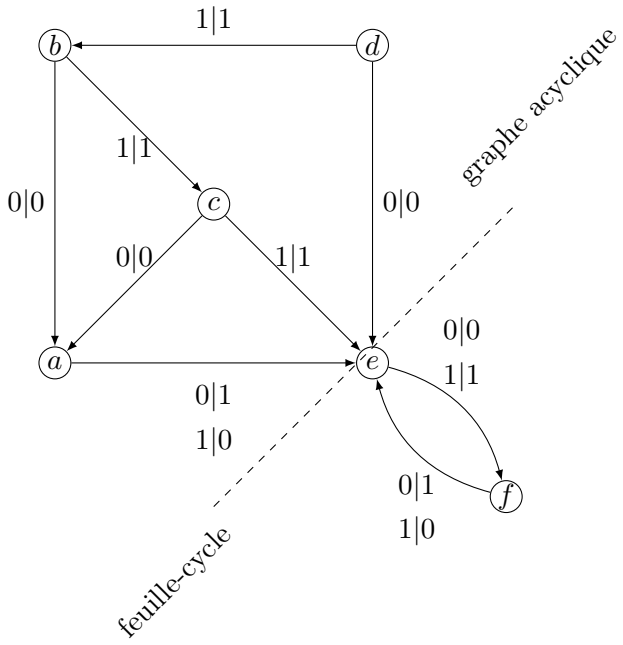


FIGURE IV.2 – Un automate avec cycles sans échappatoire, engendrant un groupe d'ordre 256.

un groupe infini, tandis qu'Antonenko a démontré l'équivalent dans le cadre des semi-groupes [3]. On va essayer d'engendrer des groupes en tirant des automates dans cette classe.

De fait, on commence par étudier un cas encore plus simple en considérant des sous-classes d'automates avec cycles sans échappatoire. Par exemple, les automates de la forme de l'automate figure IV.1, où chaque fonction de transition vaut l'identité, forment une sous-classe dans laquelle on peut directement appliquer le théorème de Dixon. On va s'intéresser à une classe moins simple et reliée aux automates étudiés par Antonenko et Russyev : les automates cycliques, c'est-à-dire les automates, tels ceux dessinés figures IV.3 et IV.4, où il existe une numérotation des états telle que δ soit la fonction additionnant 1 (selon un modulo). Cette classe correspond aux feuilles des automates avec cycles sans échappatoire, ainsi qu'à l'intersection de cette classe avec la classe des automates de Mealy biréversibles.

Dans ce chapitre, dont le matériel fait l'objet de l'article [44] on démontre un analogue au théorème de Dixon pour ces automates. Ce théorème a deux répercussions principales : la première, immédiate, est que cette classe n'est pas adaptée à la génération aléatoire, la deuxième est que, puisque ces automates cycliques sont les feuilles des automates à cycles sans échappatoire, c'est en fait toute la classe des automates à cycles sans échappatoire qui n'est pas adaptée à ce problème, ce qui suggère, ainsi qu'il est discuté section 4, qu'il est nécessaire d'avoir une structure plus complexe pour obtenir une distribution pertinente.

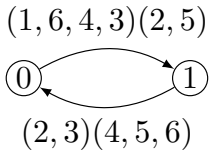


FIGURE IV.3 – Un automate cyclique à 6 lettres et 2 états, engendrant S_6^2.

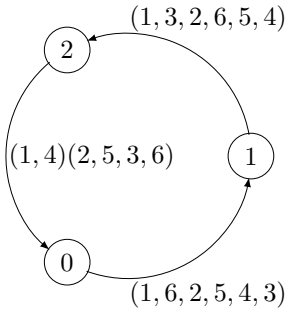


FIGURE IV.4 – Un automate cyclique à 6 lettres et 3 états, engendrant $(A_6 \times A_6 \times A_6) \rtimes \langle (1, \pi, \pi) \rangle_c$.

1 Automates cycliques

1.1 Groupe engendré par un automate cyclique

Dans cette section, on s'intéresse aux groupes engendrés par les automates cycliques, ainsi qu'à leur présentation. Comme il n'y a pas d'ambiguïté, on dessine les transitions des automates cycliques $x \xrightarrow{\rho_x} \delta(x)$ au lieu de $x \xrightarrow{i|\rho_x(i)} \delta_i(x)$, toutes les lettres menant vers le même état (*i.e.* $\delta_x(q) = \delta_y(q)$ pour tous x, y dans Σ et tout état q).

On va commencer par raffiner le résultat d'Antonenko et Russyev en montrant que le groupe engendré par un automate cyclique est un sous-groupe d'un groupe dépendant explicitement de la structure de l'automate :

Proposition 1.1

Soit $\mathcal{A}$ un automate cyclique à n états sur un alphabet à k lettres. Alors $\langle \mathcal{A} \rangle \leq S_k^n$.

Démonstration. Posons $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ avec $Q = \{0, 1, \dots n-1\}$ et $|\Sigma| = k$. Comme l'automate est formé d'un unique cycle, on peut sans perte de généralité renommer les états de manière à ce que $\delta_i(q) = q + 1 \bmod n$ (avec le changement de notation précédent). Soit un mot $\boldsymbol{s} = i_0 \dots i_\ell \in \Sigma^*$. On a $\rho_q(\boldsymbol{s}) = \rho_q(i_0)\rho_{q+1}(i_1) \dots \rho_{q+\ell \bmod n}(i_\ell)$. L'état q agit sur Σ^* comme un état isolé portant le vecteur de permutations $(\rho_q, \rho_{q+1}, \dots, \rho_{q+n-1 \bmod n}) \in S_k^n$, et comme il en va de même pour les autres états, on obtient bien $\langle \mathcal{A} \rangle \leq S_k^n$. □

Remarque 1.2

On remarque que ce résultat peut être obtenu par des méthodes de théorie des automates : $\mathfrak{d}(\mathfrak{d}\mathcal{A})^n$ est formé d'une union disjointe d'états portant le vecteur de permutations $(\rho_q, \rho_{q+1}, \ldots, \rho_{q+n-1 \bmod n}) \in S_k^n$, et comme prendre les puissances dans le dual ne modifie pas le groupe engendré par le primal, on retrouve le résultat.

On a démontré que

$$\langle \mathcal{A} \rangle = \langle (\rho_0, \rho_1, \ldots, \rho_{n-1}), (\rho_1, \rho_2, \ldots, \rho_{n-1}, \rho_1), \ldots, (\rho_{n-1}, \rho_0, \ldots, \rho_{n-2}) \rangle \ .$$

On dit alors que $\langle \mathcal{A} \rangle$ est engendré *circulairement* par le vecteur $(\rho_0, \rho_1, \ldots, \rho_{n-1})$, ce que l'on note $\langle \mathcal{A} \rangle = \langle (\rho_0, \rho_1, \ldots, \rho_{n-1}) \rangle_c$.

Remarque 1.3

On peut déjà souligner que la distribution obtenue en sélectionnant aléatoirement des automates cycliques, c'est-à-dire en considérant $\langle (\rho_0, \rho_1, \ldots, \rho_{n-1}) \rangle_c$ pour un vecteur aléatoire de permutations, n'est pas la même que celle provenant d'un tirage aléatoire d'éléments de S_k^n. En effet, pour un automate cyclique la probabilité obtenir l'automate trivial vaut $1/k!^n$, puisqu'il ne faut alors sélectionner que des permutations triviales. Si l'on regarde le groupe engendré par ℓ éléments de S_k^n, cette probabilité vaut $(1/k!^n)^\ell$. Les distributions ne pourraient donc être identiques que si l'on ne tirait qu'un unique vecteur de S_k^n, mais dans ce cas le groupe obtenu est un produit direct de groupes cycliques, ce qui n'est pas le cas en général pour $\langle (\rho_0, \rho_1, \ldots, \rho_{n-1}) \rangle_c$.

Il est en fait possible d'affiner encore la borne supérieure de la proposition précédente. On raisonne par analogie avec le théorème de Dixon : dans celui-ci, on a que, dans à peu près un quart des cas, le groupe engendré est le groupe alterné A_k. Cela s'explique simplement, car si les deux permutations tirées sont de signatures paires, alors tous les éléments du groupe engendré par ces permutations ont une signature paire, et on ne peut donc pas obtenir le groupe symétrique en entier.
De même, si toutes les permutations ρ_i sont de signatures paires, alors le groupe engendré par l'automate cyclique portant ces permutations sera un sous-groupe de A_k^n. On généralise cela en commençant par étendre la notion de signature à S_k^n, composante par composante, et en la notant toujours $\operatorname{sgn}() : S_k^n \to (\mathbb{Z}/2\mathbb{Z})^n$. De plus, pour $(\sigma_0, \ldots, \sigma_{n-1}) \in S_k^n$ et π une transposition

quelconque de S_k, on pose

$$\mathrm{sgn}_\pi(\sigma_0,\dots,\sigma_{n-1}) = (\pi^{\frac{1-\mathrm{sgn}(\sigma_0)}{2}},\dots,\pi^{\frac{1-\mathrm{sgn}(\sigma_{n-1})}{2}}).$$

On rappelle également la notion de *produit semi-direct* de groupes : soient H et K tels $H\cap K = \{1\}$ et K agit sur H par conjugaison, alors le produit semi-direct (interne) de H par K, noté $H\rtimes K$, est $G = HK$ avec comme multiplication entre $g_1 = (h_1,k_1)$ et $g_2 = (h_2,k_2)$ la formule $g_1\cdot g_2 = (h_1k_1^{-1}h_2k_1, k_1k_2) = (h_1h_2{}^{k_1}, k_1k_2)$. Réciproquement, G est le produit semi-direct de ses sous-groupes H et K si H est distingué et tout élément de G s'écrit de manière unique comme produit d'un élément de H et d'un élément de K.
Par exemple, S_k est le produit semi-direct de A_k et $\langle(1,2)\rangle$ (en fait de tout sous-groupe engendré par une transposition), soit $S_k = A_k\rtimes\langle(1,2)\rangle$, et de la même façon $S_k^n = A_k^n\rtimes\langle((1,2),\mathbb{1},\dots,\mathbb{1})\rangle_c$. On peut de même s'intéresser aux produits semi-directs de $A_k^n\rtimes\Pi$, où Π est un sous-groupe engendré par des vecteurs de transpositions. Cela nous permet d'obtenir :

Proposition 1.4

Soit $\mathcal{A}$ un automate cyclique à n états sur un alphabet à k lettres et ayant comme fonctions de production $\{\rho_0,\dots\rho_{n-1}\}$. Alors $\langle\mathcal{A}\rangle \le A_k^n\rtimes\langle\mathrm{sgn}_\pi(\rho_0,\dots,\rho_{n-1})\rangle_c$, où π est une transposition quelconque de S_k.

Démonstration. On remarque comme pour la proposition 1.1 que chaque état est équivalent à un élément $(\rho_i,\dots,\rho_{i+n-1 \bmod n})$ de S_k^n. Comme S_k^n est isomorphe à $A_k^n\rtimes\langle((1,2),\mathbb{1},\dots,\mathbb{1})\rangle_c$, on peut aussi écrire l'action ρ_i comme $\left((\overline{\rho_i},\dots,\overline{\rho_{i+n-1 \bmod n}}),(\pi^{\frac{\mathrm{sgn}(\rho_i)-1}{2}},\dots,\pi^{\frac{\mathrm{sgn}(\rho_{i+n-1 \bmod n})-1}{2}})\right)$, où $\overline{\rho}$ est la projection canonique de ρ dans A_k et π est une transposition quelconque de S_k. □

Dans ce qui suit on montre un analogue du théorème de Dixon pour les automates cycliques, au sens où l'on montre que le groupe engendré par un automate cyclique aléatoire est génériquement le plus grand possible, à savoir la borne supérieure donnée par la proposition 1.4.

Avant cela on va s'intéresser un instant au cas où l'automate est formé d'une union de plusieurs automates cycliques.

1.2 Union d'automates cycliques

En dehors de la curiosité naturelle, il est pertinent de regarder l'union d'automates cycliques car elle apparaît quand on considère les "feuilles" des automates avec cycles sans échappatoire.

De plus cette étude a permis de réfuter une conjecture émise par Klimann, Mairesse et Picantin dans [65].

Proposition 1.5

Soit $I = \{1, \dots, m\}$ et $\mathcal{A} = \bigsqcup_{i \in I} \mathcal{A}_i$ l'automate formé de l'union disjointe d'automates cycliques $\mathcal{A}_i$, chacun ayant n_i états et k_i lettres, et pour transitions $\{\rho_{i,j}\}_{j<n_i}$. Alors, si l'on pose $k = \max_i(k_i)$ et $n = \operatorname{ppcm}_I(n_i)$, on a

$$\langle \mathcal{A} \rangle \leq A_k^n \rtimes E\,,$$

où $E \leq (\mathbb{Z}/2\mathbb{Z})^n$ est d'ordre au plus 2^u, avec

$$u = \sum_{i=1}^{m} (-1)^{i-1} \sum_{i_1 < i_2 < \dots < i_j} \gcd(n_{i_1}, \dots, n_{i_j})\,. \tag{IV.1}$$

Démonstration. Dans un premier temps on va montrer que $\langle \mathcal{A} \rangle \lesssim S_k^{\operatorname{ppcm}_I(n_i)}$: comme pour la proposition 1.1, on peut montrer que $\rho_{i,j}$ agit sur dans $\langle \mathcal{A} \rangle_i$ comme $(\rho_{i,j}, \rho_{i,j+1}, \dots, \rho_{i,j+n_i-1 \bmod n_i}) \in S_{k_i}^{n_i}$. Clairement, ces permutations se plongent dans $S_k^{\operatorname{ppcm}_I(n_i)}$, d'où la borne supérieure globale (qui se trouve effectivement être atteinte).
Pour préciser E et surtout u, on va raisonner par inclusion-exclusion.
Posons $E = \langle \{\operatorname{sgn}_\pi(\rho_{i,0}, \dots, \rho_{i,n_i-1}, \rho_{i,0}, \dots, \rho_{i,n_i-1}\}_{i \in I}) \rangle_c \leq (\mathbb{Z}/2\mathbb{Z})^{\operatorname{ppcm}_I(n_i)}$.
Les vecteurs $\operatorname{sgn}_\pi(\rho_{i,0}, \dots, \rho_{i,n_i-1}, \rho_{i,0}, \dots, \rho_{i,n_i-1})$ sont périodiques, de période n_i, donc les groupes $E_i := \langle \operatorname{sgn}_\pi(\rho_{i,0}, \dots, \rho_{i,n_i-1}, \rho_{i,0}, \dots, \rho_{i,n_i-1}) \rangle_c$ sont des sous-groupes des groupes $P_i := \langle (1,0,0,\dots,0,1,0,\dots,0) \rangle_c$ (où le vecteur est de taille $\operatorname{ppcm}_I(n_i)$, de période p_i et avec un seul 1 par période).
Mais alors $|E| \leq |\prod_i E_i| \leq |\prod_i P_i|$, et les éléments de $\prod_i P_i$ peuvent se compter ainsi : on commence par prendre tous les éléments de période p_i, il y en a 2^{n_i}. Parmi eux, certains ont une période divisant n_i et n_j, et qui ont donc été comptés deux fois. Il y en a $2^{\gcd(n_i,n_j)}$, que l'on retire donc du décompte. De même les éléments dont la période divise à la fois n_i, n_j et n_ℓ ont été comptés trois fois puis retirés trois fois, il convient donc de les rajouter. Par ce principe d'inclusion-exclusion, on arrive à $u = \sum_{j=1}^{m} (-1)^{j-1} \sum_{i_1 < i_2 < \dots < i_j} \gcd(n_{i_1}, \dots, n_{i_j})$. □

Exemple 1.6

Si l'on considère l'union de trois automates de taille 2, alors l'équation (IV.1) nous donne

$$u = \underbrace{6-}_{\text{taille 1}} \underbrace{(2+2+2)}_{\text{taille 2}} \underbrace{+2}_{\text{taille 3}} = 2\,.$$

Si on prends trois automates ayant pour tailles respectives $2, 3$ et 5, on obtient pour leur union

$$u = 10 - (1+1+1) + 1 = 8\,.$$

On engendrera donc un groupe de taille au plus $|A_k|^{30} \times 2^8 = \frac{k!^{30}}{2^{22}}$.

Cette construction nous fournit un contre-exemple la conjecture émise dans [65] : "Si $\mathcal{A}$ est un automate bireversible à n états et k lettres qui engendre un groupe fini, alors $|\langle\mathcal{A}\rangle| \leq k!^n$". En effet considérons l'automate $\mathcal{A}$ issu de l'union disjointe des deux automates des figures IV.3 et IV.4. Cet automate est biréversible à 5 états et 6 lettres. Cependant on a $|\langle\mathcal{A}\rangle| = 34828517376000000 = 6!^6/4 > 6!^5$, ce qui infirme la conjecture.
On a aussi été en mesure de montrer que cette conjecture reste fausse dans le cas connexe, en utilisant une construction semblable à celle du Bread-and-Butterfly pour les automates biréversibles.

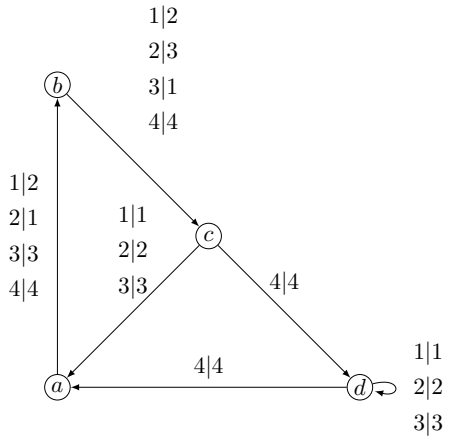


FIGURE IV.5 – Un contre-exemple connexe à la conjecture de [65], construit en prenant deux automates cycliques sur des alphabets disjoint puis en identifiant certains états. Le groupe engendré est d'ordre $8503056 = 2^4 3^{12} > 25 \times 4!^4$.

2 Cas des automates cycliques à deux états

On s'intéresse maintenant au cas des automates cycliques connexes et on prouve un analogue au théorème de Dixon dans cette classe. Pour essayer de mieux comprendre les points clefs de la preuve, on se penche tout d'abord sur le cas des automates cycliques connexes à deux états. En effet, une grande partie de la difficulté du problème s'y trouve déjà présente, tandis que le nombre réduit d'états permet de se concentrer dans un premier temps sur certains aspects qui se généralisent directement dans le cas d'un automate ayant un nombre quelconque d'états tout en simplifiant considérablement les notations.
Dans cette section $\mathcal{A}$ désigne un automate cyclique à 2 états et k lettres, donc les fonctions de production sont notées σ et τ.
Le but de cette section est de montrer :

Théorème 2.1

Soit $\mathcal{A}$ une variable aléatoire suivant la loi uniforme sur la classe des automates de Mealy cycliques à 2 états et k lettres. On a

$$\begin{cases} \lim_{k\to\infty} \mathbb{P}\left(\langle\mathcal{A}\rangle \simeq S_k \times S_k\right) & = 1/2\,, \\ \lim_{k\to\infty} \mathbb{P}\left(\langle\mathcal{A}\rangle \simeq (A_k \times A_k) \rtimes \langle(\pi,\pi)\rangle\right) & = 1/4\,, \\ \lim_{k\to\infty} \mathbb{P}\left(\langle\mathcal{A}\rangle \simeq A_k \times A_k\right) & = 1/4\,. \end{cases}$$

avec π une transposition quelconque de S_k.

Remarque 2.2

Ce théorème n'est pas une conséquence directe du théorème de Dixon appliqué composante par composante. En effet, si on applique Dixon à la paire de vecteurs $(\sigma,\tau),(\rho,\pi)$, on obtient [3] que $\langle(\sigma,\tau),(\rho,\pi)\rangle$ est asymptotiquement S_k^2 avec probabilité 3/8, isomorphe à $S_k \times A_k$ avec probabilité 3/8, $(A_k \times A_k) \rtimes \langle(\pi,\pi)\rangle$ avec probabilité 3/16 ou A_k^2 avec probabilité 1/16. En particulier, on voit qu'il est impossible de générer $S_k \times A_k$ avec une présentation circulaire, puisque que les coordonnées y jouent un rôle symétrique.

3. En fait, pour obtenir ce résultat, il est nécessaire d'effectuer un travail similaire à ce qu'on va faire pour les automates cycliques, en trouvant une manière de rendre une coordonnée triviale mais pas l'autre. Cela suggère, ainsi que le notait un rapporteur anonyme de l'article [44], un mécanisme commun et l'existence d'un méta-théorème de Dixon, je n'ai malheureusement pas réussi à caractériser ce mécanisme.

Pour arriver à ce théorème, on cherche tout d'abord à décrire le sous-groupe maximal de $\langle \mathcal{A} \rangle \leq S_k \times S_k$ dont la première coordonnée est $\mathbb{1}$.

Le lemme ci-dessous est intéressant, en cela qu'il permet de conclure dans un nombre restreint de cas, mais surtout car il donne l'idée naïve de la stratégie à appliquer pour obtenir le théorème 2.1.

Lemme 2.3

Si $\text{pgcd}(|\sigma|, |\tau|) = 1$, alors $\langle \mathcal{A} \rangle = \langle \sigma, \tau \rangle \times \langle \sigma, \tau \rangle$.

Démonstration. Comme les ordres sont premiers entre eux, on applique le lemme de Bezout : il existe des entiers u et v satisfaisant $u|\sigma| + v|\tau| = 1$.
Mais alors $(\sigma, \tau)^{u|\sigma|} = (\sigma^{u|\sigma|}, \tau^{u|\sigma|}) = (\mathbb{1}, \tau^{1-v|\tau|}) = (\mathbb{1}, \tau) \in \langle \mathcal{A} \rangle$. On obtient de façon similaire les éléments $(\mathbb{1}, \sigma), (\sigma, \mathbb{1})$ et $(\tau, \mathbb{1})$, et on en déduit $\langle \sigma, \tau \rangle \times \langle \sigma, \tau \rangle \leq \langle \mathcal{A} \rangle$, et comme il s'agit aussi d'une borne supérieure, on a le résultat. □

Cependant, il est très peu probable que des permutations aient des ordres premiers entre eux. Au contraire, Erdős et Turan ont démontré dans [35] que l'ordre de presque toutes les permutations de S_k est divisible par toutes les (puissances de) nombres premiers n'excédant pas

$$\frac{\log k}{\log\log k}\left(1 + 3\frac{\log\log\log k}{\log\log k} - \frac{\omega(k)}{\log\log k}\right),$$

avec ω une fonction tendant arbitrairement lentement vers l'infini.

Il nous faut donc affaiblir les hypothèses requises et utiliser un raisonnement plus fin.

Comme dans l'article de 1969 de Dixon, on utilise un théorème de Jordan pour montrer qu'on engendre soit A_k soit S_k.

Théorème 2.4 (Jordan)

Soit G un sous groupe primitif de S_k. Si l'un des éléments de G est un cycle de taille $p \leq k-3$, avec p premier, alors G est soit le groupe alterné A_k, soit le groupe symétrique S_k.

On rappelle qu'un sous-groupe $G \leq S_k$ est *primitif* si, pour toute partition $P = (P_1, \ldots, P_\ell)$ de $\{1, \ldots, k\}$ non triviale (différente des singletons ou de l'ensemble entier), la partition n'est pas fixée par G ($\exists i, \exists P_j,\ \exists g \in G, g.i \notin P_j$). En particulier un tel groupe est toujours transitif.

On montre que, dans le cas présent, trouver un p-cycle en deuxième coordonnée, tandis que la première vaut $\mathbb{1}$, permet de montrer que le groupe est primitif, et donc qu'on peut directement appliquer le théorème de Jordan.

On utilise la décomposition en cycles d'une permutation et les classes de conjugaison de S_k et A_k. Soit σ une permutation : il existe une unique (à l'ordre près) décomposition de σ en cycles disjoints. De plus la classe de conjugaison de σ dans S_k (*i.e.* l'ensemble $\{\sigma^\pi = \pi^{-1}\sigma\pi \mid \pi \in S_k\}$) correspond exactement à l'ensemble des permutations ayant une décomposition en cycles de même structure (*i.e.* le même nombre de cycles de mêmes tailles). Dans le groupe alterné c'est aussi vrai, sauf si la décomposition en cycles ne comporte que des tailles impaires toutes différentes [91], auquel cas il y a deux classes de conjugaison par profil de la décomposition en cycles et l'on dit alors que la classe de conjugaison se divise.

Proposition 2.5

Soit π un p-cycle de S_k avec p premier et $k \geq 5$, alors les groupes $G_\pi(S_k) = \langle \pi^\rho \mid \rho \in S_k \rangle$ et $G_\pi(A_k) = \langle \pi^\rho \mid \rho \in A_k \rangle$ sont primitifs.

Démonstration. On démontre que le résultat est vérifié pour $G_\pi(A_k)$, ce qui implique le résultat pour $G_\pi(S_k)$.
On commence par montrer que $G_\pi(A_k)$ est primitif : soient $i, j \in \{, \ldots, k\}$. Si la classe de conjugaison ne se divise pas alors $(i, j, x_3, \ldots, x_p) = \pi^\rho$ pour un $\rho \in A_k$ convenablement choisi et des x_ℓ arbitraires, et on a $\pi^\rho(i) = j$. Si la classe se divise, prenons $p \geq 5$ et $(i, j, x_3, \ldots, x_p) = \pi^\rho$, avec $\rho \in S_k \setminus A_k$ dans une classe différente de π, alors $(i, j, x_3, \ldots, x_p, x_{p-1}) = (\pi^\rho)^{(p-1,p)} = \pi^{\rho(p-1,p)}$ est dans la classe de conjugaison de π, car $\rho(p-1, p) \in A_k$. Donc $G_\pi(A_k)$ est transitif.
Montrons qu'aucune partition non triviale n'est préservée par $G_\pi(A_k)$. Soit $\Sigma_1, \ldots, \Sigma_a$ une partition de $1, \{, \ldots, k\}$ avec (quitte à renommer) $i, j \in \Sigma_1$ et $\ell \in \Sigma_2$. Considérons $\pi^\rho = (i, j, x_3, \ldots, x_{p-1}, \ell)$: comme $\pi^\rho(i) = j \in \Sigma_1$ et $\pi^\rho(\ell) = i \in \Sigma_1$, la partition n'est pas préservée. Si $\rho \in A_k$, on a le résultat attendu ; sinon $\rho(1, 2) \in A_k$, et $(j, i, x_3, \ldots, x_{p-1}, \ell) \in G_\pi(A_k)$ et on peut conclure de même.

□

Le lemme suivant est simple mais essentiel dans la suite de notre raisonnement.

Lemme 2.6

Soit $(\mathbb{1}, \pi) \in \langle \mathcal{A} \rangle$. Alors pour tout $\rho \in \langle \sigma, \tau \rangle$, on a $(\mathbb{1}, \pi^\rho) \in \langle \mathcal{A} \rangle$.

Démonstration. Comme $\rho \in \langle \sigma, \tau \rangle$, on a $\rho = \prod_i \epsilon_i$ avec $\epsilon_i \in \{\sigma, \tau\}$. Alors $(\overline{\rho}, \rho) \in \langle \mathcal{A} \rangle$, avec $\overline{\rho} = \prod_i \epsilon'_i$ et $\epsilon'_i = \sigma$ si $\epsilon_i = \tau$ et vice-et-versa. Ainsi on a $\overline{\rho}^{-1} = \overline{\rho^{-1}}$ et donc $(\mathbb{1}, \pi)^{(\overline{\rho}, \rho)} = (\mathbb{1}^{\overline{\rho}}, \pi^\rho) = (\mathbb{1}, \pi^\rho)$. □

Ainsi, si l'on trouve un p-cycle, avec p premier et de taille inférieure à $k-3$, et que $\langle \sigma, \tau \rangle = A_k$ ou S_k (ce qui est génériquement le cas), alors on pourra appliquer la suite de propositions et lemmes ci-dessus pour obtenir le groupe $\{\mathbb{1}\} \times A_k$ ou $\{\mathbb{1}\} \times S_k$, et donc le théorème 2.1. La prochaine proposition est cruciale, car elle décrit comment obtenir un tel p-cycle.

Proposition 2.7

Soient σ et τ deux permutations d'ordres différents, et telles que $\langle \sigma, \tau \rangle = A_k$ ou S_k. Alors il existe un entier premier p et un p-cycle π satisfaisant $(\mathbb{1}, \pi) \in \langle \sigma, \tau \rangle_c$.

Démonstration. Soit d le pgcd de $|\sigma|$ et $|\tau|$. Par construction $\left|\sigma^d\right|$ et $\left|\tau^d\right|$ sont premiers entre eux et au moins l'une des permutations σ^d et τ^d est différente de l'identité. Supposons $\tau^d \neq \mathbb{1}$ et choisissons p un nombre premier qui divise l'ordre de τ^d (et donc qui ne divise pas l'ordre de σ^d. Posons a le plus grand entier tel que $p^a \mid \left|\tau^d\right|$. Ainsi $\tau^{dp^{a-1}}$ est d'ordre pr avec $\operatorname{pgcd}(p, r) = 1$, et $\sigma^{dp^{a-1}}$ est d'ordre premier avec p, puisque que de même ordre que σ^d. Posons alors, pour la lisibilité, $\hat{\tau} = \tau^{dp^{a-1}}$ et $\hat{\sigma} = \sigma^{dp^{a-1}}$.
On a donc $\langle \sigma, \tau \rangle_c \ni (\hat{\sigma}, \hat{\tau})^{\frac{|\hat{\sigma}||\hat{\tau}|}{p}} = ((\hat{\sigma}^{|\hat{\sigma}|})^{\frac{|\hat{\tau}|}{p}}, (\hat{\tau}^{\frac{|\hat{\tau}|}{p}})^{|\hat{\sigma}|}) = (\mathbb{1}, (\hat{\tau}^{\frac{|\hat{\tau}|}{p}})^{|\hat{\sigma}|})$. Comme $\hat{\tau}^{\frac{|\hat{\tau}|}{p}}$ est d'ordre p et que $\operatorname{pgcd}(|\hat{\sigma}|, p) = 1$, $\check{\tau} = (\hat{\tau}^{\frac{|\hat{\tau}|}{p}})^{|\hat{\sigma}|}$ est elle aussi d'ordre p.
Ainsi, $\check{\tau}$ est un produit $\prod_i \pi_i$ de ℓ p-cycles disjoints. Pour $\ell > 1$, on va construire un p-cycle π tel que $(\mathbb{1}, \pi) \in \langle \sigma, \tau \rangle_c$. On procède par disjonction de cas :

1. Cas $p \neq 2$. Posons $\tilde{\tau}$ le conjugué $\pi_1 \prod_{i \geq 2} \pi_i^{-1}$ de $\check{\tau}$. Donc $\langle \sigma, \tau \rangle_c \ni (\mathbb{1}, \check{\tau})(\mathbb{1}, \tilde{\tau}) = (\mathbb{1}, \pi_1^2)$, et, comme $\gcd(2, p) = 1$, π_1^2 est un p-cycle.
2. Cas $p = 2$.
   (a) Pour $2\ell < k$. Alors $\tilde{\tau} = \prod_{i \geq 0}(2i+1, 2i+2)$ et $\dot{\tau} = (1, k) \prod_{i \geq 0}(2i+1, 2i+2)$ sont dans la même classe de conjugaison que $\check{\tau}$, donc $\langle \sigma, \tau \rangle_c \ni (\mathbb{1}, \tilde{\tau})(\mathbb{1}, \dot{\tau}) = (\mathbb{1}, (1, 2, k))$, on obtient donc un 3-cycle.
   (b) Sinon $\tilde{\tau} = \prod_{i \geq 0}(2i+1, 2i+2)$ et $\dot{\tau} = (1, 4)(2, 3) \prod_{i \geq 2}(2i+1, 2i+2)$ satisfont $\tilde{\tau}\dot{\tau} = (1, 3)(2, 4)$, ce qui nous ramène au cas précédent (dès lors que $k > 4$).

□

On peut maintenant démontrer le théorème :

Théorème 2.8

Soient σ and τ deux permutations de S_k, $k > 5$, d'ordres différents avec $\langle \sigma, \tau \rangle = S_k$ ou A_k. Alors

$$\left\langle \; \overset{\sigma}{\underset{\tau}{\textcircled{1} \rightleftarrows \textcircled{2}}} \; \right\rangle = \begin{cases} S_k \times S_k & \text{pour } \operatorname{sgn}(\sigma) \neq \operatorname{sgn}(\tau), \\ (A_k \times A_k) \rtimes \langle (\pi, \pi) \rangle & \text{pour } \operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau) = -1, \\ A_k \times A_k & \text{pour } \operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau) = 1, \end{cases}$$

où π est une transposition arbitraire de S_k.

Démonstration. On applique la proposition 2.7 (en gardant les même notations, donc $d = \operatorname{pgcd}(|\sigma|, |\tau|)$). Si le p-cycle ainsi construit satisfait $p \leq k-3$, on peut alors appliquer le théorème 2.4 et conclure.
Sinon, on est dans un des six cas suivants : $(|\sigma|^d, |\tau|^d)$ est $((k-2),(k-1))$, $((k-1),k)$, $((k-2),k)$, $(1,(k-2))$, $(1,(k-1))$, ou $(1,k)$, avec $d = \operatorname{pgcd}(|\sigma|, |\tau|)$ et k est premier et plus grand que 5. Dans les trois premiers cas, les ordres sont premiers entre eux et $d = 1$ au vu de la taille des cycles, et l'on peut donc conclure avec le lemme 2.3. Dans les trois derniers cas, on a que $\sigma = \mathbb{1}$, et l'on ne peut avoir $\langle \sigma, \tau \rangle = S_k$ ou A_k, ce qui contredit l'hypothèse. Pour conclure que les groupes sont bien ceux attendus, on utilise la proposition 1.4 pour la borne inférieure et $(\sigma, \tau) \in \langle \mathcal{A} \rangle$ pour prouver la borne supérieure. □

Démonstration du théorème 2.1. Pour terminer la preuve, on remarque que, d'après le théorème de Dixon, la probabilité que $\langle \sigma, \tau \rangle = S_k$ ou A_k était égale à $1 - 1/k - O(1/k^2)$ et que, comme le logarithme de l'ordre d'une permutation converge vers une loi gaussienne (continue), la probabilité que deux permutations aient le même ordre tend vers 0. Les proportions proviennent de $\mathbb{P}(\operatorname{sgn}(\sigma) = 1) = \mathbb{P}(\operatorname{sgn}(\sigma) = -1) = \frac{1}{2}$. □

2.1 Aparté : sur la probabilité que deux permutations aient le même ordre

On remarque que dans le théorème 2.1, contrairement au théorème de Dixon, on n'a pas d'estimation de la vitesse de convergence. Cela vient de l'absence d'analyse asymptotique de la

probabilité que deux permutations aient le même ordre.
En effet, si l'on peut facilement montrer que, pour $\sigma, \tau \in S_k$ deux permutations aléatoires, $\varpi(k) = \mathbb{P}(|\sigma| = |\tau|)$ est minoré par $1/k^2$, c'est-à-dire la probabilité de tirer deux k-cycles (qui sont évidemment de même ordre), il semble bien plus difficile de trouver une borne supérieure non triviale, malgré la convergence de la probabilité vers 0, assurée par le théorème de Erdős-Turan démontrant la convergence du logarithme de l'ordre vers une loi continue.
Il est possible de trouver une meilleure borne inférieure : si deux permutations sont conjuguées, alors elles ont le même ordre. Ce problème a été étudié par Flajolet *et al.* en utilisant des méthodes d'analyse complexe dans [37], puis par Blackburn *et al.* avec des méthodes plus élémentaires dans [17]. Ces auteurs obtiennent que la probabilité d'être conjugué dans S_k vaut asymptotiquement

$$W(1)/k^2\,,$$

avec $W(z) = 1 + z + 2\frac{z}{2!^2} + 14\frac{z}{3!^2} + 146\frac{z}{4!^2} + 2602\frac{z}{4!^2} + \cdots$, où les coefficients sont donnés par la somme des carrés des tailles des classes d'équivalence de S_k (suite A087132 de l'OEIS [94]), et $W(1) \approx 4,26340$. Malheureusement, aucune de ces méthodes ne semble s'étendre à l'ordre, entre autre car le ppcm complique l'expression d'une formule de récurrence.
Les expérimentations numériques menées suggèrent que cette probabilité est bien de magnitude $1/k^2$; ce qui nous amène à formuler la conjecture :

Conjecture 2.9

Soient σ, τ deux variables aléatoires suivant une loi uniforme sur S_k. Alors on a

$$\lim_{k\to\infty} \mathbb{P}\left(|\sigma| = |\tau|\right) = \frac{K}{k^2}$$

avec $W(1) \leq K \leq 12$.

Notons aussi qu'un problème proche, la probabilité que deux permutations aient le même nombre de cycles, a été étudié par Wilf [104].

Dans [17], il est également démontré que la probabilité d'être conjugué dans un groupe est un invariant pour la classe d'isoclinie d'un groupe. Plus précisément : on dit que deux groupes G et H sont *isoclins* s'il existe deux isomorphismes de groupes $\alpha : G/Z(G) \to H/Z(H)$ et $\beta : G' \to H'$ vérifiant $\beta\left([g_1, g_2]_G\right) = [\alpha(g_1), \alpha(g_2)]_H$ (où $Z(G)$ désigne le centre $\{g \in G | \forall g' \in G, gg' = g'g \in G\}$ de G, $[g_1, g_2]_G = g_1^{-1}g_2^{-1}g_1g_2$ le commutateur de g_1 et g_2 dans G et $G' = \{[g_1, g_2]_G, g_1, g_2 \in G)$. Si deux groupes G et H sont isoclins, et si on définit $\kappa(G)$ la probabilité

que deux éléments de G soient conjugués, alors on

$$\kappa(G)\,|G| = \kappa(H)\,|H| \ .$$

Cela n'est plus vrai pour la probabilité d'être de même ordre : si l'on note $\varpi(G)$ la probabilité que deux éléments de G soient de même ordre, on peut calculer $\varpi(G)\,|G|$ pour des exemples de petits groupes isoclins. En particulier, le groupe des quaternions Q_4 a huit éléments, un d'ordre 1, un d'ordre 2 et six d'ordre 4, donc $\varpi(Q_4)\,|Q_4| = (1/64 + 1/64 + 36/64) \times 8 = 38/8$; tandis que le groupe dihédral D_4 a lui aussi huit éléments, un d'ordre 1, cinq d'ordre 2 et deux d'ordre 4, donc $\varpi(D_4)\,|D_4| = (1/64 + 4/64 + 25/64) \times 8 = 30/8$. De plus ces groupes sont isoclins. On a donc

$$Q_4 \text{ et } D_4 \text{ sont isoclins et } \varpi(Q_4)\,|Q_4| \neq \varpi(D_4)\,|D_4| \ .$$

Ce résultat n'est guère surprenant car la démonstration de [17] s'appuie sur la formule des classes qui n'a pas d'équivalent connu pour les ordres.

3 Cas général

On montre maintenant que tout tirage d'automates cycliques produit une distribution de type Dixon, avec une distribution concentrée sur un petit nombre de groupes qui sont les groupes maximaux atteignables selon les signatures possible.

Comme pour le cas à deux états, on cherche à exhiber une permutation $(\mathbb{1}, \ldots, \mathbb{1}, \rho)$, avec ρ un cycle de longueur un nombre premier. On commence par considérer séparément le cas à trois états, là encore pour simplifier la lecture :

Proposition 3.1

Soient σ_0, σ_1 et σ_2 trois permutations de S_k, $k \geq 7$, n'ayant pas toutes le même ordre et telles que $\langle \sigma_0, \sigma_1, \sigma_2 \rangle$ est soit S_k soit A_k. Alors il existe un cycle π de longueur première satisfaisant $(\mathbb{1}, \mathbb{1}, \pi) \in \langle (\sigma_0, \sigma_1, \sigma_2) \rangle_c$.

Démonstration. Comme les ordres sont différents, il existe un nombre premier p, un entier c et un sous-ensemble non trivial de $\{\sigma_i\}_{i\in\{0,1,2\}}$ tel que p^c (et pas p^{c+1}) divise tous les ordres de ce sous-ensemble (et pas les ordres des autres permutations). Si ce sous-ensemble est réduit à une unique permutation, alors on peut appliquer les méthodes de la proposition 2.7 et conclure. Sinon, par des techniques semblables, on peut prendre la puissance adaptée et obtenir le vecteur $(\mathbb{1}, \tau_1, \tau_2)$ (et, par circularité, $(\tau_1, \tau_2, \mathbb{1})$ également). Comme dans la proposition 2.7, on

peut créer, par conjugaisons et multiplications, les vecteurs $(\mathbb{1}, \rho_1, \alpha)$ (*resp.* $(\beta, \rho_2, \mathbb{1})$), pour un certain p-cycles ρ_1 (*resp.* ρ_2). De plus, on peut exiger $|\alpha| = p^a$ pour un certain entier a (*resp.* $|\beta| = p^b$ pour un certain entier b), et on a donc, pour tous les ρ_1 dans une certaine classe de conjugaison sous $\langle \sigma_0, \sigma_1, \sigma_2 \rangle$, un vecteur $(\mathbb{1}, \rho_1, \alpha_{\rho_1})$ (*resp.* $(\mathbb{1}, \rho_2, \beta_{\rho_2})$). On peut alors, en choisissant correctement ρ_1 et ρ_2, multiplier ces vecteurs et obtenir $(\beta_\pi, \pi, \alpha_\pi)$, où π est un cycle de taille 3 (ou 5 pour $p = 3$), et où les ordres de α_π et β_π sont des puissances de p. On obtient alors $(\beta_\pi, \pi, \alpha_\pi)^{|\alpha_\pi||\beta_\pi|} = (\mathbb{1}, \hat{\pi}, \mathbb{1})$, où $\hat{\pi}$ est 3-cycle (*resp.* 5-cycle), et donc par conjugaison (*resp.* multiplication et conjugaison) on peut obtenir tous les 3-cycles. On peut donc engendrer A_k sur une coordonnée. Le résultat suit. □

On remarque que, comme pour la proposition 2.7, on fait l'hypothèse que les ordres ne sont pas identiques. La généralisation à un plus grand nombre d'états passe par une hypothèse plus forte en générale : on demande que le vecteur des ordres (vu comme un mot circulaire) soit primitif, c'est-à-dire qu'il ne peut pas être exprimé comme la puissance d'un mot autre que lui-même, ou bien encore qu'il n'est pas périodique.

Proposition 3.2

Soient $\sigma_0, \sigma_1, \cdots, \sigma_n$ des permutations de S_k, $k \geq 7$, telles que le vecteur $(|\sigma_0|, \ldots, |\sigma_{n-1}|)$ est primitif et $\langle (\sigma_i)_i \rangle = S_k$ ou A_k. Alors il existe un cycle π de longueur première satisfaisant $(\mathbb{1}, \mathbb{1}, \ldots, \mathbb{1}, \pi) \in \langle (\sigma_i)_i \rangle_c$.

Démonstration. Comme les ordres ne sont pas identiques, il existe un nombre premier p, un entier c et un sous-ensemble non trivial de $\{\sigma_i\}_{i \in \{0,1,\ldots,n-1\}}$ tel que p^c divise tous les ordres de ce sous-ensemble (et p^{c+1} non, et pas les ordres des permutations restantes). En prenant la puissance adaptée, on peut donc obtenir un vecteur de permutations d'ordres p ou 1.
On peut supposer que toutes les permutations non-triviales de ce vecteus sont entourées d'identités : considérons $(\alpha_0, \ldots, \alpha_a, \mathbb{1}, \pi_0, \ldots, \pi_s, \mathbb{1}, \beta_0, \ldots, \beta_b)$, où les π_i sont d'ordre p et π_1 est un p-cycle, ainsi que son permuté-conjugué $(\beta'_b, \alpha'_0, \ldots, \alpha'_a, \mathbb{1}, \pi'_0, \ldots, \pi'_s, \mathbb{1}, \beta'_0, \ldots, \beta'_{b-1})$ où les π'_i sont d'ordre p et π'_0 est un p-cycle tel que $\pi_1\pi'_0$ est d'ordre r, avec r un nombre premier diffèrent de p, et avec $|\alpha_i| = |\alpha'_i|$ et $|\beta_i| = |\beta'_i|$. En multipliant ces deux vecteurs, on obtient

$$\Delta = (\alpha_0\beta'_b, \alpha_1\alpha'_0, \ldots, \alpha_a\alpha'_{a-1}, \alpha'_a, \pi_0, \pi_1\pi'_0, \ldots, \pi_s\pi'_{s-1}, \pi'_s, \beta_0, \beta_1\beta'_0, \ldots, \beta_{b-1}\beta'_b) .$$

On remarque que, si la permutation α_i est triviale, alors la coordonnée correspondante dans Δ est d'ordre p. En prenant la bonne puissance, on obtient $(\gamma_0, \ldots, \gamma_{a-1}, \mathbb{1}, \mathbb{1}, \rho_0, \ldots, \rho_{s-1}, \mathbb{1}, \mathbb{1}, \delta_0, \ldots, \delta_{b-1})$, où les coordonnées triviales restent triviales et où les permutations non triviales sont d'ordre r,

donc, par récurrence, on construit un vecteur de permutations d'ordre premier r, où les permutations non-triviales sont encadrées de permutations triviales. Ce vecteur peut ne pas être primitif, mais on peut en construire un pour tout nombre premier plus grand que 2.
Distinguons maintenant deux cas : s'il existe un vecteur $\Pi = (\sigma_0, \dots, \sigma_{n-1})^d = (\pi_0, \dots, \pi_{n-1})$, avec $|\pi_i| \in \{1, p\}$, p premier tel le vecteur des ordres est primitif (vu circulairement), prenons alors Γ un vecteur non trivial avec les ordres des coordonnées sont soit 1 soit p et tel que les permutations non triviales soient encadrées par des permutations identités (comme construit plus haut). Comme Π est apériodique, on peut trouver une configuration où deux permutations non triviales de Γ (sous réserve que Γ contienne plus qu'une permutation non triviale) font face à, respectivement, une permutation triviale et une non triviale. En multipliant Π et Γ dans cette configuration et en prenant la puissance adaptée, on obtient un vecteur Γ_1 qui a les mêmes propriétés que Γ mais qui contient strictement moins de permutations non triviales, tout en conservant une coordonnée non triviale. On itère ce procédé jusqu'à stabilisation à $\Gamma_\infty \in \langle \mathcal{A} \rangle$ qui contient une seule permutation non triviale, d'ordre p. On peut alors, comme dans la proposition 2.7, transformer cette permutation en un p-cycle, et on conclut. S'il n'existe pas un tel vecteur Π, alors il existe deux vecteurs Π_1 et Π_2, qui ont leurs vecteurs des ordres (valant respectivement soit 1 et p_1, soit 1 et p_2) ayant des périodes t_1, t_2, non-multiples, et dont le plus petit multiple commun ne divise pas n. On peut alors construire Γ comme auparavant pour p_1. Alors, soit Γ est apériodique ou t_1 ne divise pas sa période, ou bien t_1 divise la période des ordres de Γ. Dans les premiers cas, on peut obtenir un vecteur Γ_1 ayant strictement moins de permutations non triviales que Γ, tout en ayant les même propriétés en multipliant Γ et Π_1 dans la configuration idoine. Dans le dernier cas, t_2 ne divise pas la période de Γ et on peut appliquer le même argument en considérant cette fois Π_2 au lieu de Π_1. Par induction, on arrive au résultat attendu. □

On a maintenant tous les ingrédients nécessaires pour démontrer un théorème à la Dixon pour les automates cycliques :

Théorème 3.3

Soit $\mathcal{A}_k$ une variable aléatoire suivant la loi uniforme sur la classe des automates de Mealy cycliques à n états et k lettres, dont les fonctions de sortie sont $\sigma_0, \dots, \sigma_{n-1}$. alors

$$\lim_{k\to\infty} \mathbb{P}\Big(\langle \mathcal{A}_k \rangle = A_k^n \rtimes \langle \mathrm{sgn}_\pi (\sigma_0, \dots, \sigma_{n-1}) \rangle_c \Big) = 1 \,,$$

avec π une transposition arbitraire de S_k.

Démonstration. Par le théorème de Dixon, on a génériquement $\langle (\sigma_i)_i \rangle = S_k$ ou A_k. D'après la proposition 3.2, si le vecteur des ordres est primitif, on peut trouver un élément de la forme $(\mathbb{1}, \mathbb{1}, \ldots, \mathbb{1}, \pi) \in \langle (\sigma_i)_i \rangle_c$. On peut alors appliquer le lemme 2.6, la proposition 2.5 et le théorème de Jordan comme dans le théorème 2.8 et conclure. On montre donc que le vecteur des ordres est primitif avec probabilité tendant vers 1 avec k. Pour cela, remarquons que la probabilité que le vecteur soit non primitif est inférieure à la probabilité que $|\sigma_0| = |\sigma_i|$ pour un certain i. Cette probabilité tend vers 0 quand k tend vers l'infini puisque le logarithme de l'ordre converge vers un loi continue (théorème d'Erdős-Turan) et que n est fixé. □

Là encore on utilise dans le théorème une condition suffisante sur les ordres des permutations. Cependant, si l'on force les permutations de l'automate cyclique à avoir le même ordre (ou même, plus restrictif encore, à être conjuguées), on obtient toujours empiriquement une convergence vers ces groupes (dans le cas de permutations conjuguées, on a moins de variété car toutes les permutations ont la même signature). Il est déjà connu qu'on obtient un théorème homologue à celui de Dixon pour des permutations aléatoires conjuguées [92], et il semble naturel d'essayer dans l'avenir d'étendre nos techniques à ce cas.

4 Remarques et conclusions

Ce travail sur les automates cycliques est important dans l'optique de la génération aléatoire des groupes finis par des automates de Mealy car, s'il suggère tout d'abord qu'il est nécessaire d'enrichir la structure de l'automate pour obtenir une certaine diversité pour les groupes engendrés, il montre surtout qu'on ne peut pas espérer travailler dans la classe des automates avec cycles sans échappatoire.
En effet, ces automates cycliques apparaissent inévitablement à la fin des automates avec cycles sans échappatoire, et nos résultats de convergence impliquent donc que le groupe engendré par un automate avec cycles sans échappatoire aléatoire contiendra un produit direct de groupes alternés, ce qui nous empêche donc d'obtenir de petits groupes.

De plus il semble empiriquement que si l'on fixe la structure de l'automate (choisi dans la classe des automates avec cycles sans échappatoire), et que l'on regarde le groupe engendré par cet automate où l'on a tiré les étiquettes aléatoirement, on obtient encore une convergence qui ne dépend que de cette structure et des signatures des permutations choisies. On n'a pas de résultat complet à ce propos mais les résultats préliminaires vont dans ce sens :

Dans le cas d'un automate qui se réduit à un chemin simple terminé par une boucle, on a :

Proposition 4.1

Soit $\mathcal{A}$ une variable aléatoire suivant la loi uniforme sur la classe des automates de Mealy $(Q, \Sigma, \delta, \rho)$ inversibles à k lettres et n états, et tel que $\delta_s(q) = \min(q+1, n-1)$ pour $q \in Q$ et $s \in \Sigma$. Alors

$$\lim_{k\to\infty} \mathbb{P}\big(\langle\mathcal{A}\rangle = (A_k^{n-1} \times \langle\rho_{n-1}\rangle) \rtimes P\big) = 1\,,$$

avec

$$P = \langle\{(\mathrm{sgn}_\pi(\rho_i), \ldots, \mathrm{sgn}_\pi(\rho_{n-1}), \ldots, \mathrm{sgn}_\pi(\rho_{n-1}))\}_i\rangle\,.$$

Démonstration. Par définition du groupe d'automate, l'état q induit la transformation $(\rho_q, \rho_{q+1}, \ldots, \rho_{n-1}, \ldots, \rho_{n-1}, \ldots)$ sur les mots de l'alphabet, d'où

$$\mathcal{A} \simeq \langle(\rho_0, \ldots, \rho_{n-1}), (\rho_1, \ldots, \rho_{n-1}, \rho_{n-1}), \ldots, (\rho_{n-1}, \ldots, \rho_{n-1})\rangle\,,$$

On obtient alors le résultat par le théorème de Dixon et par conjugaison. □

Ainsi le groupe $\langle\mathcal{A}\rangle$ de la proposition 4.1 est génériquement d'ordre $k!^{n-1} \times |\rho_{n-1}| / 2^{(\min_i (i|\{\mathrm{sgn}(\rho_{n-1-i})\}_i = \{-1,1\}) - 1)}$. Dans le même esprit, si l'automate est une union disjointe de tels automates-chemins, alors c'est de manière générique le produit direct de groupes alternés ou symétriques.

Si maintenant l'automate est formé d'un arbre enraciné en une boucle et dont toutes les arêtes vont des feuilles vers la racine, alors on a :

Proposition 4.2

Soit $\mathcal{A}$ une variable aléatoire suivant la loi uniforme sur la classe des automates de Mealy $(Q, \Sigma, \delta, \rho)$ inversible à k lettres est dont l'ensemble des états Q est un sous ensemble des mots de $\{0, \ldots, a-1\}^d$ (on appellera a l'arité de l'automate et d sa profondeur), et tel que $\delta_s(x_0, \ldots, x_i, x_{i+1}) = x_0, \ldots, x_i, \forall x_0, \ldots x_{i+1} \in \{0, \ldots, a-1\}^d, s \in \Sigma$. Alors on a

$$\lim_{k\to\infty} \mathbb{P}\big(\langle\mathcal{A}\rangle = (A_k^{n-1} \times \langle\rho_\epsilon\rangle) \rtimes P\big) = 1$$

avec

$$P = \langle\{(\mathrm{sgn}_\pi(\rho_{u_i u_{i-1} \ldots}), \ldots, \mathrm{sgn}_\pi(\rho_\epsilon), \ldots, \mathrm{sgn}_\pi(\rho_\epsilon))\}_i\rangle\,.$$

Démonstration. L'état $u_0 \cdots u_i$ induit la transformation $(\rho_{u_0u_1\ldots u_i}, \rho_{u_0u_1\ldots u_{i-1}}, \ldots, \rho_\epsilon, \ldots, \rho_\epsilon, \ldots)$ sur Σ^*. On aboutit donc au résultat en appliquant encore le théorème de Dixon et par conjugaison. □

D'autre part, les expérimentations effectuées en **GAP** suggèrent qu'on peut aboutir à des théorèmes semblables pour les autres structures rencontrées dans les automates à cycles sans échappatoire. Il nous faut donc, dans l'optique d'une génération efficace, trouver une autre classe dans laquelle tirer nos automates.
Klimann a montré dans [63] que les automates biréversibles à deux états avaient un problème de finitude décidable. On peut alors essayer de tirer uniformément, par une méthode de rejet, des automates biréversibles à deux états engendrant des groupes finis. Cette méthode à cependant l'inconvénient majeur d'être très vite inefficace quand la taille de l'alphabet augmente. En fait, on peut, dans le cas des automates biréversibles à 2 états, identifier la forme des permutations qui permettent d'engendrer des groupes finis :

Lemme 4.3

Soit $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate biréversible à deux états (0 et 1) et k lettres. Alors $\langle \mathcal{A} \rangle$ est fini si et seulement si on peut partitionner l'alphabet en trois sous-ensembles disjoints $\Sigma = \Sigma_s \sqcup \Sigma_f \sqcup \Sigma_c$, préservés par ρ_x, pour tout $x \in \Sigma$ et tels que

- $x \in \Sigma_s \iff \forall q \in Q, \delta_x(q) = q$,
- $x \in \Sigma_f \iff \forall q \in Q, \delta_x(q) \neq q$,
- $x \in \Sigma_c \iff (\delta_x(0) = 0 \Leftrightarrow \delta_x(1) = 1, \delta_x(0) = 1 \Leftrightarrow \delta_x(1) = 0)$, et $\rho_0(x) = \rho_1(x)$.

Démonstration. Supposons que $\mathcal{A}$ satisfait les hypothèses énoncées dans le théorème. Alors dans $\mathfrak{d}\mathcal{A}$, l'ensemble Σ des états est partitionné en trois ensembles de composantes fortement connexes $\Sigma = \Sigma_s \sqcup \Sigma_f \sqcup \Sigma_c$ et les états de Σ_s (*resp.* Σ_f) ont tous la même action, égale à l'identité (*resp.* la négation), on peut donc minimiser cet automate et on obtient que Σ_s (*resp.* Σ_f) a un seul état bouclant sur lui-même. Alors l'automate $\mathfrak{dmd}\mathcal{A}$ se minimise vers un automate à un unique état.
Réciproquement, prenons un automate engendrant un groupe fini. D'après le résultat de Klimann [63], cet automate est $\mathfrak{md}$-trivial. Sans perte de généralité, on suppose que $\mathcal{A}$ est minimal, et que la condition de partition n'est pas respectée, et donc qu'il existe $x \in \Sigma$ telle que $\delta_x(0) = 0$ et $\delta_x(1) = 0$, ou bien $\delta_x(0) = 1, \delta_x(1) = 0$, et $\rho_0(x) = \rho_1(x)$ (le cas $\delta_x(0) = 0, \delta_x(1) = 1$ se traite de la même façon). Dans la première situation, l'automate n'est pas réversible, et on peut donc l'exclure. Dans la seconde, on a toujours dans $\mathfrak{dmd}\mathcal{A}$ que $\delta_x(0) = 1, \delta_x(1) = 0$, et $\rho_0(x) =$

$\rho_1(x)$, et donc 0 et 1 sont dans des classes de Nerode différentes. Ainsi la suite dualisation-minimalisation ne converge pas vers l'automate trivial, et donc $|\langle\mathcal{A}\rangle| = +\infty$. □

Cependant, même avec cet outil, il semble que l'on obtient une convergence vers un petit ensemble qui ne dépend que de la taille des composantes de cette partition de l'alphabet. Des investigations sont en cours à ce propos.

Une autre piste possible est de renverser la méthode de la $\mathfrak{md}$-réduction : au lieu de partir d'un automate et de chercher à le simplifier tout en gardant la finitude, on peut essayer de partir d'un automate simple, que l'on sait engendrer un groupe fini, et de le complexifier pour engendrer un groupe toujours fini mais plus sophistiqué.

Définition 4.4 (Expansion de l'automate)

Soient $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ un automate de Mealy biréversible connexe, $\ell \in \mathbb{N}$ et $\{\sigma_x\}_{x\in\Sigma}$ des permutations de S_ℓ. L'expansion de $\mathcal{A}$ selon σ est l'automate $\mathfrak{e}_{(\sigma_x)_x}\mathcal{A}$ dont l'ensemble des état est $Q \times \{0, \dots, \ell - 1\}$, l'alphabet Σ, les fonctions de production $\rho_{(q,i)} = \rho_q$ et

$$\delta_x((q, i)) = \delta_x(q)_{\sigma_x(i)} .$$

L'expansion d'un automate non connexe peut également être définie en se restreignant aux composantes connexes. Dans la suite, on notera $\mathfrak{e}\mathcal{A}$ pour une expansion arbitraire de $\mathcal{A}$ (quand on voudra parler de propriétés ne dépendant pas du choix des permutations)

On a alors :

Lemme 4.5

Soit $\mathcal{A}$ un automate de Mealy. On a $\mathfrak{me}\mathcal{A} = \mathfrak{m}\mathcal{A}$.

Lemme 4.6

Le groupe engendré par $\mathcal{A}$ est isomorphe au groupe engendré par $\mathfrak{e}\mathcal{A}$.

Comme pour la minimisation, on peut alterner expansion dans le primal et expansion dans le dual. On parlera de $\mathfrak{ed}$-extension. Un exemple de $\mathfrak{ed}$-extension est dessiné figure IV.6.

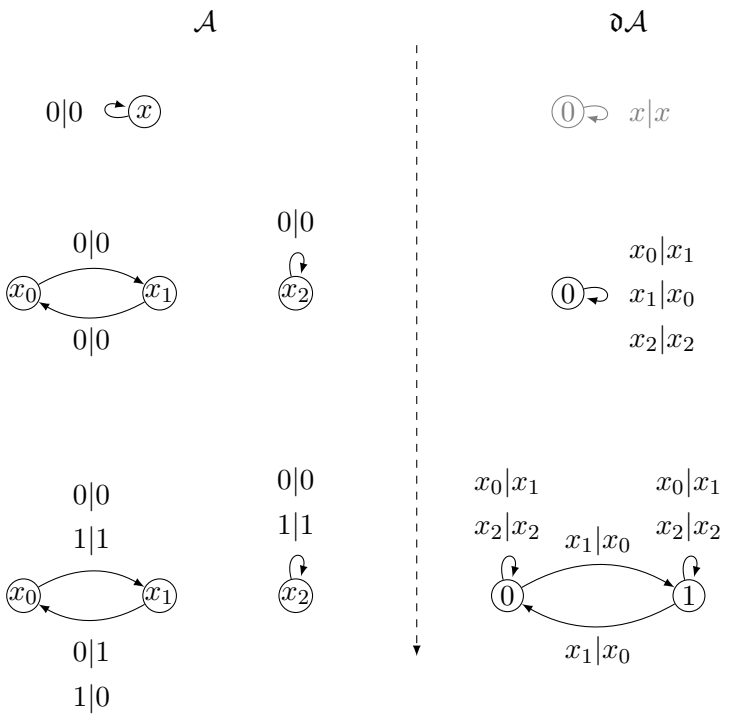


FIGURE IV.6 – Un exemple de $\mathfrak{ed}$-extension. On commence par l'expansion selon $(0,1)(3)$ puis dans le dual on effectue l'expansion $\mathfrak{e}_{(0,1)}$

Si l'on part d'un automate $\mathcal{T}$ engendrant un groupe fini, on a que la suite d'automates $\mathfrak{ede}\cdots\mathfrak{de}\mathcal{T}$ n'engendre que des groupes finis. On peut alors, par exemple, construire un automate aléatoire en effectuant une suite finie de $\mathfrak{ed}$-extensions depuis l'automate trivial. Remarquons que cette approche recouvre celle des automates cycliques (si l'on restreint les permutations utilisées dans les extensions) ou biréversibles à deux états. De plus, cette méthode laisse beaucoup de liberté dans le choix des paramètres : lois régissant la longueur de la suite, la taille de l'expansion, le choix des permutations. Tous cela permet d'espérer éviter une convergence vers un nombre trop réduit de groupes. Il convient maintenant de se demander quels paramètres peuvent être adaptés selon la situation, et surtout le montrer formellement.

Cette notion s'inscrit aussi dans l'étude du problème de finitude d'un groupe d'automate, et pourrait permettre de mieux appréhender la relation entre la taille d'un groupe et celle de celui engendré par son dual. En particulier, la compréhension de la relation entre $\langle\mathcal{A}\rangle$ et $\langle\mathfrak{ded}\mathcal{A}\rangle$, même dans le cas d'une expansion selon des permutations choisies dans un sous-ensemble spécifique, devrait être très instructive.

Conclusion et perspectives

Dans cette thèse, on a mis en lumière comment la théorie des automates peut servir à expliquer, approfondir et analyser des problèmes issus de la théorie des (semi-)groupes.
En particulier, les chapitres II et III, mettent en évidence des transferts de propriétés structurelles de l'automate de Mealy au groupe qu'il engendre, tandis que le chapitres III et IV montrent comment les automates de Mealy peuvent fournir un nouvel éclairage à un problème classique de théorie des automates.

Dans le chapitre II, on a créé et étudié de nouveaux outils pour chercher à savoir si un automate de Mealy réversible peut engendrer un groupe de Burnside infini. On a apporté une réponse négative à ce problème dans de nombreux cas, et un objectif naturel est maintenant d'adapter nos preuves et méthodes pour montrer le cas général, ou tout du moins le cas d'un automate connexe. Il est aussi légitime de se demander si nos outils ont un sens dans le cas d'un automate qui n'est pas inversible, ce qui nous amènerait à nous pencher sur le problème de Burnside pour les semi-groupes d'automate.
D'autre part, les arbres de Schreier et les chemins auto-repliants contiennent assez d'information pour être utilisés dans d'autres contextes de la théorie des groupes, notamment dans les problèmes de croissances. Les résultats de Klimann [64] suggèrent que la réversibilité induit un type spécifique de croissance, bornée ou exponentielle. Plus ambitieusement, il semble raisonnable de chercher à montrer que le problème de finitude est décidable pour les groupes engendrés par un automate de Mealy (bi)réversible, ainsi que l'a fait Klimann pour le cas à deux états.
De façon plus globale, il nous semble intéressant de déterminer si une propriété structurelle donnée de l'automate peut être reliée avec une propriété du (semi-)groupe, et dans l'avenir proche on cherchera à savoir si des problèmes comme celui du sac à dos ou bien celui de la transitivité par niveau sont décidables pour les groupes engendrés par des automates appartenant à des sous-classes spécifiques. Il paraît aussi intéressant de chercher à généraliser à l'univers des semi-groupes des résultats connus pour les groupes, par exemple en cherchant à savoir s'il existe une notion de semi-groupe à activité bornée liée à la structure de l'automate de Mealy et déterminer si les problèmes de l'ordre ou de la conjugaison sont décidables pour cette classe.

Dans le chapitre III, on a vu comment des notions classiques de théorie des automates et de théorie des langages (entropie, langage accepté par un automate de Büchi), permettaient de retrouver et généraliser des résultats connus de théorie des groupes, et cela par des méthodes bien plus élémentaires. Cette approche nous paraît donc très pertinente et on cherchera à l'approfondir en essayant de redémontrer des résultats classiques, dans l'espoir de les étoffer, ainsi qu'en essayant dès que possible d'utiliser ces notions dans de nouveaux problèmes.
Dans ce chapitre, très proche de la dynamique symbolique, le lien entre automates de Mealy et pavages de Wang a aussi été (re)mis en avant . On a utilisé une approche différente de celle de Gillibert, mais de façon générale ce lien semble fort et s'étend vraisemblablement aux automates cellulaires et aux sous-shifts de type fini, qui généralisent les pavages de Wang. Cette intuition est appuyée par les récents travaux de Delacourt et Ollinger mettant en correspondance le problème de la finitude dans les groupes d'automate avec celui de la périodicité dans les automates cellulaires unidirectionnels permutifs. Si les deux communautés sont conscientes que ce lien existe, il est manifestement nécessaire de partager nos points de vue et de démêler les ressemblances superficielles des similitudes profondes.

Le chapitre IV contient lui aussi de nombreuses directions possibles pour continuer nos travaux : du côté des groupes finis, on peut chercher à effectuer la génération aléatoire dans une classe d'automates de Mealy plus riche. On peut aussi se demander du côté des (semi-)groupes infinis si les (semi-)groupes d'automate aléatoires possèdent génériquement une propriété donnée. Grâce au chapitre II, on sait que le semi-groupe engendré par un automate de Mealy inversible et réversible est génériquement sans torsion (et donc que le groupe est infini), peut-on obtenir d'autres résultats, par exemple sur l'hyperbolicité du groupe ou la malnormalité des sous-groupes ? Là encore, ces questions sont assez étroitement reliées au problème de finitude ; mais on peut aussi se demander comment générer aléatoirement des automates de Mealy aux propriétés spécifiques. En effet, il est facile de tirer uniformément au hasard un automate de Mealy inversible, ou réversible ou même ayant simultanément ces deux propriétés, et, avec le travail de De Felice et Nicaud, on sait aussi générer uniformément des automates à cycles sans échappatoire. Cependant certaines classes semblent plus difficiles à manier dans ce contexte : par exemple celle des automates biréversibles, pour laquelle ne sait pas effectuer une génération efficace, et où tout résultat de dénombrement serait bienvenu.

Il reste également de nombreux problèmes liés à ces automates de Mealy qui n'ont pas été abordés dans cette thèse. On peut par exemple essayer de lier graphes de Schreier et graphes expanseurs, ou encore, ce qui est sans doute une des questions centrales pour ces groupes, se demander s'il existe des groupes ou monoïdes résiduellement finis et ayant un problème du mot décidable qui ne sont pas des groupes d'automate. On connaît de tels exemples pour les semi-groupes, mais très peu et on est encore loin d'une caractérisation. Cette question est

aussi à mettre en relation avec les traductions possibles entre (semi-)groupes d'automate et (semi-)groupes automatiques, ainsi qu'avec les (semi-)groupes d'automates cellulaires et de sous-shifts.

Index

Bibliographie

[1] A. Akhavi et al. "On the finiteness problem for automaton (semi)groups". In : *International Journal of Algebra and Computation* 22.6 (2012), p. 1–26 (cf. p. 25, 28, 29, 42, 49, 66, 70, 92, 129).

[2] S.V. Alešin. "Finite automata and the Burnside problem for periodic groups". In : *Akademiya Nauk SSSR. Matematicheskie Zametki* 11 (1972), p. 319–328 (cf. p. 2, 12, 47, 61).

[3] A. S. Antonenko. "On transition functions of Mealy automata of finite growth". In : *Matematychni Studii.* 29.1 (2008), p. 3–17 (cf. p. 18, 32, 49, 129, 130).

[4] W.R. Ashby, C.E. Shannon et J. McCarthy. *Automata Studies : Annals of Mathematics Studies. Number 34.* Annals of Mathematics Studies. Princeton University Press, 1956 (cf. p. 1).

[5] L. Bartholdi. "Algorithmic Decidability of Engel's Property for Automaton Groups". In : *Computer Science - Theory and Applications - 11th International Computer Science Symposium in Russia, CSR 2016, St. Petersburg, Russia, June 9-13, 2016, Proceedings.* 2016, p. 29–40 (cf. p. 51).

[6] L. Bartholdi. *FR – GAP package "Computations with functionally recursive groups", Version 2.2.1. http ://www.gap-system.org/Packages/fr.html.* 2015 (cf. p. 10).

[7] L. Bartholdi. "Lower Bounds on the growth of a group acting on the binary rooted tree". In : *International Journal of Algebra and Computation* 11.01 (2001), p. 73–88. eprint : `http://www.worldscientific.com/doi/pdf/10.1142/S0218196701000395` (cf. p. 55).

[8] L. Bartholdi. "The growth of Grigorchuk′s torsion group". In : *Internat. Math. Res. Notices* (1998), p. 1049–1054 (cf. p. 55).

[9] L. Bartholdi, I.I. Reznykov et V.I. Sushchansky. "The smallest Mealy automaton of intermediate growth". In : *Journal of Algebra* 295.2 (2006), p. 387–414 (cf. p. 55).

[10] L. Bartholdi et Z. Šunić. “On the word and period growth of some groups of tree automorphisms”. In : *Communications in Algebra* 29-11.11 (2001), p. 4923–4964 (cf. p. 61).

[11] F. Bassino, C. Nicaud et P. Weil. “Generic properties of subgroups of free groups and finite presentations”. In : *Contemporary Mathematics* 677 (2016), p. 1–44 (cf. p. 127).

[12] F. Bassino, C. Nicaud et P. Weil. “Random Generation of Finitely Generated Subgroups of a Free Group”. In : *IJAC* 18.2 (2008), p. 375–405 (cf. p. 127).

[13] Frédérique Bassino, Cyril Nicaud et Pascal Weil. “On the genericity of Whitehead minimality”. In : *Journal of Group Theory* 19.1 (2016), p. 137–159 (cf. p. 127).

[14] F. Bassino et al. “Statistical properties of subgroups of free groups”. In : *Random Struct. Algorithms* 42.3 (2013), p. 349–373 (cf. p. 127).

[15] V.V. Belyaev, N.F. Sesekin et V.I. Trofimov. “Growth functions of semigroups and loops”. In : *Ural. Gos. Univ. Mat. Zap* 10 (1977), p. 3–8 (cf. p. 55).

[16] M. V. Berlinkov. “On the Probability of Being Synchronizable”. In : *Algorithms and Discrete Applied Mathematics - Second International Conference, CALDAM 2016, Thiruvananthapuram, India, February 18-20, 2016, Proceedings*. 2016, p. 73–84 (cf. p. 127).

[17] S. R. Blackburn, J.R. Britnell et M Wildon. “The probability that a pair of elements of a finite group are conjugate”. In : *J. London Math. Society* 86.3 (2012), p. 755–778 (cf. p. 141, 142).

[18] I. V. Bondarenko et R. V. Kravchenko. “Finite-state self-similar actions of nilpotent groups”. In : *Geometriae Dedicata* 163.1 (2013), p. 339–348 (cf. p. 52).

[19] I. V. Bondarenko et al. “On the conjugacy problem for finite-state automorphisms of regular rooted trees”. In : *Groups Geom. Dyn.* 7.2 (2013). With an appendix by R. M. Jungers, p. 323–355 (cf. p. 2, 18, 32, 50).

[20] I. Bondarenko, D. D’Angeli et T. Nagnibeda. “Ends of Schreier graphs and cut-points of limit spaces of self-similar groups”. http ://arxiv.org/abs/1601.07587 (cf. p. 101, 118).

[21] I. Bondarenko, D. D’Angeli et E. Rodaro. “The lamplighter group $Z_3 \wr Z$ generated by a bireversible automaton”. In : *Communications in Algebra* (to appear). http ://arxiv.org/abs/1502.07981 (cf. p. 50).

[22] I. Bondarenko et al. “Groups generated by 3-state automata over a 2-letter alphabet. II”. In : *Journal of Mathematical Sciences* 156.1 (2009), p. 187–208 (cf. p. 21).

[23] T. Brough et A. J. Cain. “Automaton semigroups : new construction results and examples of non-automaton semigroups”. In : *ArXiv e-prints* (jan. 2016). arXiv : `1601.01168 [math.GR]` (cf. p. 41, 46).

[24] W. Burnside. “On an unsettled question in the theory of discontinuous groups”. In : *Quart. J. Math.* 33 (1902), p. 230–238 (cf. p. 12, 46).

[25] K.-U. Bux *et al. Selfsimilar groups and conformal dynamics Problem List* (cf. p. 46).

[26] A. J. Cain. “Automaton semigroups”. In : *Theoretical Computer Science* 410.47 (2009), p. 5022–5038 (cf. p. 37, 113).

[27] L. Caponi. “On the classification of groups generated by automata with 4 states over a 2-letter alphabet”. Thèse de doct. University of South Florida, 2014 (cf. p. 21, 70, 94, 95).

[28] D. D’Angeli et E. Rodaro. “A geometric approach to (semi)-groups defined by automata via dual transducers”. In : *Geometriae Dedicata* 174 (2015), p. 375–400 (cf. p. 62, 66, 67).

[29] D. D’Angeli et al. “Boundary action of automaton groups without critical points and Wang tilings”. (in preparation) (cf. p. 5, 102, 115).

[30] S. De Felice et C. Nicaud. “Random generation of deterministic acyclic automata using the recursive method”. In : *Computer Science - Theory and Applications - 8th International Computer Science Symposium in Russia, CSR 2013, Ekaterinburg, Russia, June 25-29, 2013. Proceedings*. 2013, p. 88–99 (cf. p. 21).

[31] J. D. Dixon. “The probability of generating the symmetric group”. In : *Mathematische Zeitschrift* 110.3 (1969), p. 199–205 (cf. p. 128).

[32] P. Erdős. “Graph theory and probability”. In : *canad. J. Math* 11.11 (1959), p. 34–38 (cf. p. 127).

[33] P. Erdős. “Some remarks on the theory of graphs”. In : *Bull. Amer. Math. Soc.* 53.4 (avr. 1947), p. 292–294 (cf. p. 127).

[34] P. Erdős et P. Turán. “On some problems of statistical group theory III”. In : *Acta. Math. Acad. Sci. Hungar.* 18 (1967), p. 309–320 (cf. p. 128).

[35] P. Erdős et P. Turán. “On some problems of statistical group theory V”. In : *Acta. Math. Acad. Sci. Hungar.* 1 (1971), p. 5–13 (cf. p. 137).

[36] J. Fabrykowski et N. Gupta. “On groups with sub-exponential growth functions”. In : *J. Indian Math. Soc. (N.S.)* 49.3-4 (1985), 249–256 (1987) (cf. p. 2, 20, 55).

[37] P. Flajolet et al. “A Hybrid of Darboux’s Method and Singularity Analysis in Combinatorial Asymptotics”. In : *Electronic Journal of Combinatorics* 13(1).1 (2006), p. 1–35 (cf. p. 141).

[38] E. Frenkel, A. Nikolaev et A. Ushakov. “Knapsack problems in products of groups”. In : *Journal of Symbolic Computation* 74 (2016), p. 96–108 (cf. p. 52).

[39] R. Frucht. “Herstellung von Graphen mit vorgegebener abstrakter Gruppe.” German. In : *Compos. Math.* 6 (1938), p. 239–250 (cf. p. 1).

[40] GAP – *Groups, Algorithms, and Programming*. Version 4.7.7. http ://www.gap-system.org. The GAP Group. 2015 (cf. p. 10).

[41] P. Gillibert. “The finiteness problem for automaton semigroups is undecidable”. In : *International Journal of Algebra and Computation* 24-1.1 (2014), p. 1–9 (cf. p. 2, 49, 121, 125, 129).

[42] Y. Glasner et S. Mozes. “Automata and square complexes”. In : *Geometriae Dedicata* 111 (2005), p. 43–64 (cf. p. 2, 25, 49, 121).

[43] V. M. Gluškov. “Abstract theory of automata”. In : *Akademiya Nauk SSSR i Moskovskoe Matematicheskoe Obshchestvo. Uspekhi Matematicheskikh Nauk* 16-5 (1961), p. 3–62 (cf. p. 2, 8, 42).

[44] Th. Godin. “An Analogue to Dixon Theorem for Automaton Groups.” ANALCO17 (cf. p. 4, 130, 136).

[45] Th. Godin et I. Klimann. “Connected Reversible Mealy Automata of Prime Size Cannot Generate Infinite Burnside Groups”. In : *41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016, August 22-26, 2016 - Kraków, Poland*. 2016, 44 :1–44 :14 (cf. p. 3, 58, 62, 64).

[46] Th. Godin, I. Klimann et M. Picantin. “On torsion-free semigroups generated by invertible reversible Mealy automata”. In : *Language and automata theory and applications*. T. 8977. Lecture Notes in Comput. Sci. Springer, Cham, 2015, p. 328–339 (cf. p. 3, 58, 61, 64, 92).

[47] E. S. Golod. “On nil-algebras and finitely residual groups”. In : *Izv. Akad. Nauk SSSR. Ser. Mat.* 28 (1964), p. 273–276 (cf. p. 46).

[48] E. S. Golod et I. Shafarevich. “On the class field tower”. In : *Izv. Akad. Nauk SSSR Ser. Mat.* 28 (1964), p. 261–272 (cf. p. 46).

[49] R. I. Grigorchuk. “Degrees of growth of finitely generated groups and the theory of invariant means”. In : *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya* 48-5.5 (1984), p. 939–985 (cf. p. 2, 19, 55).

[50] R. I. Grigorchuk. “On Burnside’s problem on periodic groups”. In : *Akademiya Nauk SSSR. Funktsional′nyĭ Analiz i ego Prilozheniya* 14-1 (1980), p. 53–54 (cf. p. 2, 12, 48, 61).

[51] R. I. Grigorchuk. “Some topics of the dynamics of group actions on rooted trees”. In : *The Proceedings of the Steklov Institute of Math.* 273 (2011), p. 1–118 (cf. p. 101, 102, 115).

[52] R. I. Grigorchuk, V. V. Nekrashevich et V. I. Sushchanskiĭ. “Automata, dynamical systems, and groups”. In : *Trudy Matematicheskogo Instituta Imeni V. A. Steklova. Rossiĭskaya Akademiya Nauk* 231 (2000), p. 134–214 (cf. p. 56, 101).

[53] R. I. Grigorchuk et D. Savchuk. “Ergodic decomposition of group actions on rooted trees”. In : *Proceedings of the Steklov Institute of Mathematics* 292.1 (2016), p. 94–111 (cf. p. 101).

[54] R. I. Grigorchuk et D. Savchuk. “Self-similar groups acting essentially freely on the boundary of the binary rooted tree”. In : *Group theory, combinatorics, and computing.* T. 611. Contemp. Math. Amer. Math. Soc., Providence, RI, 2014, p. 9–48 (cf. p. 115).

[55] R. I. Grigorchuk et A. Żuk. “On a torsion-free weakly branch group defined by a three state automaton”. In : *International Journal of Algebra and Computation* 12.1-2 (2002). International Conference on Geometric and Combinatorial Methods in Group Theory and Semigroup Theory (Lincoln, NE, 2000), p. 223–246 (cf. p. 2).

[56] M. Gromov. “Groups of polynomial growth and expanding maps”. In : *Publ. Math., Inst. Hautes Étud. Sci* (1981), p. 53–73 (cf. p. 54).

[57] N. Gupta et S. Sidki. “On the Burnside problem for periodic groups”. In : *Mathematische Zeitschrift* 182-3 (1983), p. 385–388 (cf. p. 2, 20, 61).

[58] P. de la Harpe. *Topics in Geometric Group Theory.* Chicago Lectures in Mathematics. University of Chicago Press, 2000 (cf. p. 11, 12).

[59] E. Jeandel et M. Rao. “An aperiodic set of 11 Wang tiles”. In : *ArXiv e-prints* (juin 2015). arXiv : `1506.06492 [cs.DM]` (cf. p. 121).

[60] M. Kambites, P. V. Silva et B. Steinberg. “The spectra of lamplighter groups and Cayley machines”. In : *Geometriae Dedicata* 120 (2006), p. 193–227 (cf. p. 104).

[61] J. Kari. “The Nilpotency Problem of One-Dimensional Cellular Automata”. In : *SIAM Journal on Computing* 21.3 (1992), p. 571–586. eprint : `http://dx.doi.org/10.1137/0221036` (cf. p. 121, 124).

[62] M. Kassabov et I. Pak. “Groups of oscillating intermediate growth”. In : *Ann. of Math. (2)* 177.3 (2013), p. 1113–1145 (cf. p. 55).

[63] I. Klimann. “Automaton Semigroups : The Two-state Case”. In : *Theor. Comput. Syst. (special issue STACS’13)* (2014), p. 1–17 (cf. p. 2, 17, 27, 50, 58, 61, 76, 79, 147).

[64] I. Klimann. “On level-transitivity and exponential growth”. In : *Semigroup Forum* (2016), p. 1–7 (cf. p. 56, 99, 151).

[65] I. Klimann, J. Mairesse et M. Picantin. “Implementing Computations in Automaton (Semi)groups”. In : *Proc. 17th CIAA*. T. 7381. LNCS. 2012, p. 240–252 (cf. p. 134, 135).

[66] I. Klimann et M. Picantin. “A Characterization of Those Automata That Structurally Generate Finite Groups”. In : *LATIN 2014 : Theoretical Informatics - 11th Latin American Symposium, Montevideo, Uruguay, March 31 - April 4, 2014. Proceedings.* 2014, p. 180–189 (cf. p. 18, 49, 129).

[67] I. Klimann, M. Picantin et D. Savchuk. “A Connected 3-State Reversible Mealy Automaton Cannot Generate an Infinite Burnside Group”. In : *Developments in Language Theory - 19th International Conference, DLT 2015, Liverpool, UK, July 27-30, 2015, Proceedings.* 2015, p. 313–325 (cf. p. 17, 58, 61–64, 66, 67, 70, 79, 92).

[68] I. Klimann, M. Picantin et D. Savchuk. “Orbit automata as a new tool to attack the order problem in automaton groups”. In : *Journal of Algebra* 445 (2016), p. 433–457 (cf. p. 64, 70, 94, 95).

[69] D. König, M. Lohrey et G. Zetzsche. “Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups”. In : *ArXiv e-prints* (juil. 2015). arXiv : `1507.05145 [math.GR]` (cf. p. 52).

[70] B. Le Gloannec. “The 4 way deterministic Periodic Domino Problem is undecidable”. https ://hal.archives-ouvertes.fr/hal-00985482. 2014 (cf. p. 122, 124, 125).

[71] M. W. Liebeck et A. Shalev. “The probability of generating a finite simple group”. In : *Geometriae Dedicata* 56.1 (1995), p. 103–113 (cf. p. 128).

[72] V. Lukkarila. “The 4-way deterministic tiling problem is undecidable”. In : *Theoretical Computer Science* 410.16 (2009), p. 1516–1533 (cf. p. 124).

[73] A. Mann. *How Groups Grow.* London Mathematical Society Lecture Note Series. Cambridge University Press, 2011 (cf. p. 19, 53).

[74] V. D. Mazurov et E. I. Khukhro. “Unsolved Problems in Group Theory. The Kourovka Notebook. No. 18 (English version)”. In : *ArXiv e-prints* (jan. 2014). arXiv : `1401.0300 [math.GR]` (cf. p. 45).

[75] G. Mealy. “a Method for Synthesizing Sequential Circuits”. In : *Bell System Tech. Jour.* 34 (1955), p. 1045–1079 (cf. p. 22).

[76] J. Milnor. “Problem 5603”. In : *Amer. Math. Monthly* 75.6 (1968), p. 685–686 (cf. p. 19).

[77] Y. Muntyan et D. Savchuk. *AutomGrp – GAP package for computations in self-similar groups and semigroups, Version 1.2.4. http ://www.gap-system.org/Packages/automgrp.html.* 2014 (cf. p. 10).

[78] V. Nekrashevych. *Self-similar groups.* T. 117. Mathematical Surveys and Monographs. Providence, RI : American Mathematical Society, 2005, p. xii+231 (cf. p. 27, 28, 50, 66).

[79] E. Netto. *Substitutionstheorie und ihre Anwendung auf die Algebra.* 1882 (cf. p. 128).

[80] C. Nicaud. “Fast Synchronization of Random Automata”. In : (2016), 43 :1–43 :12 (cf. p. 127).

[81] P. S. Novikov et S. I. Adian. “Infinite periodic groups. I, II, III”. In : *Mathematics of the USSR-Izvestiya* 2 (1968), p. 665 (cf. p. 47).

[82] Y. Ollivier. “A January 2005 invitation to random groups”. In : *Ensaios Matemáticos 10, Sociedade Brasileira de Matemática, Rio de Janeiro*. 2005 (cf. p. 127).

[83] D. Perrin et J.-É. Pin. *Infinite words : automata, semigroups, logic and games*. Pure and applied mathematics. London, San Diego (Calif.) : Academic, 2004 (cf. p. 106).

[84] M. Picantin. “Automatic semigroups vs automaton semigroups”. In : *ArXiv e-prints* (sept. 2016). arXiv : `1609.09364 [math.GR]` (cf. p. 24).

[85] J-É. Pin. “Logic, Semigroups and Automata on Words”. In : *Ann. Math. Artif. Intell.* 16 (1996), p. 343–384 (cf. p. 2).

[86] A. Russyev. “Finite groups as groups of automata with no cycles with exit”. In : *Algebra and Discrete Mathematics* 9.1 (2010), p. 86–102 (cf. p. 18, 32, 49, 129).

[87] J. Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009 (cf. p. 73).

[88] A. Salomaa. *Formal languages*. ACM monograph series. Academic Press, 1973 (cf. p. 2).

[89] M.-P. Schützenberger. “On Finite Monoids Having Only Trivial Subgroups”. In : *Information and Control* 8.2 (1965), p. 190–194 (cf. p. 1).

[90] M.-P. Schützenberger. “Une théorie algébrique du codage”. In : *Séminaire Dubreil-Pisot, année 1955-56*. Exposé No. 15, 27 février 1956, 24 pages. Paris : Inst. H. Poincaré, 1956 (cf. p. 1).

[91] W. R. Scott. *Group Theory*. Dover Books on Mathematics. Dover Publications, 1964 (cf. p. 138).

[92] A. Shalev. “Random Generation of Simple Groups by Two Conjugate Elements”. In : *Bulletin of the London Mathematical Society* 29.5 (1997), p. 571–576 (cf. p. 145).

[93] S. Sidki. “Automorphisms of one-rooted trees : growth, circuit structure, and acyclicity”. In : *Journal of Mathematical Sciences (New York)* 100.1 (2000). Algebra, 12, p. 1925–1943 (cf. p. 32).

[94] N.J.A. Sloane. *The On-Line Encyclopedia of Integer Sequences*. published electronically at (cf. p. 141).

[95] L. Staiger. “Entropy of finite-state omega-languages.” In : *Problems of Control and Information Theory* 14.5 (1985), p. 383–392 (cf. p. 111).

[96] B. Steinberg. “On some algorithmic properties of finite state automorphisms of rooted trees”. In : *Algorithmic problems of group theory, their complexity, and applications to cryptography*. T. 633. Contemp. Math. Amer. Math. Soc., Providence, RI, 2015, p. 115–123 (cf. p. 19, 56).

[97] B. Steinberg, M. Vorobets et Y. Vorobets. “Automata over a binary alphabet generating free groups of even rank”. In : *International Journal of Algebra and Computation* 21.1-2 (2011), p. 329–354 (cf. p. 2, 115).

[98] Z Šunić et E. Ventura. “The conjugacy problem in automaton groups is not solvable”. In : *Journal of Algebra* 364 (2012), p. 148–154 (cf. p. 51).

[99] A. M. Vershik. “Nonfree actions of countable groups and their characters”. In : *Journal of Mathematical Sciences* 174.1 (2011), p. 1–6 (cf. p. 102).

[100] M. Vorobets et Y. Vorobets. “On a free group of transformations defined by an automaton”. In : *Geometriae Dedicata* 124 (2007), p. 237–249 (cf. p. 49).

[101] M. Vorobets et Y. Vorobets. “On a series of finite automata defining free transformation groups”. In : *Groups, Geometry, and Dynamics* 4.2 (2010), p. 377–405 (cf. p. 49).

[102] Y. Vorobets. “Notes on the Schreier graphs of the Grigorchuk group”. In : *Dynamical systems and group actions*. T. 567. Contemp. Math. Amer. Math. Soc., Providence, RI, 2012, p. 221–248 (cf. p. 57, 102–105, 109).

[103] H. Wang. “Proving theorems by pattern recognition II”. In : *The Bell System Technical Journal* 40.1 (jan. 1961), p. 1–41 (cf. p. 121).

[104] H. S. Wilf. “The variance of the Stirling cycle numbers”. In : *ArXiv Mathematics e-prints* (nov. 2005). eprint : `math/0511428` (cf. p. 141).

[105] J. S. Wilson. “On exponential growth and uniformly exponential growth for groups”. In : *Invent. Math.* 155.2 (2004), p. 287–303 (cf. p. 55).

[106] E. I. Zel′manov. “Solution of the restricted Burnside problem for 2-groups”. In : *Matematicheskiĭ Sbornik* 182-4.4 (1991), p. 568–592 (cf. p. 44, 92).

[107] E. I. Zel′manov. “Solution of the restricted Burnside problem for groups of odd exponent”. In : *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya* 54-1.1 (1990), p. 42–59, 221 (cf. p. 44, 92).