Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

SEMI-GROUPES FORTEMENT AUTOMATIQUES

Paul Mercat

Tome 141
Fascicule 3

2013

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 423-479

Bull. Soc. math. France
141 (3), 2013, p. 423–479

SEMI-GROUPES FORTEMENT AUTOMATIQUES

BY PAUL MERCAT

ABSTRACT. — Dans cet article, nous introduisons la notion de semi-groupe fortement automatique, qui entraîne la notion d'automaticité des semi-groupes usuelle. On s'intéresse particulièrement aux semi-groupes de développements en base β, pour lesquels on obtient un critère de forte automaticité.

RÉSUMÉ (*Strongly automatic semigroups*). — In this paper, we introduce the notion of strongly automatic semigroup, which implies the usual notion of automaticity. We focus on semigroups of β-adics developpements, for which we obtain a criterion of strong automaticity.

1. Introduction

1.1. Organisation de l'article. — Dans cet article, nous introduisons la notion de semi-groupe fortement automatique, qui consiste à avoir un ensemble de relations qui soit un langage rationnel, c'est-à-dire reconnaissable par un automate fini. On démontre que la forte automaticité entraîne l'automaticité au sens usuel.

Texte reçu le 18 novembre 2011 et accepté le 3 juillet 2012.

PAUL MERCAT, Université Paris-Sud 11, 91405 Orsay •
E-mail : paul.mercat@math.u-psud.fr • *Url :* http://www.math.u-psud.fr/~mercat

2010 Mathematics Subject Classification. — 20M17, 20M05, 20M35, 11A63, 68R15.

Key words and phrases. — Semi-groupes, monoïdes, présentation finie, automaticité, automates finis, langages rationnels, nombres algébriques, nombres de Salem, développements β-adiques, croissance.

Pour les semi-groupes correspondant aux développements en base β, on démontre le résultat suivant :

THÉORÈME 1.1. — *Définissons un semi-groupe* Γ *engendré par les transformations :*

$$x \mapsto \beta x + t$$

pout $t \in A \subset \mathbb{C}$*, où* A *est une partie finie de* $\mathbb{C}$*, et* β *est un nombre complexe.*

Si le nombre complexe β *est transcendant, ou bien algébrique mais sans conjugué de module 1, alors pour toute partie* $A \subset \mathbb{C}$ *finie, le semi-groupe* Γ *est fortement automatique.*

Réciproquement, si le nombre complexe β *est algébrique et a au moins un conjugué de module 1, alors il existe une partie* $A \subset \mathbb{C}$ *finie telle que le semi-groupe* Γ *n'est pas fortement automatique.*

On commencera par faire des rappels sur les automates (voir partie 2). Puis dans la partie 3, on définira ce qu'est un semi-groupe fortement automatique, et l'on donnera quelques propriétés. On rappellera ensuite ce qu'est un semi-groupe automatique, et l'on montrera que les semi-groupes fortement automatiques sont automatiques. On s'intéressera ensuite aux semi-groupes correspondants aux développements en base β dans la partie 4 où l'on démontrera le théorème annoncé (voir théorème 4.2 et proposition 4.15). Enfin, la partie 5 est consacrée à des exemples, et rappelle des travaux en lien avec cet article.

Je remercie Laurent Bartholdi pour ses remarques qui ont entre autres permis d'obtenir un exemple de semi-groupe qui soit fortement automatique mais qui ne soit pas de présentation finie (voir proposition 4.31), et permis de généraliser plusieurs résultats. Je remercie aussi Vincent Guirardel pour ses nombreuses remarques pertinentes qui ont permis d'améliorer ce texte.

1.2. Motivation. — Ces notions d'automaticité et de forte automaticité fournissent d'une part une façon de représenter un semi-groupe infini avec une quantité finie de données (et donc cela permet de manipuler facilement ce semi-groupe sur ordinateur), et d'autre part donnent des informations combinatoires sur le semi-groupe (on obtient par exemple une asymptotique très précise du nombre d'éléments du semi-groupe). La notion de forte automaticité que l'on introduit, bien que plus simple que la notion d'automaticité, ne semble pas avoir été étudiée parce-qu'elle n'est pas intéressante pour les groupes. Mais il existe des exemples de semi-groupes fortement automatiques intéressants :

Voici un exemple simple de semi-groupe fortement automatique. Considérons le monoïde engendré par les trois transformations affines :

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3. \end{cases}$$

Par définition, c'est l'ensemble des composées de ces trois applications (en incluant l'identité).
Voici quelques questions que l'on peut se poser :

- Quel est l'asymptotique du nombre d'éléments pour la longueur des mots ?
- Comment peut-on déterminer si deux mots en les générateurs représentent le même élément du semi-groupe ?
- Y a-t'il une façon de représenter les éléments du semi-groupes par des mots uniques particuliers (que l'on appelera mots réduits) ?

La réponse à ces questions est donnée par la structure automatique du semi-groupe. Celle-ci est donnée par des automates tels que l'on peut en voir sur les figures suivantes (voir la partie 2 pour des rappels sur les automates) :

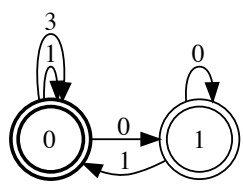


FIGURE 1. Automate reconnaissant un ensemble de mots réduits du semi-groupe. Les mots réduits sont ici les mots minimaux pour l'ordre lexicographique inverse, avec $0 < 1 < 3$.

On appelle *mots réduits* un choix de représentants uniques pour les éléments du semi-groupe par des mots en les générateurs. On voit sur l'automate de la figure 1 que les mots réduits sont ici exactement les mots ne contenant pas le mot 03.

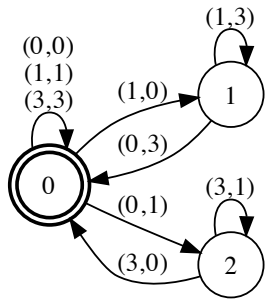


FIGURE 2. Automate reconnaissant les relations du semi-groupe.

On voit sur l'automate de la figure 2 que les relations du semi-groupe Γ s'obtiennent toutes à partir des relations $11^n0 = 03^n3$, par concaténation.

EXEMPLE 1.2. — *Le mot* $(1,0)(1,3)(0,3)$ *est reconnu par l'automate de la figure 2, et on a en effet la relation* $1 \circ 1 \circ 0 = 0 \circ 3 \circ 3$, *puisque l'on a l'égalité*

$$\frac{\frac{x}{3}+1}{3}+1 = \frac{\frac{x}{3}+3}{3}+3.$$

Deux mots $u_1...u_n$ et $v_1...v_n$ en les générateurs $\{0,1,3\}$ représentent le même élément du semi-groupe si et seulement si le mot $(u_1,v_1)...(u_n,v_n)$ est reconnu par l'automate de la figure 2.

L'automate de la figure 1 fournit un moyen de connaître le nombre d'éléments du semi-groupe de longueur n donnée : celui-ci est en effet égal au nombre de chemins de longueur n de l'état initial 0 vers les états finaux 0 et 1. Ceci est donné par la somme des deux premiers coefficients des puissances de la matrice d'adjacence du graphe :

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

dont les valeurs propres sont $\frac{\sqrt{5}+3}{2}$ et $\frac{3-\sqrt{5}}{2}$. Ainsi, on voit que le nombre d'éléments du semi-groupe de longueur n est exactement f_{2n+2}, où $(f_n)_{n\in\mathbb{N}}$ est la suite de Fibonnacci :

$$\begin{aligned} f_0 &= 0, \\ f_1 &= 1, \\ f_{n+2} &= f_{n+1} + f_n. \end{aligned}$$

En particulier, le nombre d'éléments du semi-groupe de longueur n est asymptotiquement

$$c\left(\frac{\sqrt{5}+3}{2}\right)^n + O\left(\left(\frac{3-\sqrt{5}}{2}\right)^n\right)$$

pour une constante $c > 0$.

Ici, le monoïde admet une présentation finie :

$$< 0, 1, 3 | 1 \circ 0 = 0 \circ 3 > .$$

Autrement dit, toutes les relations de ce semi-groupe se déduisent de la relation $1 \circ 0 = 0 \circ 3$. Par exemple, on en déduit la relation $1 \circ 1 \circ 0 = 1 \circ 0 \circ 3 = 0 \circ 3 \circ 3$.

2. Rappels sur les automates et les langages rationnels

Dans cette partie, je donne des rappels sur les automates qui seront utiles dans la suite. Les automates sont en quelques sortes des machines qui peuvent réaliser tous les calculs en temps linéaire ne nécessitant qu'une mémoire finie. Pour plus de détails, voir par exemple [3], sections 1.5.2, 1.6, et 1.7.

Définition 2.1. — *On appelle* automate *un quintuplet* $\mathcal{A} := (\Sigma, Q, T, I, F)$, *où*

1. Σ *est un ensemble fini appelé* alphabet,
2. Q *est un ensemble fini d'*états,
3. $T \subseteq Q \times \Sigma \times Q$ *est l'ensemble des* transitions,
4. $I \subseteq Q$ *est l'ensemble des* états initiaux,
5. $F \subseteq Q$ *est l'ensemble des* états finaux.

On dira que l'automate est déterministe *si l'on a* $\#I = 1$ *et*

$$[(p, a, q) \in T \text{ et } (p, a, r) \in T] \text{ implique } q = r.$$

Autrement dit, quand l'automate $\mathcal{A}$ *est déterministe,* T *est le graphe d'une fonction partielle de transition* $Q \times \Sigma \to Q$, *et il n'y a qu'un seul état initial.*

On considèrera parfois des automates infinis, c'est-à-dire des automates pour lesquels l'ensemble d'états Q est infini.

Notation . — *On notera* $p \xrightarrow{a} q$ *si* $(p, a, q) \in T$.

Notation . — *Étant donné un alphabet* Σ, *on notera* $\Sigma^* := \Sigma^{(\mathbb{N})}$ *l'ensemble des mots finis. Pour* $u \in \Sigma^*$, *on notera également* $u^* := \cup_{n \in \mathbb{N}} \{u^n\} = \{u\}^*$.

Représentation graphique. — On représente les automates comme des graphes dont les arêtes sont étiquetées par des lettres de l'alphabet. Sur les dessins de ce chapitre, l'état initial est en gras, et les états finaux sont les ronds dessinés avec un trait double.

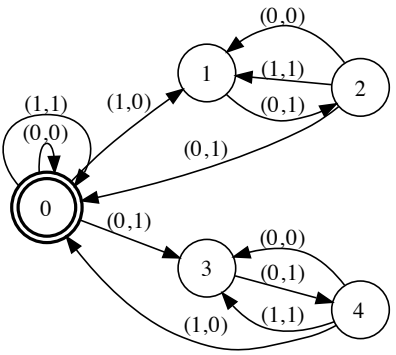


FIGURE 3. Automate ayant pour états {0, 1, 2, 3, 4}, pour alphabet {(0,0), (0,1), (1,0), (1,1)}, pour ensemble d'états initiaux {0} et pour ensemble d'états finaux {0}.

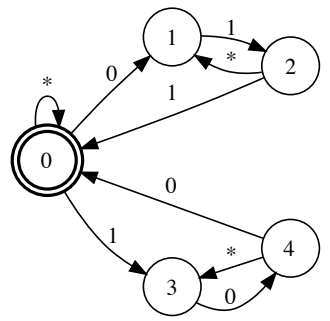


FIGURE 4. Automate ayant pour états {0, 1, 2, 3, 4}, pour alphabet {0, 1, *}, pour ensemble d'états initiaux {0} et pour ensemble d'états finaux {0}.

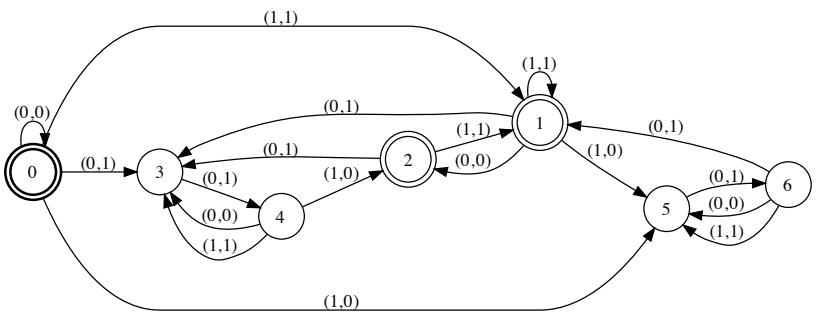


FIGURE 5. Automate ayant pour états {0, 1, 2, 3, 4, 5, 6}, pour alphabet {(0,0), (0,1), (1,0), (1,1)}, pour ensemble d'états initiaux {0} et pour ensemble d'états finaux {0, 1, 2}.

DÉFINITION 2.2. — *On appelle* langage reconnu par un automate $\mathscr{A} = (\Sigma, Q, T, I, F)$ *l'ensemble* $L_{\mathscr{A}}$ *des mots* $a_1 \dots a_n \in \Sigma^*$ *tels qu'il existe un*

chemin

$$I \ni q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \ldots\ldots \xrightarrow{a_{n-1}} q_{n-1} \xrightarrow{a_n} q_n \in F$$

dans l'automate A, d'un état initial vers un état final.
On dit qu'un mot $u \in \Sigma^*$ est reconnu *par l'automate $\mathscr{A}$ si l'on a $u \in L_{\mathscr{A}}$.*

Un mot $a_1 \ldots a_n$ est donc reconnu par l'automate $\mathscr{A}$ s'il existe un chemin dans le graphe, étiqueté par $a_1, a_2, \ldots, a_n$, partant d'un état initial et aboutissant à un état final.

REMARQUE 2.3. — *Si l'automate est déterministe, un tel chemin est unique.*

EXEMPLE 2.4. — *Voir figures 5, 7, 8 et 9.*

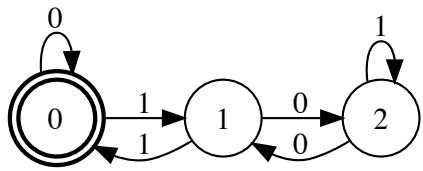


FIGURE 6. Automate reconnaissant l'ensemble des nombres écrits en binaires qui sont divisibles par 3.

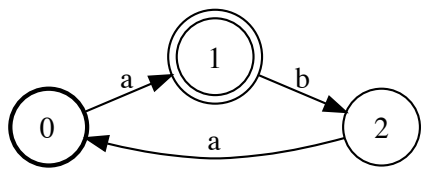


FIGURE 7. Automate reconnaissant l'ensemble des mots de la forme $a(baa)^n$.

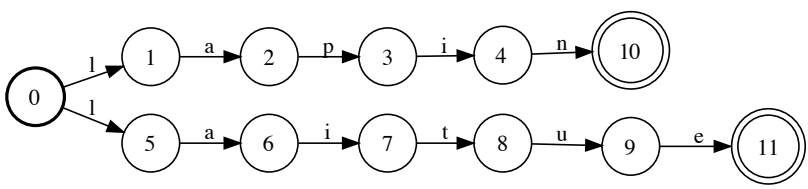


FIGURE 8. Automate non déterministe reconnaissant l'ensemble de mots {lapin, laitue}.

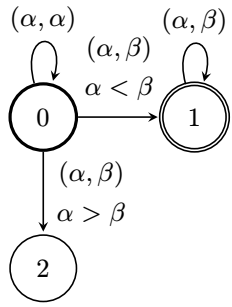


FIGURE 9. Automate reconnaissant les couples (u, v) de mots avec u strictement inférieur à v dans l'ordre lexicographique.

Dans la figure 9, dire qu'un couple (u, v) de mots de Σ^* est reconnu signifie qu'un mot $(u_1, v_1) \dots (u_n, v_n) \in (\Sigma \times \Sigma)^*$ est reconnu, avec $u = u_1 \dots u_n$ et $v = v_1 \dots v_n$. On suppose que l'alphabet Σ est muni d'une relation d'ordre totale.

DÉFINITION 2.5. — *On dit que deux automates $\mathcal{A}$ et $\mathcal{A}'$ sont* équivalents *s'ils reconnaissent le même langage : $L_{\mathcal{A}} = L_{\mathcal{A}'}$.*

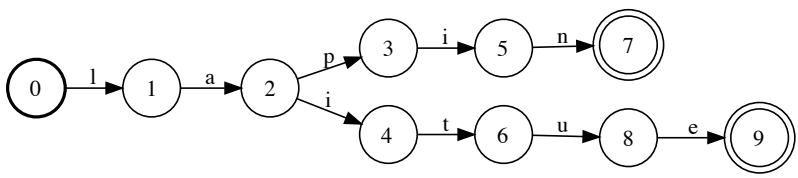


FIGURE 10. Automate déterministe équivalent à celui de la figure 8.

On a la proposition suivante :

PROPOSITION 2.6. — *Tout automate est équivalent à un automate déterministe.*

DÉFINITION 2.7. — *On appelle* automate minimal *d'un automate $\mathcal{A}$, un automate $\mathcal{A}'$ déterministe, équivalent à $\mathcal{A}$, et ayant un nombre minimal de sommets pour ces propriétés.*

PROPOSITION 2.8. — *L'automate minimal d'un automate $\mathcal{A}$ est unique. De plus si l'automate $\mathcal{A}$ est déterministe et complet, alors l'automate minimal s'obtient comme le quotient de l'automate $\mathcal{A}$ par une relation d'équivalence consistant à identifier des sommets entre eux.*

EXEMPLE 2.9. — *L'automate de la figure 10 est minimal.*

DÉFINITION 2.10. — *On appelle* transposée *d'un automate* $\mathcal{A} = (\Sigma, Q, T, I, F)$ *l'automate*

$$\mathcal{A}^t := (\Sigma, Q, T^t, F, I)$$

où $T^t := \{(p, a, q) \in Q \times \Sigma \times Q | (q, a, p) \in T\}$.

REMARQUE 2.11. — *Le langage reconnu par l'automate transposé* $\mathcal{A}^t$ *est la transposée du langage reconnu par l'automate initial* $\mathcal{A}$.

DÉFINITION 2.12. — *On appelle* émondé *d'un automate, l'automate restreint aux sommets par lesquels il passe un chemin d'un état initial à un état final. On dit qu'un automate est* émondé *s'il est égal à son émondé.*

Autrement dit, un automate est émondé s'il n'existe pas de sommet qui ne sert à rien !

PROPOSITION 2.13. — *Un automate (éventuellement infini) émondé déterministe, et de transposée déterministe est minimal. En particulier, s'il est infini, le langage qu'il reconnait n'est pas rationnel.*

Démonstration. — Soit L un langage sur l'alphabet Σ. Pour tout mot $w \in \Sigma^*$, on définit un quotient à gauche

$$w^{-1}L := \{u \in \Sigma^* | wu \in L\}.$$

Il est alors bien connu que le langage L est rationnel si et seulement si l'ensemble de ses quotients à gauche est fini (voir prop. 1.82 dans [3]), et l'on peut construire un automate minimal pour le langage L dont les états sont les quotients à gauche (voir déf. 1.83 dans [3]).

Soit maintenant $\mathcal{A}$ un automate émondé déterministe, et de transposée déterministe, reconnaissant un langage L. On peut associer à chaque état q de l'automate $\mathcal{A}$ un quotient à gauche $w^{-1}L$ pour un mot w étiquetant un chemin de l'état initial jusqu'à l'état q. Cela est possible puisque l'automate est émondé, et ce quotient ne dépend alors pas du mot w choisi : on le notera L_q. On a alors le fait suivant.

FAIT 1. — *Les quotients à gauches qui correspondent à deux états distincts de l'automate* $\mathcal{A}$ *sont distinctes.*

En effet, l'automate étant de transposée déterministe, si l'on considère un chemin d'un état q à un état final étiqueté par un mot w, alors il ne peut pas exister de chemin d'un état $q' \neq q$ vers un état final étiqueté par le même mot w. Cela se traduit par la disjonction $L_q \cap L_{q'} = \varnothing$. Or, chacun des deux langages est non vide, puisque l'automate est supposé émondé, d'où $L_q \neq L_{q'}$ si $q \neq q'$ sont deux états distincts de l'automate $\mathcal{A}$.

Les états de l'automate $\mathcal{A}$ correspondent donc à des quotients à gauche tous distincts, et la définition 1.83 dans [3] donne un automate minimal pour le langage L qui est exactement l'automate $\mathcal{A}$, d'où le résultat. □

Remarque 2.14. — *La réciproque est fausse : un automate minimal fini n'est pas nécessairement de transposée déterministe.*

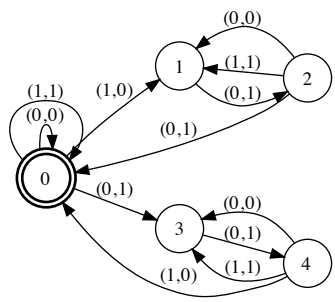


Figure 11. Automate minimal car vérifiant les conditions de la proposition 2.13.

Notation . — *Dans tout cet article, ϵ dénote le* mot vide*, c'est-à-dire le mot ayant* 0 *lettres.*

Définition 2.15. — *On définit l'ensemble des* langages rationnels *comme étant la plus petite partie* $\mathrm{Rat} \subset \mathcal{P}(\Sigma^*)$ *de l'ensemble des langages sur l'alphabet* Σ *vérifiant :*

1. $\varnothing \in \mathrm{Rat}$,
2. $\{\epsilon\} \in \mathrm{Rat}$ *(où ϵ est le mot vide),*
3. $\{a\} \in \mathrm{Rat}$ *pour tout* $a \in \Sigma$,
4. Rat *est stable par union :* $L, L' \in \mathrm{Rat}$ *implique* $L \cup L' \in \mathrm{Rat}$.
5. Rat *est stable par concaténation :* $L, L' \in \mathrm{Rat}$ *implique* $LL' \in \mathrm{Rat}$.
6. Rat *est stable par complémentaire :* $L \in \mathrm{Rat}$ *implique* $\Sigma^* \backslash L \in \mathrm{Rat}$.
7. Rat *est stable par étoile :* $L \in \mathrm{Rat}$ *implique* $L^* \in \mathrm{Rat}$.

On a le théorème suivant :

THÉORÈME 2.16 (Kleene). — *Un langage $L \subseteq \Sigma^*$ est rationnel si et seulement si c'est le langage d'un automate.*

Voir par exemple [3], théorème 1.59, page 36.

DÉFINITION 2.17. — *Étant donnés deux langages $L \subseteq \Sigma^*$ et $K \subseteq \Lambda^*$, respectivement sur les alphabets Σ et Λ, on appelle* produit *des deux langages, le langage noté $L \times K$ sur l'alphabet $\Sigma \times \Lambda$ définit par :*

$$L \times K := \{(a_1, b_1) \dots (a_n, b_n) \in (\Sigma \times \Lambda)^* | a_1 \dots a_n \in L \text{ et } b_1 \dots b_n \in K\}.$$

PROPOSITION 2.18. — *Le produit de deux langages rationnels est un langage rationnel.*

DÉFINITION 2.19. — *Étant donné un langage $L \subset (\Sigma \times \Lambda)^*$, on définit les projetés $p_1(L) \subset \Sigma^*$ et $p_2(L) \subset \Lambda^*$ du langage L par*

$$p_1(L) := \{u \in \Sigma^* | \textit{Il existe } v \in \Lambda^* \textit{ tel que } (u, v) \in L\},$$

$$p_2(L) := \{v \in \Lambda^* | \textit{Il existe } u \in \Sigma^* \textit{ tel que } (u, v) \in L\}.$$

PROPOSITION 2.20. — *Un projeté d'un langage rationnel est un langage rationnel.*

Voir [3], Proposition 1.95.

LEMME 2.21 (de l'étoile). — *Si un langage L est rationnel, alors il existe une constante $N > 0$ telle que pour tout mot $u_1u_2u_3 \in \Sigma^*$ avec $|u_2| > N$, il existe trois mots v_1, v_2 et v_3 avec $|v_2| > 0$ tels que l'on ait $u_2 = v_1v_2v_3$ et*

$$\textit{pour tout entier } n \in \mathbb{N}, \quad u_1v_1{v_2}^n v_3u_3 \in L.$$

(Ici, $|u|$ dénote la longueur du mot u)

3. Semi-groupe automatique et fortement automatique

Dans cette partie, nous allons définir ce que sont les structures automatique et fortement automatique, et nous allons voir comment déterminer la structure fortement automatique d'un sous-semi-groupe de type fini d'un groupe.

Dans toute la suite, Γ est un sous-semi-groupe d'un groupe G, et Σ est une partie génératrice finie de Γ. On notera e l'élément neutre du groupe G.

REMARQUE 3.1 (Laurent Bartholdi). — *Tous les résultats qui suivent se généralisent aux monoïdes simplifiables. Mais on se place dans un cadre moins général par soucis de clarté.*

3.1. Semi-groupe fortement automatique

DÉFINITION 3.2. — *On dit que le semi-groupe* Γ *est* fortement automatique *pour la partie génératrice* Σ *si l'ensemble des relations*

$$L^{\mathrm{rel}} := \{(u_1, v_1)\dots(u_n, v_n) \in (\Sigma \times (\Sigma \cup \{e\}))^* | u_1 \dots u_n = v_1 \dots v_n \text{ dans } \Gamma\}$$

est un langage rationnel. On dira qu'un semi-groupe est fortement automatique s'il existe une partie génératrice pour laquelle il est fortement automatique. On appelera automate des relations *du semi-groupe* Γ *l'automate minimal reconnaissant le langage* L^{rel}.

EXEMPLE 3.3. — *Le monoïde engendré par les trois transformations*

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3. \end{cases}$$

est fortement automatique : voir figure 12. Voir par exemple [6] *ou le théorème 4.2 pour un preuve.*

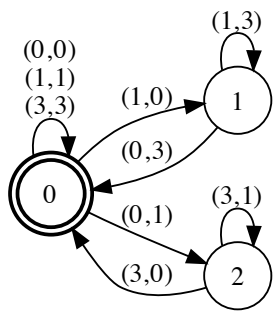


FIGURE 12. Automate des relations du monoïde de l'exemple 3.3

REMARQUE 3.4. — *Cette définition est valable pour n'importe quel semi-groupe* Γ *de type fini, et pas seulement pour les semi-groupes qui se plongent dans un groupe.*

Obtention de la structure fortement automatique d'un monoïde. — Dans ce paragraphe, nous allons voir comment obtenir la structure fortement automatique d'un sous-monoïde Γ d'un groupe.

REMARQUE 3.5. — *Un semi-groupe est fortement automatique si et seulement si le monoïde engendré (c'est-à-dire le semi-groupe auquel on ajoute l'élément neutre) l'est.*

DÉFINITION 3.6. — *On définit un automate* $\mathscr{A} = (\Sigma_{\mathscr{A}}, Q, T, I, F)$ *(éventuellement infini) de la façon suivante :*

1. $\Sigma_{\mathscr{A}} = \Sigma \times (\Sigma \cup \{e\})$,
2. $Q = \Gamma^{-1}\Gamma \subseteq G$,
3. $I = \{e\}$,
4. $F = \{e\}$,
5. T *est définit par :* $(p, (g, h), q) \in T$ *si et seulement si* $q = g^{-1}ph$,

où Γ *est un sous-monoïde d'un groupe, d'élément neutre* e*, et engendré par une partie finie* Σ *(qui contient éventuellement l'élément* e*).*

PROPOSITION 3.7. — *L'émondé de l'automate* $\mathscr{A}$ *est l'automate minimal* $\mathscr{A}^{\mathrm{rel}}$ *des relations du monoïde* Γ.

On considèrera cet automate $\mathscr{A}^{\mathrm{rel}}$ dans la suite, même s'il est infini.

REMARQUE 3.8. — *On peut généraliser ce résultat aux monoïdes simplifiables.*

Démonstration. — Montrons que l'automate $\mathscr{A}$ reconnait bien le langage L^{rel}. Si $(a_1, b_1) \dots (a_n, b_n)$ est un mot reconnu par l'automate, alors par définition on a

$$a_n^{-1} \dots a_1^{-1} e b_1 \dots b_n = e$$

dans G. Donc on a bien $a_1 \dots a_n = b_1 \dots b_n$ dans Γ. Réciproquement, la relation $a_1 \dots a_n = b_1 \dots b_n$ dans Γ donne un chemin

$$e \xrightarrow{(a_1,b_1)} a_1^{-1} b_1 \to \dots \xrightarrow{(a_n,b_n)} a_n^{-1} \dots a_1^{-1} b_1 \dots b_n = e$$

dans l'automate $\mathscr{A}$.

Montrons maintenant que l'automate émondé est minimal. D'après la proposition 2.13, il suffit de montrer qu'il est déterministe et de transposée déterministe. L'automate est clairement déterministe, et la transposée s'obtient en remplaçant l'ensemble des transitions par les $p \xrightarrow{(g,h)} q$ pour $q = gph^{-1}$, ce qui donne bien un automate déterministe. □

PROPRIÉTÉS 3.9. — *On a les propriétés :*

1. *Un groupe est fortement automatique si et seulement s'il est fini.*
2. *Un monoïde est libre (pour un système de générateurs donné) si et seulement si son automate des relations est trivial (c'est-à-dire réduit à un seul état).*
3. *Si un monoïde* Γ *est fortement automatique et simplifiable, et qu'il contient une relation entre deux éléments de longueurs distinctes, alors c'est un groupe fini.*
4. *Il y a unicité de la partie génératrice pour laquelle un semi-groupe ne contient pas de relation entre deux éléments de longueurs distinctes.*

De ces propriétés, on déduit qu'un semi-groupe possédant une partie génératrice pour laquelle il n'y a pas de relation entre deux éléments de longueurs distinctes est fortement automatique si et seulement si il l'est pour cette partie génératrice.

Preuve des propriétés. —

1. Si Γ est un groupe, alors l'automate $\mathcal{A}$ est déjà émondé et a pour ensemble de sommets Γ, d'où la propriété.
2. Si le semi-groupe Γ n'est pas libre pour la partie génératrice Σ, alors il existe une relation $a_1 \dots a_n = b_1 \dots b_n$ pour des éléments $a_i \in \Sigma$ et $b_i \in \Sigma \cup \{e\}$, avec $n \geq 1$ et $a_1 \neq b_1$. Le mot $(a_1, b_1) \dots (a_n, b_n)$ est reconnu par l'automate des relations, et donc il existe une arête de e à ${a_1}^{-1} b_1 \neq e$ dans l'automate des relations. Réciproquement, si l'automate des relations n'est pas trivial, alors il existe un chemin de e vers un état $g \neq e$, et de g vers e puisque l'automate est émondé. Le chemin de e vers e obtenu en concaténant ces deux chemins fournit alors une relation non triviale dans le semi-groupe Γ (puisque les relations triviales de Γ correspondent à des chemins qui ne passent que par l'état e dans l'automate des relations).
3. Supposons qu'il existe une relation $u = v$ dans le semi-groupe fortement automatique Γ, pour deux mots u et $v \in \Sigma^*$, avec u de longueur strictement supérieure à v : $|u| > |v|$. Considérons alors le mot $w_n \in \Sigma \times (\Sigma \cup \{e\})$ correspondant au couple (u^n, v^n). Celui-ci termine par au moins n fois une lettre de la forme (a, e) pour des lettres $a \in \Sigma$. On a la relation $u^n = v^n$ dans le semi-groupe Σ, et donc le mot w_n est reconnu par l'automate $\mathcal{A}^{\mathrm{rel}}$. En utilisant le lemme de l'étoile (voir 2.21), avec u_2 de la forme $(a_1, e) \dots (a_k, e)$, on obtient, pour un entier k assez grand (et donc pour un entier n assez grand), une relation de la forme

$$u_1 u_2^k u_3 = v_1 e^{\alpha k + \beta} = v_1 \text{ dans } \Gamma, \text{ pour tout entier } k \in \mathbb{N},$$

avec $\alpha > 0$, et u_2 de longueur α. On a donc $u_1 u_2^k u_3 = u_1 u_2^{k+1} u_3$, d'où $u_2 = e$ dans le semi-groupe Γ, en simplifiant à droite et à gauche. De ceci, on déduit l'existence d'un générateur $a \in \Sigma$ qui est inversible à droite dans Γ (i.e. $a_d^{-1} \in \Gamma$). Posons $a' \in \Sigma^*$ tel que $a' = a_d^{-1}$ dans le semi-groupe Γ. En considérant maintenant la relation $a^n (a')^n b^n = b^n$ dans le semi-groupe Γ, pour un générateur $b \in \Sigma$ quelconque, le lemme de l'étoile nous donne, en prenant n assez grand, l'égalité $a^n (a')^n b^{n+kp} = b^n$ dans le semi-groupe Γ, pour un entier $p > 0$, et pour tout entier $k \in \mathbb{N}$. On obtient alors $b^{kp} = e$ en simplifiant, et donc le générateur b est inversible (à gauche et à droite). Tous les générateurs du semi-groupe étant ainsi inversibles, on en déduit que le semi-groupe Γ est un groupe. Par la première propriété, c'est un groupe fini.

4. Supposons que l'on ait deux partie génératrices Σ et Σ' du même semi-groupe Γ. Alors un générateur $a \in \Sigma$ s'écrit comme produit d'éléments de Σ' qui eux-même s'écrivent chacun comme produit d'éléments de Σ. Mais la longueur en la partie génératrice Σ du dernier produit obtenu doit être 1 puisque sinon on obtiendrait une relation entre des éléments de longueurs distinctes. On en déduit que l'on a $a \in \Sigma'$. Ainsi, on a l'inclusion $\Sigma \subseteq \Sigma'$, et par symétrie $\Sigma = \Sigma'$. □

EXEMPLE 3.10. — *Le sous-semi-groupe $\mathbb{Z}_{\geq 1}$ est fortement automatique, tandis que le sous-semi-groupe $\mathbb{Z}_{\geq 2}$ ne l'est pas.*

EXEMPLE 3.11. — *Le sous-semi-groupe de $SL(2,\mathbb{Z})$ engendré par les trois matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$ est fortement automatique. Cela peut se démontrer en utilisant l'isomorphisme $PSL(2,\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, où $*$ dénote le produit libre des deux groupes cycliques. Les générateurs s'expriment sous la forme : abab, ababa et baba où $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 2 et $b = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ est d'ordre 3 dans $PSL(2,\mathbb{Z})$.*

Voir la partie 5 pour plus d'exemples.

REMARQUE 3.12. — *Déterminer si une partie finie d'un groupe engendre un semi-groupe libre (et donc déterminer si l'automate des relations correspondant est trivial) est décidable pour les sous-semi-groupes de type fini de $GL(2,\mathbb{Z})$ mais est indécidable pour les sous-semi-groupes de $SL(3,\mathbb{N})$ de type ≥ 13. C'est une question ouverte pour les sous-semi-groupes de type fini de $SL(2,\mathbb{Q})$. Voir* [4] *pour plus de détails. Ainsi, il ne peut pas exister d'algorithme pour déterminer la structure fortement automatique des sous-semi-groupes de type fini de $SL(3,\mathbb{N})$.*

QUESTION . — *Le problème de déterminer si un sous-semi-groupe de type fini de $PSL(2,\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ est fortement automatique est-il décidable ?*

(Ici, $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ est le produit libre des deux groupes $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.)

3.2. Monoïde rationnel. — Nous faisons ici le lien entre la notion de semi-groupe fortement automatique, et celle de monoïde rationnel. Dans son article [9], Sakarovitch introduit la notion de monoïde rationnel, que l'on peut définir de la façon suivante (voir [1] pour d'autres caractérisations) :

DÉFINITION 3.13. — *On dit qu'un monoïde M est* rationnel *s'il existe un ensemble fini Σ de générateurs, une partie $L^{\mathrm{red}} \subseteq \Sigma^*$ et un langage rationnel $L^{\mathrm{rat}} \subseteq (\Sigma \times \{0,1\})^*$ tels que*

- L^{red} *est un système de mots réduits. C'est-à-dire que pour tout élément* γ *de* M*, il existe un unique mot en les générateurs* Σ *qui est dans* L^{red} *et qui est égal à* γ *dans le monoïde* M*.*
- *Pour tout mot* $u \in \Sigma^*$*, il existe un mot* $w \in L^{\mathrm{rat}}$ *tel que* $p_0(w) = u$*.*
- *Pour tout mot* $w \in L^{\mathrm{rat}}$*,* $p_1(w)$ *est un mot réduit équivalent à* $p_0(w)$ *(c'est-à-dire que les deux mots sont égaux dans le monoïde* M*).*

où $p_0 : (\Sigma \times \{0,1\})^* \to \Sigma^*$ *et* $p_1 : (\Sigma \times \{0,1\})^* \to \Sigma^*$ *sont les morphismes naturels tels que* $p_i(\Sigma \times \{j\}) = \begin{cases} \{\epsilon\} & \text{si } i \neq j, \\ \Sigma \times \{j\} & \text{si } i = j. \end{cases}$

Reprenons l'exemple de l'introduction :

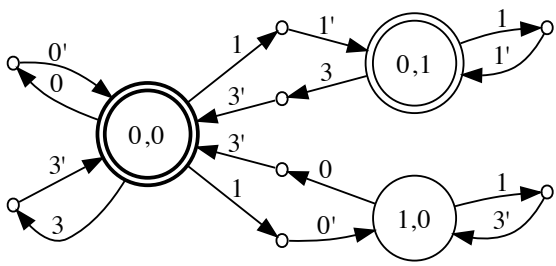
EXEMPLE 3.14. — *Le monoïde engendré par les trois applications*

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3. \end{cases}$$

est rationnel, pour l'alphabet $\Sigma = \{0,1,3\}$*, l'ensemble de mots réduits*

$$\begin{aligned} L^{\mathrm{red}} &= \{\textit{mots de } \Sigma^* \textit{ ne contenant pas le mot } 10 \textit{ comme sous-mot }\} \\ &= (0|3|11^*3)^*, \end{aligned}$$

et le langage $L^{\mathrm{rat}} \subseteq (\Sigma \times \{0,1\})^*$ *reconnu par l'automate* $\mathcal{A}_{L^{\mathrm{rat}}}$ *suivant :*



où l'on a remplacé l'alphabet $\Sigma \times \{0\}$ *par* $\{0,1,3\}$ *et l'alphabet* $\Sigma \times \{1\}$ *par* $\{0',1',3'\}$ *pour alléger les notations.*

La notion de monoïde rationnel est assez proche de celle de monoïde fortement automatique comme le montre les résultats suivants :

PROPOSITION 3.15. — *Si un monoïde* M *est fortement automatique, alors il est rationnel.*

Voici une réciproque :

PROPOSITION 3.16. — *Soit M un monoïde engendré par une partie finie Σ telle qu'il n'y ait pas d'égalité dans le monoïde entre deux mots en Σ de mêmes longueurs. Alors le monoïde M est rationnel si et seulement si il est fortement automatique.*

Et voici un exemple qui montre que les deux notions diffèrent :

EXEMPLE 3.17. — *Le monoïde de présentation $< 0, 1 | 010 = 11 >$ est rationnel (voir figure 13) mais n'est pas fortement automatique (par 3.9, puisqu'il est simplifiable et infini).*

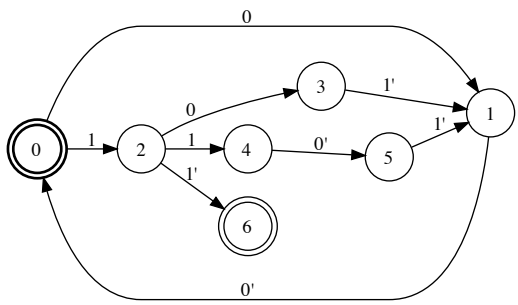


FIGURE 13. Automate $\mathcal{A}_{L^{\mathrm{rat}}}$ de l'exemple 3.17

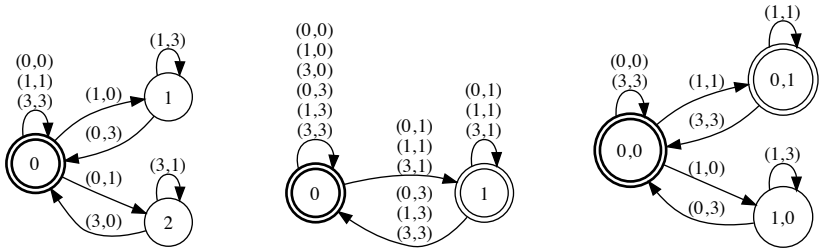
Preuve de la proposition 3.15. — Soit le langage rationnel

$$L := L^{\mathrm{rel}} \cap \left(\Sigma^* \times L^{\mathrm{red}} e^* \cup \Sigma^* e^* \times L^{\mathrm{red}}\right),$$

où L^{red} est le langage rationnel des mots réduits correspondant aux mots minimaux dans l'ordre lexicographique. Soit $\mathcal{A}$ un automate déterministe et émondé reconnaissant le langage L. On modifie l'automate en remplaçant chaque transition

- $p \xrightarrow{(a,e)} q$ par $p \xrightarrow{(a,0)} q$,
- $p \xrightarrow{(e,a)} q$ par $p \xrightarrow{(a,1)} q$,
- $p \xrightarrow{(a,b)} q$ par $p \xrightarrow{(a,0)} p' \xrightarrow{(b,1)} q$, où p' est un nouvel état,

pour toutes lettres a et b dans Σ. On vérifie alors que le monoïde est rationnel avec l'ensemble de générateur Σ, les mots réduits L^{red} et le langage L^{rat} reconnu par l'automate que l'on vient de construire. □



Automate des relations | Automate reconnaissant le langage $\Sigma^* \times L^{\text{red}}$ | Automate reconnaissant l'intersection L

FIGURE 14. Construction d'un automate reconnaissant le langage L de la preuve ci-dessus pour l'exemple 3.14

Preuve de la proposition 3.16. — Montrons qu'un monoïde rationnel qui satisfait l'hypothèse est fortement automatique. Soit L^{rat} le langage de la définition 3.13, et soit $\mathscr{A}_{L^{\text{rat}}}$ un automate déterministe et émondé qui reconnait le langage L^{rat}.

LEMME 3.18. — *Les cycles de l'automate $\mathscr{A}_{L^{\text{rat}}}$ sont étiquetés par des mots contenant chacun autant de lettre de l'alphabet $\Sigma\times\{0\}$ que de l'alphabet $\Sigma\times\{1\}$.*

Démonstration. — Supposons qu'il existe un cycle dans l'automate $\mathscr{A}_{L^{\text{rat}}}$ étiqueté par un mot $u \in (\Sigma \times \{0\} \sqcup \Sigma \times \{1\})^*$, avec par exemple $|p_0(u)| < |p_1(u)|$. L'automate $\mathscr{A}_{L^{\text{rat}}}$ étant émondé, il existe un mot $w \in L^{\text{rat}}$ qui parcours ce cycle. Plus précisément, on peut écrire $w = xuy$, tel qu'il existe des états p, q et r tels que $p \xrightarrow{x} q \xrightarrow{u} q \xrightarrow{y} r$ et avec $p \in I$ et $r \in F$. Le mot xy est alors aussi reconnu par l'automate, et on a

$$|p_0(xuy)|-|p_1(xuy)| = |p_0(xy)|-|p_1(xy)|+|p_0(u)|-|p_1(u)| < |p_0(xy)|-|p_1(xy)|\,.$$

Cela est impossible, puisque l'hypothèse que le monoïde ne contient que des relations entre des mots de même longueur entraîne que pour tout mot v reconnu par l'automate $\mathscr{A}_{L^{\text{rat}}}$, on a $|p_0(v)| - |p_1(v)| = 0$. On a donc bien montré le résultat par l'absurde. □

Il existe donc une borne M sur les différences $||p_0(u)| - |p_1(u)||$ sur tous les mots u qui sont préfixes d'un mot du langage L^{rat}.

Construisons alors un automate $\mathscr{A} = (\Sigma_{\mathscr{A}}, Q, T, I, F)$ en posant :

- $\Sigma_{\mathscr{A}} := (\Sigma \cup \{e\})^2$,
- $Q := Q_{\mathscr{A}_{L^{\text{rat}}}} \quad \sqcup \quad Q_{\mathscr{A}_{L^{\text{rat}}}} \times \bigcup_{i=1}^{M} \Sigma^i \times \{0\} \quad \sqcup \quad Q_{\mathscr{A}_{L^{\text{rat}}}} \times \bigcup_{i=1}^{M} \Sigma^i \times \{1\}$,
- $I := I_{\mathscr{A}_{L^{\text{rat}}}}$,

– $F := F_{\mathcal{A}_{L^{\mathrm{rat}}}}$,
– T est le plus petit ensemble tel que
  • Si $p \xrightarrow{(a,0)} q$ dans $\mathcal{A}_{L^{\mathrm{rat}}}$, alors pour tout $u \in \bigcup_{i=0}^{M-1} \Sigma^i$,
    * $(p,u,0) \xrightarrow{\epsilon} (q,ua,0)$ dans $\mathcal{A}$,
    * $(p,ub,1) \xrightarrow{(a,b)} (q,u,1)$ dans $\mathcal{A}$,
  avec la convention que $(p,\epsilon,0) = p$ et $(q,\epsilon,1) = q$.
  • Si $p \xrightarrow{(a,1)} q$ dans $\mathcal{A}_{L^{\mathrm{rat}}}$, alors pour tout $u \in \bigcup_{i=0}^{M-1} \Sigma^i$,
    * $(p,u,1) \xrightarrow{\epsilon} (q,ua,1)$ dans $\mathcal{A}$,
    * $(p,ub,0) \xrightarrow{(b,a)} (q,u,0)$ dans $\mathcal{A}$,
  avec la convention que $(p,\epsilon,1) = p$ et $(q,\epsilon,0) = q$.

Les « transitions » étiquetées par ϵ s'appellent des ϵ-transitions. On peut démontrer qu'un automate avec ϵ-transition est équivalent à un automate déterministe sans ϵ-transition (voir [3] pour plus de détails). Ainsi, le langage L de l'automate $\mathcal{A}$ est rationnel.

L'automate $\mathcal{A}$ ci-dessus consiste à « synchroniser » l'automate $\mathcal{A}_{L^{\mathrm{rat}}}$, en stoquant en mémoire (grâce à de nouveaux états) le nombre fini de lettres qui font qu'un des deux mots, l'un sur l'alphabet $\Sigma \times \{0\}$ et l'autre sur l'alphabet $\Sigma \times \{1\}$, est plus long que l'autre. À un chemin dans $\mathcal{A}_{L^{\mathrm{rat}}}$, on fait donc correspondre un chemin dans l'automate $\mathcal{A}$ étiqueté par les mêmes lettres regroupées par couples (avec à gauche les lettres de l'alphabet $\Sigma \times \{0\}$ et à droite celles de $\Sigma \times \{1\}$), et avec les lettres qui restent qui sont « mémorisée » par l'état dans lequel on aboutit.

LEMME 3.19. — *On a $L = L^{\mathrm{rel}} \cap \left(\Sigma^* \times L^{\mathrm{red}}\right)$, où L est le langage de l'automate $\mathcal{A}$ défini ci-dessus.*

Démonstration. — Il y a correspondance entre un chemin dans l'automate $\mathcal{A}_{L^{\mathrm{rat}}}$ et dans l'automate $\mathcal{A}$, par la construction ci-dessus. On vérifie que l'on a un chemin $p \xrightarrow{u} q$ dans l'automate $\mathcal{A}_{L^{\mathrm{rat}}}$, si et seulement si le chemin correspondant $p \xrightarrow{(x,y)} (q,z,\alpha)$ dans l'automate $\mathcal{A}$ est tel que $p_0(u) = \begin{cases} xz \text{ si } \alpha = 0 \\ x \quad \text{si } \alpha = 1 \end{cases}$ et $p_1(u) = \begin{cases} y \quad \text{si } \alpha = 0 \\ yz \text{ si } \alpha = 1 \end{cases}$. Ainsi, un mot $(x,y) = (x_1,y_1)\dots(x_n,y_n)$ est reconnu par l'automate $\mathcal{A}$ si et seulement si il lui correspond un mot $u \in L^{\mathrm{rat}}$ tel que $x = p_0(u)$ et $y = p_1(u)$. □

La preuve de la proposition 3.16 est alors une conséquence du lemme suivant. □

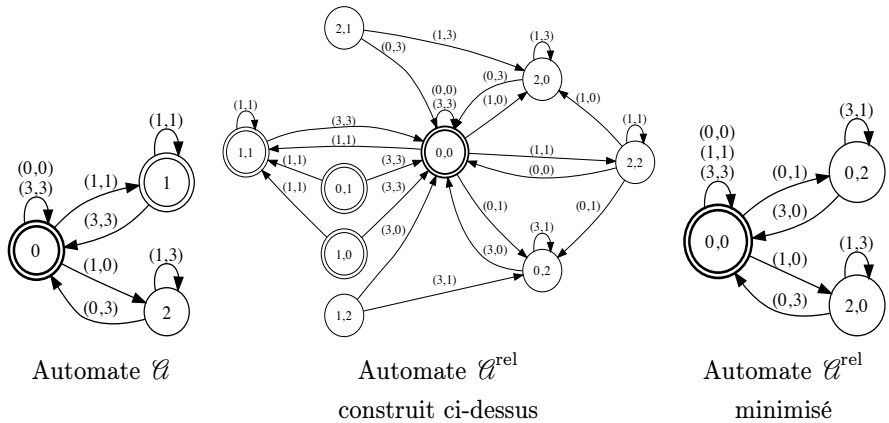


FIGURE 15. Construction d'un automate reconnaissant le langage L^{rel} à partir d'un automate reconnaissant le langage $L = L^{\mathrm{rel}} \cap \left(\Sigma^* \times L^{\mathrm{red}}\right)$ pour l'exemple 3.14

LEMME 3.20. — *Si le langage $L = L^{\mathrm{rel}} \cap \left(\Sigma^* \times L^{\mathrm{red}}\right)$ est rationnel, alors le langage L^{rel} l'est aussi.*

Démonstration. — Soit $\mathbb{L} := L \times L \subseteq (\Sigma^2 \times \Sigma^2)^*$ et $\mathbb{L}' := \mathbb{L} \cap \{(a,c,b,c) | a,b,c \in \Sigma\}$. Montrons que l'on a alors $L^{\mathrm{rel}} = p_{13}(\mathbb{L}')$ où p_{13} est la projection sur les 1ère et 3e coordonnées.

Par définition, on a

$$(a,b) \in p_{13}(\mathbb{L}') \quad \Longleftrightarrow \quad \exists c \in L^{\mathrm{red}}, (a,c) \in L^{\mathrm{rel}} \text{ et } (b,c) \in L^{\mathrm{rel}}.$$

On a l'implication $(a,c) \in L^{\mathrm{rel}}$ et $(b,c) \in L^{\mathrm{rel}} \Rightarrow (a,b) \in L^{\mathrm{rel}}$ par définition de L^{rel}, et l'autre implication $(a,b) \in L^{\mathrm{rel}} \Rightarrow \exists c \in L^{\mathrm{red}}, (a,c) \in L^{\mathrm{rel}}$ et $(b,c) \in L^{\mathrm{rel}}$ découle de la définition de L^{red}. □

3.3. Semi-groupe automatique. — La structure fortement automatique est utile pour déterminer facilement si deux mots représentent le même élément du semi-groupe, et nous allons voir qu'elle permet également d'obtenir d'autres informations sur le semi-groupe puisqu'elle impliquera la structure automatique usuelle :

DÉFINITION 3.21. — *On dit que le semi-groupe Γ est* automatique *s'il existe une partie génératrice Σ, un automate $\mathscr{A}^{\mathrm{red}}$ appelé* automate des mots réduits *et une famille d'automates $(\mathscr{A}^g)_{g \in \Sigma}$ appelés* automates de multiplication *vérifiants les propriétés :*

1. *$\mathscr{A}^{\mathrm{red}}$ a pour alphabet Σ,*

2. *Le langage $L_{\mathscr{A}^{\mathrm{red}}}$ est un ensemble de mots réduits. C'est-à-dire que l'on a :*

   pour tout $\gamma \in \Gamma$, il existe un unique $u \in L_{\mathscr{A}^{\mathrm{red}}}$ tel que $\gamma = u$ dans Γ.

   Autrement dit, l'application de Σ^* dans Γ induit une bijection de $L_{\mathscr{A}^{\mathrm{red}}}$ dans Γ : on peut identifier un mot réduit à un élément de Γ.
3. *Pour tout $g \in \Sigma$, $\mathscr{A}^g$ a pour alphabet $(\Sigma \cup \{e\}) \times (\Sigma \cup \{e\})$,*
4. *Pour tout $g \in \Sigma$, l'automate $\mathscr{A}^g$ reconnait si un mot réduit de Γ s'obtient à partir d'un autre par multiplication à droite par g. Plus précisément, le langage $L_{\mathscr{A}^g}$ est l'ensemble des mots $(u_1, v_1) \dots (u_n, v_n)$ vérifiant :*

$$(u_1, v_1) \dots (u_n, v_n) \in (L_{\mathscr{A}^{\mathrm{red}}} g \times L_{\mathscr{A}^{\mathrm{red}}} e^*) \cup (L_{\mathscr{A}^{\mathrm{red}}} g e^* \times L_{\mathscr{A}^{\mathrm{red}}}), \tag{1}$$

$$u_1 \dots u_n = v_1 \dots v_n \text{ dans } \Gamma. \tag{2}$$

Remarque 3.22. — *Il existe des variantes de la notion de structure automatique, qui autorise par exemple une notion de mots réduits un peu plus souple, ou encore qui reconnait si un mot réduit de Γ s'obtient à partir d'un autre par multiplication à droite par g d'une façon différente. Voir* [2] *pour plus de détails.*

Exemple 3.23. — *Les semi-groupes suivants sont automatiques :*

- *$\mathbb{Z}$: voir figure 16.*
- *Le semi-groupe donné en introduction : voir figures 17, 18, 19 et 20.*
- *Les groupes hyperboliques.*

Il y a de nombreux autres exemples de groupes automatiques. Voir par exemple [5].

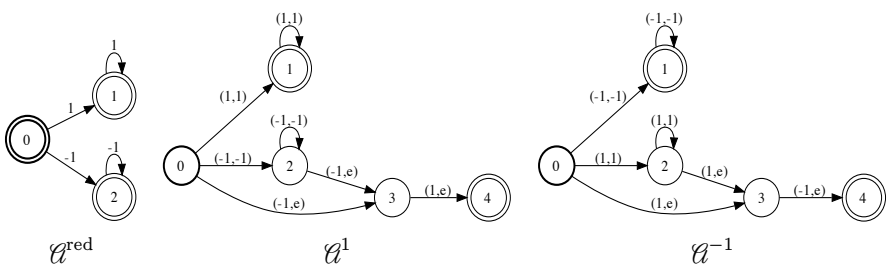


Figure 16. Structure automatique de $\Gamma = \mathbb{Z}$ avec $\Sigma = \{-1, 1\}$

La structure automatique d'un semi-groupe permet de manipuler celui-ci grâce à un système de mots réduits. Cela permet par exemple d'effectuer des calculs dans le semi-groupe sur ordinateur. Mais voici aussi un résultat donnant des informations sur le semi-groupe à partir de la structure automatique :

PROPOSITION 3.24. — *Si Γ est automatique, alors le nombre c_n d'éléments de Γ de longueur n vérifie*

$$c_n = P(n)\alpha^n(1 + O_{n\to\infty}(e^{-\epsilon n}))$$

où P est un polynôme, $\epsilon > 0$ est un réel, et $1 \leq \alpha \leq \#\Sigma$ est un réel.

Plus précisément, c_n s'obtient comme la somme de coefficients de la puissance $n^{ième}$ de la matrice d'adjacence du graphe de l'automate $\mathscr{A}^{\mathrm{red}}$.

Démonstration. — Le nombre c_n cherché est le nombre de chemins de longueur n de l'automate $\mathscr{A}^{\mathrm{red}}$, partant de l'état initial et aboutissant à un état final. Ceci est donné par les puissances de la matrice d'adjacence du graphe. Si l'automate est supposé émondé, le théorème de Perron-Frobenius nous donne l'existence d'une plus grande valeur propre $\alpha > 0$, pour laquelle on a l'asymptotique annoncée. □

EXEMPLE 3.25. — *Pour $\Gamma = \mathbb{Z}$ et $\Sigma = \{-1, 1\}$ (voir figure 16), la matrice d'adjacence du graphe de l'automate $\mathscr{A}^{\mathrm{red}}$ est*

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

qui est idempotente. Le nombre c_n d'éléments de Γ de longueur n est donc $c_0 = 1$ pour $n = 0$ et $c_n = 2$ pour $n > 0$ (il s'agit en effet des éléments n et $-n$).

Les 4 figures qui suivent donnent une structure automatique complète de l'exemple de l'introduction :

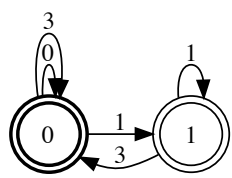


FIGURE 17

Automate $\mathscr{A}^{\mathrm{red}}$ du monoïde engendré par les trois applications

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3, \end{cases}$$

pour l'ordre lexicographique (avec $0 < 1 < 3$).

On voit que les mots réduits sont ici les mots ne contenant pas le sous-mot 10.

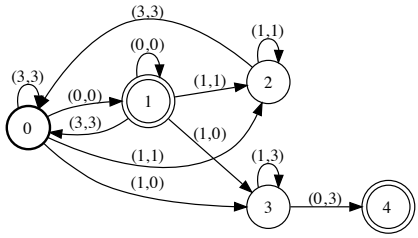


FIGURE 18

Automate $\mathscr{A}^0$ du monoïde engendré par les trois applications

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3. \end{cases}$$

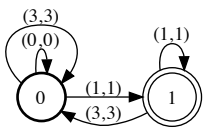


FIGURE 19

Automate $\mathscr{A}^1$ du monoïde engendré par les trois applications

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3. \end{cases}$$

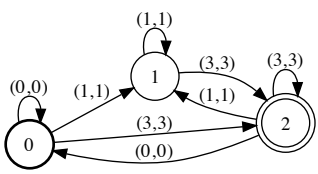


FIGURE 20

Automate $\mathscr{A}^3$ du monoïde engendré par les trois applications

$$\begin{cases} 0 : x \mapsto x/3, \\ 1 : x \mapsto x/3 + 1, \\ 3 : x \mapsto x/3 + 3. \end{cases}$$

On voit sur la figure 19 que le langage de $\mathscr{A}_1$ est formé des couples $(u1, u1)$ pour les mots u réduits. Sur la figure 20, on voit de même que le langage de $\mathscr{A}_3$ est formé des couples $(u3, u3)$ pour les mots u réduits. L'automate de la figure 18 est plus compliqué puisque le mot $u0$ n'est pas réduit quand le mot réduit u termine par un 1 : son langage est l'ensemble des couples $(u1^n0, u03^n)$ pour les mots réduits u et les entiers $n \in \mathbb{N}$.

3.4. Fortement automatique implique automatique. — Voici un lien entre la structure fortement automatique et automatique :

PROPOSITION 3.26. — *Si le monoïde* Γ *est fortement automatique, alors il est automatique.*

Démonstration. — Supposons que le semi-groupe Γ soit fortement automatique : il existe donc un automate des relations $\mathscr{A}^{\mathrm{rel}}$, qui reconnait un langage rationnel L^{rel}. Par le point 1 des propriétés 3.9, le semi-groupe contient une relation entre des éléments de longueurs distinctes si et seulement si c'est un groupe fini. Mais il est facile de voir qu'un groupe fini est automatique. Ainsi, on supposera dans la suite de la preuve que les relations sont toujours entre des éléments de même longueur. On a donc l'inclusion de l'ensemble des relations L^{rel} dans $(\Sigma \times \Sigma)^*$.

3.4.0.1. *Construction de l'automate des mots réduits.* — Considérons alors le langage rationnel

$$L := L^{\mathrm{lex}} \cap L^{\mathrm{rel}},$$

où L^{lex} est le langage de l'automate de la figure 9, en ayant muni l'alphabet Σ d'un ordre total. Posons alors

$$L^{\mathrm{nonred}} := p_2(L),$$

le projecté du langage L suivant la deuxième coordonnée. Par la proposition 2.20, c'est un langage rationnel. Alors L^{nonred} est l'ensemble des mots de Σ^* qui sont non réduits pour l'ordre lexicographique. En effet, le langage L est l'ensemble des couples de mots équivalents (u, v) de Σ^* tels que u est strictement inférieur à v pour l'ordre lexicographique. Ainsi, un mot v est dans le langage L^{nonred} si et seulement s'il existe un mot u équivalent et strictement inférieur dans l'ordre lexicographique. En posant

$$L^{\mathrm{red}} := \Sigma^* \backslash L^{\mathrm{nonred}},$$

le langage L^{red} est donc un ensemble de mots réduits, et il est rationnel.

Ainsi, on a bien démontré l'existence de l'automate des mots réduits $\mathscr{A}^{\mathrm{red}}$.

3.4.0.2. *Construction des automates de multiplication.* — Le paragraphe précédent a montré que le langage L^{red} des mots réduits est rationnel. Pour $g \in \Sigma$, considérons alors le langage rationnel

$$L^g := (L^{\mathrm{red}} g \times L^{\mathrm{red}}) \cap L^{\mathrm{rel}}.$$

C'est bien un langage rationnel par la proposition 2.18. Pour obtenir un automate de multiplication $\mathscr{C}^g$, il suffit de considérer un automate $\mathscr{C}^g$ reconnaissant le langage L^g.

Ceci termine la preuve de la proposition 3.26. □

3.5. Recherche du mot réduit. — Comment trouver le mot réduit correspondant à un mot donné ? La structure automatique permet de faire cela :

PROPOSITION 3.27. — *Si le semi-groupe est automatique, alors il existe un algorithme quadratique qui prend en entrée un mot et rend le mot réduit correspondant.*

Démonstration. — Voir [5]. □

Ceci permet en particulier de résoudre le problème des mots (i.e. déterminer si deux mots donnés sont équivalents) en temps quadratique :

COROLLAIRE 3.28. — *Si le semi-groupe est automatique, il existe un algorithme prenant en entrée deux mots et répondant en temps quadratique si les deux mots sont équivalents ou non.*

Lorsque le semi-groupe est fortement automatique, le problème des mots se résoud en temps linéaire et avec une mémoire constante puisqu'il est résolu par un automate. Mais on peut aussi trouver le mot réduit correspondant à un mot donné rapidement :

PROPOSITION 3.29. — *Si le semi-groupe est fortement automatique, alors il existe un algorithme linéaire prenant en entrée un mot et rendant le mot réduit correspondant.*

Démonstration. — Définissons le langage

$$L := \{(a_1, b_1) \dots (a_n, b_n) \in L^{\mathrm{rel}} | b_1 \dots b_n \in L^{\mathrm{red}} e^*\} = (\Sigma^* \times L^{\mathrm{red}} e^*) \cap L^{\mathrm{rel}}.$$

Alors le langage L est rationnel.

Soit $\mathscr{C} = (\Sigma \times (\Sigma \cup \{e\}), Q, T, I, F)$ un automate déterministe reconnaissant le langage L. Définissons alors l'automate $\mathscr{C}' = (\Sigma, Q', T', I', F')$ par :

- $Q' := \mathscr{P}(Q)$ (l'ensemble des parties de Q),
- $I' := \{I\}$,
- $F' := \{P \in \mathscr{P}(Q) | P \cap F \neq \varnothing\}$,

– T' est défini par

$$(A, a, B) \in T' \text{ si et seulement si}$$

$$B = \{q \in Q | \text{Il existe } b \in (\Sigma \cup \{e\}) \text{ et } p \in A \text{ tels que } (p, (a, b), q) \in T\}.$$

L'automate $\mathcal{A}'$ est clairement déterministe, et il reconnait le langage Σ^*, puisque pour tout mot $u \in \Sigma^*$, il existe un mot réduit $v \in \Sigma^*$ tel que l'on ait la relation $u = v$ dans le semi-groupe Γ, ce qui donne un mot (u, ve^k) reconnu par l'automate $\mathcal{A}$ (en supposant que les mots réduits sont de longueur minimale).

Voici maintenant un algorithme permettant de trouver le mot réduit correspondant à un mot $u \in \Sigma^*$. Considérons le chemin

$$A_0 \xrightarrow{u_1} A_1 \to \ldots \xrightarrow{u_n} A_n$$

dans l'automate $\mathcal{A}'$ étiqueté par le mot $u = u_1 \ldots u_n$. Choisissons alors un état final $q_n \in A_n$ de l'automate $\mathcal{A}$. Par définition, il existe alors une lettre $v_n \in (\Sigma \cup \{e\})$ et un état $q_{n-1} \in A_{n-1}$ tels que l'on ait la transition $q_{n-1} \xrightarrow{(u_n, v_n)} q_n$ dans l'automate $\mathcal{A}$. Et on peut trouver la lettre v_n et l'état q_{n-1} en temps constant. On peut alors continuer : on trouve une lettre $v_{n-1} \in (\Sigma \cup \{e\})$ et un état $q_{n-2} \in A_{n-2}$ tels que l'on ait la transition $q_{n-2} \xrightarrow{(u_{n-1}, v_{n-1})} q_{n-1}$ dans l'automate $\mathcal{A}$, et ainsi de suite. On obtient finalement un chemin $q_0 \xrightarrow{(u_0, v_0)} q_1 \to \ldots \xrightarrow{(u_n, v_n)} q_n$ dans l'automate $\mathcal{A}$. L'état q_0 est un état initial de l'automate $\mathcal{A}$ puisque l'on a $q_0 \in A_0 \in I' = \{I\}$. On obtient donc un mot $v_1 \ldots v_n \in (\Sigma \cup \{e\})^*$ tel que le mot $(u_1, v_1) \ldots (u_n, v_n)$ est dans le langage L. Le mot $v = v_1 \ldots v_n$ est donc dans le langage $L^{\text{red}} e^*$, et on a la relation $u_1 \ldots u_n = v_1 \ldots v_n$ dans le semi-groupe Γ. Ainsi, on obtient le mot réduit correspondant au mot u en éliminant les lettres e à la fin du mot v. Et tout ce calcul s'effectue en temps linéaire. □

4. Semi-groupes correspondant aux développements β-adique

Soit k un corps. Dans cette partie, on s'intéresse au semi-groupe Γ engendré par les transformations affines

$$x \mapsto \beta x + t$$

pout $t \in A \subset k$, où A est une partie finie de k, et β est un élément de k.

REMARQUE 4.1. — *Si le corps k est de caractéristique 0, alors on peut supposer que l'on a $k = \mathbb{C}$.*

Ce semi-groupe correspond au développement en base β, en utilisant l'ensemble de chiffres A. Par exemple, l'exemple donné en introduction correspond au développement en base 3 en utilisant l'ensemble de chiffres $\{0, 1, 3\}$.

Nous donnons un critère de forte automaticité pour ces semi-groupes.

4.1. Forte automaticité. — Cette sous-section est consacrée à la preuve du théorème suivant qui donne la forte automaticité de la plupart des semi-groupes de développement en base β.

THÉORÈME 4.2. — *Le semi-groupe* Γ *est fortement automatique, sauf éventuellement dans le cas où le corps* k *est de caractéristique nulle, et que le nombre complexe* β *est algébrique, avec un conjugué de module 1.*

Preuve du théorème 4.2. — Commençons par le cas où β est une racine de l'unité. Par hypothèse, le corps k est alors de caractéristique finie. Dans ce cas, le semi-groupe Γ est un groupe fini (et est donc fortement automatique par le point 1 des propriétés 3.9). En effet, tous les générateurs sont d'ordre fini donc c'est un groupe, et il est fini puisque toutes les applications de Γ sont de la forme $x \mapsto \beta^k x + t$ avec $1 \leq k \leq n$ où n est l'ordre de β et t dans le sous-$\mathbb{F}_p$-espace vectoriel de dimension finie de k engendré par $\cup_{k=1}^{n} \beta^k A$.

Supposons maintenant que β ne soit pas une racine de l'unité. Par les propriétés 3.9, le semi-groupe est automatique si et seulement si il l'est pour la partie génératrice considérée ici, puisque les relations du semi-groupe Γ sont entre des éléments de même longueur. C'est-à-dire que si l'on a une égalité $a_1 \dots a_n = b_1 \dots b_n$ dans Γ pour deux mots $a_1 \dots a_n \in \Sigma^*$ et $b_1 \dots b_n \in (\Sigma \cup \{e\})^*$, alors on a $b_1 \dots b_n \in \Sigma^*$. Ainsi, on peut considérer l'automate des relations $\mathscr{A}^{\mathrm{rel}}$ (à priori infini) sur l'alphabet $\Sigma \times \Sigma$ donné par la proposition 3.7, et on va montrer qu'il est fini (i.e. qu'il a un nombre fini d'états). On peut aussi supposer que le semi-groupe Γ est un monoïde quitte à lui ajouter un élément neutre (ce qui ne change pas le fait qu'il soit fortement automatique).

Comme il n'y a pas d'égalité dans le semi-groupe entre deux mots de longueur différentes, on est ramené à ce que les états de l'automates soient tous de la forme $x \mapsto x + t$ pour $t \in k$. Ainsi, quitte à remplacer Γ par son inverse (ce qui ne change pas le fait qu'il soit fortement automatique), l'automate $\mathscr{A}^{\mathrm{rel}}$ est donc l'émondé de l'automate $\mathscr{A} = (\Sigma_{\mathscr{A}}, Q_{\mathscr{A}}, T_{\mathscr{A}}, I_{\mathscr{A}}, F_{\mathscr{A}})$ définit par :

1. $\Sigma_{\mathscr{A}} = \Sigma \times \Sigma$,
2. $Q_{\mathscr{A}} = k$,
3. $I_{\mathscr{A}} = \{0\}$,
4. $F_{\mathscr{A}} = \{0\}$,
5. $T_{\mathscr{A}} \subseteq Q_{\mathscr{A}} \times \Sigma_{\mathscr{A}} \times Q_{\mathscr{A}}$ est définit par :

$$(p, (g, h), q) \in T_{\mathscr{A}} \text{ si et seulement si } q = \beta p + g - h.$$

REMARQUE 4.3. — *J'aurait pu considérer l'automate* $\mathscr{A}$ *qui correspond directement à celui du semi-groupe* Γ *et non pas à son inverse. Cela aurait donné les transitions* $(p, (g, h), q) \in T_{\mathscr{A}} \Leftrightarrow q = (p - g + h)/\beta$. *Mais la formule donnant les transitions de l'automate* $\mathscr{A}$ *pour le semi-groupe inverse me semblait plus agréable.*

Le lemme suivant fournit une critère algébrique d'appartenance à l'ensemble des sommets de l'automate des relations $\mathscr{A}^{\mathrm{rel}}$:

LEMME 4.4. — *Un élément $x \in k$ est un état de l'automate des relations $\mathscr{A}^{\mathrm{rel}}$ (c'est-à-dire de l'émondé de l'automate $\mathscr{A}$) si et seulement si il existe deux polynômes $P, Q \in (A-A)[X]$ à coefficients dans $A-A$ tels que l'on ait $x = P(\beta) = \beta^{-1}Q(\beta^{-1})$.*

Preuve du lemme. — Un élément $x \in k$ est un état de l'automate des relations $\mathscr{A}^{\mathrm{rel}}$ si et seulement si il existe un chemin

$$0 \xrightarrow{(a_1,b_1)} \dots \xrightarrow{(a_n,b_n)} x \xrightarrow{(a'_k,b'_k)} \dots \xrightarrow{(a'_0,b'_0)} 0$$

dans l'automate $\mathscr{A}$, avec a_i, b_i, a'_i et $b'_i \in A$. On a alors $x = \sum_{i=0}^{n-1}(a_{n-i}-b_{n-i})\beta^i$ et $\beta^k x + \sum_{i=0}^{k-1}(a'_i - b'_i)\beta^i = 0$, d'où $x = P(\beta) = \beta^{-1}Q(\beta^{-1})$, avec

$$P(X) = \sum_{i=0}^{n-1}(a_{n-i} - b_{n-i})X^i \quad \text{et} \quad X^{-1}Q(X^{-1}) = \sum_{i=0}^{k-1}(a'_i - b'_i)X^{i-k}.$$

Et réciproquement, deux tels polynômes nous donnent un chemin de 0 à 0 passant par x. □

Notons $\mathbb{F}_p := \mathrm{Frac}(\mathbb{Z}/p\mathbb{Z})$ le corps de fractions de $\mathbb{Z}/p\mathbb{Z}$ où p est la caractéristique du corps k. On a ainsi $\mathbb{F}_0 = \mathbb{Q}$ si le corps k est de caractéristique nulle, et sinon $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est le corps fini à p éléments.

Considérons D le $\mathbb{F}_p(\beta)$-espace vectoriel engendré par la partie A, et soit C une base de cet espace vectoriel. Considérons la base duale $(c^*)_{c\in C}$ de C. Les formes linéaires $c^* : D \to \mathbb{F}_p(\beta)$ vérifient donc

$$\sum_{c\in C} c^* \cdot c = \mathrm{id}_D\,.$$

Pour chaque $c \in C$, considérons alors le semi-groupe Γ_c engendré par les transformations

$$x \mapsto \beta x + t, \text{ pour } t \in c^*(A).$$

On a alors le lemme :

LEMME 4.5. — *Le semi-groupe Γ est fortement automatique si et seulement si les semi-groupes Γ_c, $c \in C$, sont tous fortement automatiques.*

Démonstration. — On peut voir le semi-groupe Γ comme le produit

$$\Gamma = \prod_{c\in C} \Gamma_c,$$

et chaque semi-groupe Γ_c est fortement automatique si et seulement s' il l'est pour la partie génératrice naturelle, de même que pour Γ, d'après les propriétés 3.9. On conclut donc avec le lemme qui suit. □

LEMME 4.6. — *Soit Σ une partie d'un produit de semi-groupes $\Gamma_1 \times \Gamma_2$, et soient Σ_1 et Σ_2 les projetés de Σ sur chacun des semi-groupes du produit. Alors la partie Σ engendre un semi-groupe fortement automatique (relativement à la partie Σ) si et seulement si chacune des parties Σ_i engendre un semi-groupe fortement automatique (relativement à Σ_i), pour $i = 1$ et 2.*

Démonstration. — On a $L^{\mathrm{rel}}_{<\Sigma>^+} = \prod_{i=1}^{2} L^{\mathrm{rel}}_{<\Sigma_i>^+}$. □

Grâce au lemme 4.5, on se ramène à ce que l'on ait $A \subseteq \mathbb{F}_p(\beta)$. Quitte à multiplier la partie A par un élément du corps k (ce qui ne change pas le semi-groupe), on peut supposer que l'on a même $A \subseteq (\mathbb{Z}/p\mathbb{Z})[\beta]$. Ainsi, on peut supposer que l'ensemble des états de l'automate $\mathscr{A}$ est $(\mathbb{Z}/p\mathbb{Z})[\beta]$.
Il y a maintenant deux cas à considérer :

– Si β est transcendant : Dans ce cas, on a $(\mathbb{Z}/p\mathbb{Z})[\beta] \simeq (\mathbb{Z}/p\mathbb{Z})[X]$, et on peut voir A comme une partie de $(\mathbb{Z}/p\mathbb{Z})[X]$. Montrons alors que le degré des états de l'automate $\mathscr{A}^{\mathrm{rel}}$ (vus comme des polynômes) est strictement majoré par

$$\max_{P \in A-A} \deg P.$$

Soit Q un état non nul de l'automate $\mathscr{A}$ de degré $\deg Q \geq \max\limits_{P \in A-A} \deg P$. Pour toute transition $(Q, (U, V), R)$, on a alors

$$\deg R = \deg(XQ + U - V) = 1 + \deg Q \geq \max_{P \in A-A} \deg P,$$

car $\deg(U - V) \leq \max_{P \in A-A} \deg P < \deg(XQ)$. Ainsi, par récurrence, il ne peut pas exister de chemin de l'état Q vers l'état final 0, donc l'état Q n'est pas dans l'automate émondé $\mathscr{A}^{\mathrm{rel}}$.

Si le corps k est de caractéristique non nulle, cela prouve donc que l'ensemble des états de l'automate $\mathscr{A}^{\mathrm{rel}}$ est fini.

Supposons maintenant que le corps k soit de caractéristique nulle. Montrons alors que les polynômes $P \in \mathbb{Z}[X]$ qui sont des états de l'automate $\mathscr{A}^{\mathrm{rel}}$ ont leur $i^{\text{ème}}$ coefficient borné par

$$\sum_{j \geq i} \max_{\sum_s p_s X^s \in A-A} |p_j| .$$

Soit $Q = \sum_j q_j X^j$ un état de l'automate $\mathscr{A}$ ayant le $i^{\text{ème}}$ coefficient trop grand : $q_i > \sum_{j \geq i} \max_{\sum_j p_j X^j \in A-A} |p_j|$, et soit $(Q, (U, V), R)$ une transition de l'automate $\mathscr{A}$. Alors le $(i+1)^{\text{ème}}$ coefficient du polynôme

$R = XQ + U - V$ est trop grand :

$$\begin{aligned}|q_i + u_{i+1} - v_{i+1}| &> \Big(\sum_{j\geq i} \max_{\sum_s p_s X^s \in A-A} |p_j|\Big) - |u_{i+1} - v_{i+1}| \\ &\geq \Big(\sum_{j\geq i} \max_{\sum_s p_s X^s \in A-A} |p_j|\Big) - \max_{\sum_s p_s X^s \in A-A} |p_{i+1}| \\ &= \sum_{j\geq i+1} \max_{\sum_s p_s X^s \in A-A} |p_j|\,.\end{aligned}$$

De la même façon que précédemment, il ne peut donc pas exister de chemin de l'état Q vers l'état final 0, donc l'état Q n'est pas dans l'automate émondé $\mathscr{A}^{\mathrm{rel}}$.

On a montré que les polynômes P qui sont des états de l'automate $\mathscr{A}^{\mathrm{rel}}$ ont tous leur coefficients bornés et ont leur degré borné. On conclut donc que l'automate $\mathscr{A}^{\mathrm{rel}}$ est fini, et donc le semi-groupe Γ est fortement automatique.

– Si β est algébrique : Alors dans le cas où le corps k est de caractéristique non nulle, l'ensemble $(\mathbb{Z}/p\mathbb{Z})[\beta]$ des états de $\mathscr{A}$ est fini, et donc l'automate $\mathscr{A}^{\mathrm{rel}}$ est aussi fini.

Supposons donc que le corps k est de caractéristique nulle. Sans perte de généralité, on supposera que l'on a $k = \mathbb{Q}(\beta)$.

Définition 4.7. — *Soit $\mathscr{P}$ l'ensemble (fini) des valeurs absolues v du corps $k = \mathbb{Q}(\beta)$ qui sont telles que $|\beta|_v \neq 1$. L'hypothèse sur le nombre β garantit que $\mathscr{P}$ contient toutes les valeurs absolues archimédiennes. On définit un anneau $\mathscr{R}$ stable par multiplication par β et par β^{-1}, par*

$$\mathscr{R} = \{x \in k |\ \textit{Pour toute valeur absolue } v \notin \mathscr{P}, |x|_v \leq 1\}.$$

Proposition 4.8. — *L'anneau $\mathscr{R}$ est un réseau dans l'espace*

$$E := \prod_{v\in\mathscr{P}} k_v,$$

dans lequel il est plongé diagonalement, où k_v est le complété du corps k pour la valeur absolue v.

Preuve de la proposition 4.8. — La discrétude de $\mathscr{R}$ dans E est une conséquence de la formule du produit :

Proposition 4.9 (Formule du produit). —
Pour tout $x \in k\backslash\{0\}$, on a

$$\prod_{v\in\mathscr{P}_k} |x|_v = 1,$$

où $\mathscr{P}_k$ est l'ensemble des valeurs absolues du corps k (à équivalence près).

REMARQUE 4.10. — *Dans la proposition précédente, on a choisi les valeurs absolues « canoniques » dans chaque classe d'équivalence. Voir* [8]*, V.1. pour plus de détails.*

Etant donné un point $x_0 \in \mathscr{R}$, et un ensemble non vide de valeurs absolues $\mathscr{P}_0 \subseteq \mathscr{P}$ contenant les valeurs absolues archimédiennes, la formule du produit nous donne que le voisinage

$$V := \{x \in E | \text{ Pour toute valeur absolue } v \in \mathscr{P}\backslash\mathscr{P}_0, |x - x_0|_v \leq 1, \\ \text{et pour toute valeur absolue } v \in \mathscr{P}_0, |x - x_0|_v < 1\}$$

a pour intersection $\{x_0\}$ avec $\mathscr{R}$, ce qui donne bien la discrétude de $\mathscr{R}$ dans E.

Montrons maintenant la co-compacité de $\mathscr{R}$ dans E.

Pour cela, on utilise le théorème :

THÉORÈME 4.11. —
Le corps k est discret et co-compact dans l'ensemble des adèles $\mathbb{A}_k$.

Voir [8] pour la définition des adèles et une preuve du résultat.
L'espace $E' := E \times \prod_{v \in \mathscr{P}_k \backslash \mathscr{P}} \mathscr{O}_{k_v}$ est une partie ouverte de l'ensemble des adèles $\mathbb{A}_k$, donc son image dans le quotient $\mathbb{A}_k/k$ est aussi ouverte. On en déduit qu'elle est aussi fermée, puisque l'on peut écrire l'orbite de k sous l'action du groupe additif E' comme l'union des autres E'-orbites. Ainsi, l'image de E' dans le quotient $\mathbb{A}_k/k$ est compacte, d'où la co-compacité de $\mathscr{R} = k \cap E'$ dans E' et donc dans E. □

L'espace E est le produit d'un nombre fini de corps p-adiques, et de copies de $\mathbb{R}$ et $\mathbb{C}$.

EXEMPLE 4.12. — *Pour $\beta = \frac{1+\sqrt{-14}}{5}$, l'espace E est*

$$E = \mathbb{C} \times \mathbb{Q}_3 \times \mathbb{Q}_5.$$

Pour $\beta = \frac{\sqrt{-14}}{5}$, l'espace E est

$$E = \mathbb{C} \times \mathbb{Q}_5 \times \mathbb{Q}_5 \times E_2 \times E_7,$$

où E_2 et E_7 sont respectivement des extensions de degré 2 de $\mathbb{Q}_2$ et de $\mathbb{Q}_7$.

On va montrer que l'ensemble des états de l'automate $\mathscr{A}^{\text{rel}}$ est inclu dans une partie compacte de E, ce qui prouvera sa finitude. Soit $v \in \mathscr{P}$

une des valeurs absolues. Montrons que les états x de l'automate $\mathscr{A}^{\mathrm{rel}}$ vérifient

$$|x|_v < \frac{1}{|1-|\beta|_v|} \max_{a\in A-A} |a|_v .$$

Par définition de $\mathscr{P}$, on a $|\beta|_v \neq 1$. On a alors deux cas :

1. $|\beta|_v < 1$
   D'après le lemme 4.4, il existe un polynôme $P \in (A-A)[X]$ tel que l'on ait $x = P(\beta)$. On a alors
   $$|x|_v = |P(\beta)|_v < \max_{a\in A-A} |a|_v \sum_{i=0}^{\infty} |\beta|_v^i = \frac{1}{1-|\beta|_v} \max_{a\in A-A} |a|_v .$$
2. $|\beta|_v > 1$
   D'après le lemme 4.4, il existe un polynôme $Q \in (A-A)[X]$ tel que l'on ait $x = \beta^{-1}Q(\beta^{-1})$. On a alors
   $$|x|_v = \left|\beta^{-1}Q(\beta^{-1})\right|_v < \frac{1}{|\beta|_v - 1} \max_{a\in A-A} |a|_v .$$

Le domaine de l'espace E délimité par ces inégalités est relativement compact. Ainsi, la discrétude de l'anneau $\mathscr{R}$ dans l'espace E entraîne que l'automate $\mathscr{A}^{\mathrm{rel}}$ n'a qu'un nombre fini d'états. Donc le semi-groupe Γ est fortement automatique.

Ceci termine la preuve du théorème 4.2. □

Remarque 4.13. — *Dans les directions p-adiques, le fait que les valeurs absolues soient ultra-métriques permet d'obtenir les inégalités plus précises suivantes :*

$$|x|_p \leq \max_{a\in A-A} |a|_p \left|\beta^{-1}\right|_p \ \textit{ si } \ |\beta|_p > 1,$$
$$|x|_p \leq \max_{a\in A-A} |a|_p \ \textit{ si } \ |\beta|_p < 1,$$

pour tout état x non nul de l'automate $\mathscr{A}^{\mathrm{rel}}$.

Remarque 4.14. — *La condition pour le nombre algébrique β d'être sans conjugué de module 1 est nécessaire : voir exemple 4.23 et proposition 4.15. Cependant, il existe tout de même des nombres algébriques ayant au moins un conjugué de module 1 et pour lequels le semi-groupe est automatique. Par exemple, le semi-groupe engendré par les deux applications*

$$\begin{cases} x \mapsto \beta x \\ x \mapsto \beta x + 1 \end{cases}$$

est libre (et donc fortement automatique) dès que le nombre β a un conjugué de module strictement supérieur à 2. Ainsi, par exemple, il est libre pour le nombre de Salem qui est racine du polynôme $X^4 - 3X^3 - 3X^2 - 3X + 1$.

4.2. Réciproque. — Voici une réciproque au théorème 4.2, qui permet de voir que la condition sur le nombre β pour que le semi-groupe soit fortement automatique est optimale.

PROPOSITION 4.15. — *En caractéristique nulle, si β est un nombre algébrique ayant un conjugué de module* 1*, alors il existe une partie finie $A \subset \mathcal{R}$ telle que le semi-groupe Γ n'est pas fortement automatique.*

REMARQUE 4.16. — *D'après le lemme 4.4, la proposition 4.15 revient à dire que si β a un conjugué de module 1, alors il existe une partie finie $A \subset \mathcal{R}$ telle que l'ensemble*

$$\{x \in \mathcal{R} | \textit{Il existe } P, Q \in (A-A)[X] \textit{ tels que } x = P(\beta) = \beta^{-1}Q(\beta^{-1})\}$$

est infini.

REMARQUE 4.17. — *Dans la proposition 4.15, on peut même choisir $A \subset \mathbb{Z}[\beta]$.*

REMARQUE 4.18. — *Sous les hypothèses de la proposition, pour tout γ conjugué de β, l'inverse $1/\gamma$ est aussi un conjugué de β.*

En effet, si $\gamma \in \mathbb{C}$ est de module 1, alors $1/\gamma$ est son conjugué complexe.

L'idée de la preuve de la proposition 4.15 est la suivante : grâce au lemme 4.19 on se ramène à seulement montrer l'existence de chemins jusqu'à 0, plutôt que dans les deux sens. On choisit alors une partie finie A et un domaine infini $\mathbb{D}$ qui soient tels que l'on puisse trouver des transitions des points de $\mathbb{D}$ vers d'autres points de $\mathbb{D}$ plus proche de 0, jusqu'à tomber dans une partie compacte. Il suffira alors de rajouter à la partie A le bon ensemble fini de points pour obtenir des transitions de tous les points du compact vers 0.

Preuve de la proposition 4.15. — Soit $\beta \in \mathbb{C}$ un nombre algébrique ayant un conjugué de module 1. Pour toute partie A finie de $k = \mathbb{Q}(\beta)$, on considèrera l'automate $\mathcal{A}$ définit dans la preuve du théorème 4.2. D'après la proposition 4.8, on peut plonger l'anneau $\mathcal{R}$ dans un espace E qui est un produit de corps p-adiques et de copies des corps $\mathbb{R}$ et $\mathbb{C}$, de façon à ce que l'anneau $\mathcal{R}$ soit un réseau dans l'espace E. On peut alors écrire l'espace E comme un produit de trois espaces :

$$E = E_- \times E_0 \times E_+,$$

où

- l'espace E_+ est le produit des complétés du corps k pour les valeurs absolues v telles que $|\beta|_v > 1$,
- l'espace E_0 est le produit des complétés du corps k pour les valeurs absolues archimédiennes v telles que $|\beta|_v = 1$,

– l'espace E_- est le produit des complétés du corps k pour les valeurs absolues v telles que $|\beta|_v < 1$.

On notera respectivement $\mathscr{P}_-$, $\mathscr{P}_0$ et $\mathscr{P}_+$ les ensembles de valeurs absolues des corps des espaces E_-, E_0 et E_+. On notera aussi $\|.\|_0$ la norme infinie sur E_0.

NOTATION . — *Etant donné $x = P(\beta) \in \mathscr{R}$, on note $\overline{x} := P(\beta^{-1}) \in \mathscr{R}$.*

L'application $x \mapsto \overline{x}$ est un élément de $\mathrm{Gal}(\mathbb{Q}(\beta)/\mathbb{Q})$ d'après la remarque 4.18.

LEMME 4.19. — *S'il existe un chemin de x à 0 dans l'automate $\mathscr{A}$, alors il existe aussi un chemin de 0 à $\overline{x}/\beta$.*

Preuve du lemme. — De même que dans la preuve du lemme 4.4, l'existence d'un chemin de x à 0 est équivalente à l'existence d'un polynôme $Q \in (A-A)[X]$ tel que $x = \beta^{-1}Q(\beta^{-1})$. On obtient alors un chemin de 0 à $\overline{x}/\beta = Q(\beta)$ dans l'automate $\mathscr{A}$. □

On va montrer qu'il existe une partie finie $A \subset \mathscr{R}$ et un domaine $\mathbb{D}$ de l'espace E, tels que pour tout point x de l'ensemble infini $\mathbb{D} \cap \mathscr{R}$, il existe un chemin de x à 0 dans l'automate $\mathscr{A}$.

REMARQUE 4.20. — *L'existence d'un tel chemin revient à démontrer que pour tout point $x \in \mathbb{D} \cap \mathscr{R}$, il existe un polynôme $Q \in (A - A)[X]$ tel que l'on ait $x = \beta^{-1}Q(\beta^{-1})$.*

4.2.0.3. *Construction de la partie A.* — Nous allons construire la partie A en deux morceaux : la partie A_R nous permettra de rapprocher de 0 les éléments de grande norme, tandis que la partie A' permettra d'obtenir une transition de tous les autres éléments vers 0.

Pour $R > 0$, on définit une partie $A_R \subseteq \mathscr{R}$ par $x \in A_R$ si et seulement si l'on a

$$|x|_v < R,$$

pour toute valeur absolue v. On va maintenant fixer un réel R assez grand de la façon suivante :

Soit r le diamètre d'une maille (c'est-à-dire d'un domaine fondamental) du réseau $\mathscr{R}$ dans E. Définissons une partie $K \subseteq E_0 \times E_+$ par $x \in K$ si et seulement si

$$\text{pour toute valeur absolue } v \in \mathscr{P}_0, \quad |x|_v < 3r,$$
$$\text{pour toute valeur absolue } v \in \mathscr{P}_+, \quad |x|_v < |\beta|_v\, r.$$

En choisissant le rayon $R = 3r \max_{v\in\mathscr{P}} |\beta|_v$, la partie A_R est r-couvrante dans l'ensemble K (c'est bien une partie de l'espace $E_0 \times E_+$, comme partie

du corps k, qui se plonge diagonalement dans le produit de ses complétés). C'est-à-dire tel que l'on a :

$$K \subseteq \bigcup_{x \in A_R} B(x,r) \subseteq E_0 \times E_+.$$

On définit maintenant une partie $A' \subseteq \mathscr{R}$ par $x \in A'$ si et seulement si l'on a

$$\text{pour toute valeur absolue } v \in \mathscr{P}_+, \quad |x|_v < |\beta|_v \, r,$$
$$\text{pour toute valeur absolue } v \in \mathscr{P}_0, \quad |x|_v < 3r,$$
$$\text{pour toute valeur absolue } v \in \mathscr{P}_-, \quad |x|_v < \frac{\max_{x \in A_R} |x|_v}{1 - |\beta|_v},$$

La partie A finie de $\mathscr{R}$ que l'on considère est

$$A := A' \cup A_R.$$

4.2.0.4. *Construction du domaine* $\mathbb{D}$. —
On considère le domaine $\mathbb{D} \subseteq E$ définit par $x \in \mathbb{D}$ si et seulement si

$$|x|_v < r, \quad \text{pour toute valeur absolue } v \in \mathscr{P}_+,$$
$$|x|_v < \frac{\max_{x \in A_R} |x|_v}{1 - |\beta|_v}, \quad \text{pour toute valeur absolue } v \in \mathscr{P}_-.$$

4.2.0.5. *Preuve de la non finitude de* $\mathscr{A}^{\mathrm{rel}}$. — Montrons pour commencer qu'il existe une transition de tout point assez grand du domaine $\mathbb{D}$, vers un point strictement plus proche de 0.

LEMME 4.21. — *Pour tout point $x \in \mathbb{D} \cap k$ tel que $\|x\|_0 \geq 3r$, il existe un point $y \in \mathbb{D} \cap k$ tel que*

- *Il existe une transition dans l'automate $\mathscr{A}$ de x à y,*
- *On a l'inégalité $\|y\|_0 < \|x\|_0$.*

Démonstration. — Soit x un point de $\mathbb{D} \cap k$ tel que $\|x\|_0 \geq 3r$. Dans l'espace E_0, considérons une boule fermée B_0 de centre c sur le segment $[0, \beta x]$, de rayon r, ne contenant pas 0, et qui soit incluse dans la boule de centre 0 et de rayon $3r$. Le point de coordonnées c dans l'espace E_0 et βx dans l'espace E_+ est dans le compact K de l'espace $E_0 \times E_+$. La partie A_R étant r-couvrante, on peut alors trouver un point $t \in A_R$ qui est dans la boule B_0 dans l'espace E_0 et à distance au plus r de x dans l'espace E_+. Alors le point $y := \beta x - t$ convient car

1. Il y a bien une transition de x à y dans l'automate $\mathscr{A}$ puisque l'on a
$$-t \in -A \subseteq A - A.$$
2. Dans l'espace E_+, on a bien pour toute valeur absolue $v \in \mathscr{P}_+, |\beta x - t|_v < r$, puisque le point βx est dans la boule de centre t et de rayon r.

3. Dans l'espace E_0, par construction de la boule B_0, le fait que t soit dans B_0 nous donne l'inégalité stricte
$$\|\beta x - t\|_0 < \|\beta x\|_0 = \|x\|_0.$$
4. Dans l'espace E_-, on a bien pour toute valeur absolue $v \in \mathscr{P}_-$,

$$|\beta x - t|_v \leq |\beta|_v |x|_v + |t|_v < \frac{|\beta|_v \max_{a\in A_R} |a|_v}{1-|\beta|_v} + \max_{a\in A_R} |a|_v \leq \frac{\max_{a\in A_R} |a|_v}{1-|\beta|_v}. \quad \square$$

LEMME 4.22. — *Pour tout point $x \in \mathbb{D} \cap \mathscr{R}$, il existe un chemin de x à 0 dans l'automate $\mathscr{A}$.*

Démonstration. — Soit $x \in \mathbb{D} \cap \mathscr{R}$.

Supposons d'abord que l'on ait $\|x\|_0 < 3r$. Dans ce cas l'élément βx est dans l'ensemble A' (puisque l'on a $\|\beta x\|_0 = \|x\|_0 < 3r$). Il existe donc un élément $t \in -A' \subseteq -A \subseteq A - A$ tel que $\beta x + t = 0$, ce qui prouve l'existence d'une transition de x vers 0.

On est donc ramené à supposer que l'on ait $\|x\|_0 \geq 3r$. Le lemme 4.21 permet alors d'obtenir une transition vers un état de norme $\|.\|_0$ strictement inférieure. Par récurrence, et par discrétude de $\mathscr{R}$ dans E, on est donc ramené au premier cas. $\square$

Pour achever la preuve de la proposition 4.15, il suffit de remarquer que les lemmes 4.22 et 4.19 entraînent que les éléments de l'ensemble infini
$$\mathbb{D} \cap \beta^{-1}\overline{\mathbb{D}} \cap \mathscr{R}$$
sont des états de l'automate émondé $\mathscr{A}^{\mathrm{rel}}$. $\square$

4.3. Un exemple non fortement automatique. — La proposition 4.15 nous donne des parties A finies pour lesquelles le semi-groupe n'est pas fortement automatique. Voici un exemple de semi-groupe non fortement automatique pour une partie $A = \{0, 1\}$ fixée.

PROPOSITION 4.23. — *Soit le nombre de Salem $\beta = \frac{1+\sqrt{2}+\sqrt{2\sqrt{2}-1}}{2} \simeq 1.8832035059$ (qui est une racine du polynôme $X^4 - 2X^3 + X^2 - 2X + 1$). Alors, le monoïde engendré par les deux applications*
$$\begin{cases} 0 : x \mapsto \beta x \\ 1 : x \mapsto \beta x + 1 \end{cases}$$
n'est pas fortement automatique.

COROLLAIRE 4.24. — *Pour le nombre de Salem β de la proposition précédente, il n'existe aucune partie $A \subset \mathbb{C}$ finie et de cardinal au moins 2, telle que le monoïde Γ soit fortement automatique.*

Preuve du corollaire. — Soit $A_0 \subseteq A$ une partie de A de cardinal 2, et soit Γ_0 le semi-groupe engendré par les deux applications

$$x \mapsto \beta x + t, \text{ pour } t \in A_0.$$

Alors les sommets de l'automate $\mathscr{A}^{\mathrm{rel}}_{\Gamma_0}$ sont aussi des sommets de l'automate $\mathscr{A}^{\mathrm{rel}}_{\Gamma}$. En effet, tout chemin de l'automate $\mathscr{A}^{\mathrm{rel}}_{\Gamma_0}$ est aussi un chemin de l'automate $\mathscr{A}^{\mathrm{rel}}_{\Gamma}$. Ainsi, la forte automaticité du semi-groupe Γ entraîne celle du semi-groupe Γ_0. Or, le semi-groupe Γ_0 est le même que le semi-groupe de la proposition 4.23 modulo similitude (et donc le même d'un point de vue combinatoire). Ainsi, la proposition 4.23 implique que le semi-groupe Γ n'est pas fortement automatique. □

L'idée de la preuve de la proposition est la suivante : De même que dans la preuve de la proposition 4.15, on se ramène à montrer l'existence de chemins des points d'un domaine infini $\mathbb{D}$ vers 0. Et de la même façon, on commence par ramener tout point dans une partie compacte, puis on montre qu'il existe un chemin vers 0 pour chaque point de la partie compacte.

Ici il n'est pas possible de choisir la partie A pour pouvoir rapprocher les points de 0 en suivant une seule transition. Ce que l'on fera est de donner, suivant l'endroit où se trouve le point dans la partie contractante, des suites d'arêtes qui permettent de se rapprocher de 0 tout en restant bien dans le domaine $\mathbb{D}$.

Preuve de la proposition. — Le réel β est strictement supérieur à 1, et possède un conjugué réel de module strictement inférieur à 1, ainsi que deux conjugués complexes conjugués de module 1. L'anneau des entiers $\mathbb{Z}[\beta] = \mathscr{R}$ de β se plonge donc dans $\mathbb{R}^2 \times \mathbb{C}$, et on a trois plongements σ_+, σ_0 et σ_- dans les complétés du corps k pour les valeurs absolues respectives $|.|_+$, $|.|_0$ et $|.|_-$ telles que $|\beta|_+ > 1$, $|\beta|_0 = 1$ et $|\beta|_- < 1$. La preuve du théorème 4.2 nous permet de voir que les sommets de l'automate $\mathscr{A}^{\mathrm{rel}}$ sont dans un domaine de $\mathbb{R}^2 \times \mathbb{C}$ délimité par les inégalités

$$|x|_i < \frac{1}{||\beta|_i - 1|}, \text{ pour } i \in \{+, -\}.$$

Définissons alors le domaine $\mathbb{D} \subset \mathbb{R}^2 \times \mathbb{C}$ délimité par les inégalités

$$x \in \mathbb{D} \text{ si et seulement si } |x|_+ < \frac{c}{|\beta|_+ - 1} \text{ et } |x|_- < \frac{1}{1 - |\beta|_-},$$

où $0 < c < 1$ est une constante qui sera fixée ultérieurement.

De même que dans la preuve de la proposition 4.15, on souhaite démontrer le lemme :

LEMME 4.25. — *Pour tout point x de $\mathbb{D}\cap\mathbb{Z}[\beta]$, il existe un chemin dans l'automate $\mathcal{A}$ qui part de x et aboutit en 0.*

REMARQUE 4.26. — *Ceci revient à démontrer le résultat suivant :*

Pour tout $x\in\mathbb{D}\cap\mathbb{Z}[\beta]$, il existe $Q\in\{-1,0,1\}[X]$ tel que $x=\beta^{-1}Q(\beta^{-1})$.

Pour cela, nous allons donner une stratégie qui permet, partant d'un point $x\in\mathbb{D}$, d'aboutir à un sommet $y\in\mathbb{D}$ tel que $|y|_0<|x|_0$, en suivant des transitions de l'automate $\mathcal{A}$ données par une suite d'étiquettes dans $\{-1,0,1\}$. Nous allons donner cette stratégie de la façon suivante : étant donné un intervalle dans lequel se situe le point $(\beta-1)x$ dans la direction dilatante $E_+=\mathbb{R}$, nous donnerons trois suites d'éléments de $\{-1,0,1\}$ qui donnent des chemins vers trois états dont l'un au moins sera de module strictement inférieur à $|x|_0$ dans la direction correspondant aux complexes conjugués.

Pour obtenir cela, nous avons découpé l'intervalle de la direction dilatante correspondant au domaine $\mathbb{D}$ en intervalles vérifiant le lemme :

LEMME 4.27. — *Soit I un intervalle de $E_+=\mathbb{R}$. S'il existe trois suites $(a_i^1)_{1\le i\le n_1}$, $(a_i^2)_{1\le i\le n_2}$ et $(a_i^3)_{1\le i\le n_3}$ de $\{-1,0,1\}^{(\mathbb{N})}$ vérifiant :*

1. *Dans l'espace $E_0=\mathbb{C}$, les trois nombres complexes*
$$c_j:=\sum_{i=1}^{n_j}a_i^j\beta^{-i}\qquad\text{pour } j\in\{1,2,3\},$$
forment un triangle contenant 0 dans son intérieur.
2. *Pour tout $j\in\{1,2,3\}$, on a l'inclusion*
$$\beta^{n_j}I+\sum_{i=1}^{n_j}a_i^j\beta^{n_j-i}\subseteq\mathbb{D},$$

alors pour tout point $x\in\mathbb{D}$ tel que $\sigma_+(x)\in I$ et tel que $|x|_0$ est assez grand, il existe un chemin $x\xrightarrow{a_1^j}\dots\xrightarrow{a_{n_j}^j}y$ pour un $j\in\{1,2,3\}$, vers un point $y\in\mathbb{D}$ tel que $|y|_0<|x|_0$.

Démonstration. — La première condition permet de trouver un $j\in\{1,2,3\}$ tel que l'on ait l'inégalité
$$|x+c_j|_0<|x|_0\,,$$
dès que $|x|_0$ est assez grand.
En effet, il suffit que dans l'espace $E_0=\mathbb{C}$ le point x soit en dehors du triangle formé par les médiatrices des segments $[0,-c_j]$, $j=1,2,3$.

La deuxième condition assure que le point $y := \beta^{n_j}(x + c_j)$ est dans le domaine $\mathbb{D}$, et on a $|y|_0 = |x + c_j|_0$. Et pour finir, la définition de y donne l'existence du chemin

$$x \xrightarrow{a_1^j} \dots \xrightarrow{a_{n_j}^j} y$$

dans l'automate $\mathcal{A}$. □

Voici cette stratégie, pour $c = 0.883204$, en supposant que l'on parte d'un point $x \in \mathbb{D}$ tel que $|x|_0 > 3.883201$ et $\sigma_+(x) \geq 0$, et où les intervalles sont dilatés d'un facteur $\beta - 1$:

[0.468990, 0.601232]	[0.601232, 0.647807]	[0.647807, 0.671454]
-1 0 -1 1	-1 -1 0 1 1	-1 -1 0 0 1 1
-1 0 -1	-1 -1 1 -1 1	-1 -1 0 1 0 -1
-1 0 0	-1 0 -1 -1 1	-1 0 -1 -1 1 -1
[0.671454, 0.685095]	[0.685095, 0.708742]	[0.708742, 0.718028]
-1 0 -1 -1 -1 1	-1 -1 0 0 0 1	-1 -1 0 0 1 -1
-1 -1 0 1 0 -1	-1 -1 0 0 1 -1	-1 0 -1 -1 -1 0
-1 0 -1 -1 0 -1	-1 0 -1 -1 0 -1	-1 0 -1 -1
[0.718028, 0.780048]	[0.780048, 0.812982]	[0.812982, 0.832782]
-1 -1 -1 1 1	-1 -1 -1 0 1 1	-1 -1 -1 0
-1 -1 -1	-1 -1 -1 0 1	-1 -1 -1 0 1 0 -1
-1 -1 0 -1 1	-1 -1 -1 1 -1 1	-1
[0.832782, 0.850270]	[0.850270, 0.883204]	[-0.468990, 0.468990]
-1 -1 -1 0 0 1 -1	-1 -1 -1 -1 1	0^n
-1 -1 -1 0 0 0	-1 -1 -1 -1	
-1 -1 -1 0 1 -1 -1	-1 -1 -1 0 0	

Si l'on part d'un point $x \in \mathbb{D}$ tel que $|x|_0 > 3.883201$ et $\sigma_+(x) < 0$, alors on déduit la stratégie de celle donnée ci-dessus : il suffit de faire l'opposé de la suite de coups de l'intervalle opposé.
Quand on arrive dans l'intervalle [-0.468990, 0.468990], il suffit de suivre suffisamment d'arêtes étiquetées par 0 pour retomber dans l'un des intervalles ci-dessus ou son opposé.

Il reste ensuite à donner la stratégie pour $|x|_0 \leq 3.883201$. Le nombre de points est alors fini : il y en a 76. Voici une stratégie pour 38 de de ces points :

$1 \to$ -1 -1 -1 -1 1	$\beta - 2 \to$ 1 -1
$\beta - 1 \to$ -1 -1 -1	$2\beta - 3 \to$ -1 -1
$\beta^2 - 3\beta + 1 \to$ 1 1 1	$\beta^2 - 3\beta + 2 \to$ 0 1
$\beta^2 - 3\beta + 3 \to$ -1	$\beta^2 - 2\beta \to$ 0 0 1
$\beta^2 - 2\beta + 1 \to$ -1	$\beta^2 - \beta - 1 \to$ -1
$2\beta^2 - 4\beta \to$ 0 1	$2\beta^2 - 4\beta + 1 \to$ -1
$2\beta^2 - 3\beta - 1 \to$ -1	$\beta^3 - 3\beta^2 + \beta + 1 \to$ 1
$\beta^3 - 3\beta^2 + 2\beta \to$ 1	$\beta^3 - 3\beta^2 + 2\beta + 1 \to$ -1 -1 -1 1 1
$\beta^3 - 3\beta^2 + 3\beta - 2 \to$ 1	$\beta^3 - 3\beta^2 + 3\beta - 1 \to$ -1 -1 0 1 1 -1
$\beta^3 - 3\beta^2 + 4\beta - 3 \to$ -1 0 -1	$\beta^3 - 2\beta^2 - \beta + 2 \to$ 0 1
$\beta^3 - 2\beta^2 \to$ 0 1	$\beta^3 - 2\beta^2 + 1 \to$ -1 0 0 -1 1
$\beta^3 - 2\beta^2 + \beta - 2 \to$ 1	$\beta^3 - 2\beta^2 + \beta - 1 \to$ 0 -1 -1 -1 1
$\beta^3 - \beta^2 - 2\beta \to$ 1 0 1 -1	$\beta^3 - \beta^2 - 2\beta + 1 \to$ -1
$\beta^3 - \beta^2 - \beta - 1 \to$ -1	$\beta^3 - 4\beta \to$ 1 1 1
$\beta^3 - 3\beta \to$ -1	$2\beta^3 - 5\beta^2 + 3\beta - 2 \to$ 1
$2\beta^3 - 5\beta^2 + 4\beta - 3 \to$ -1 1 0 1 1	$2\beta^3 - 4\beta^2 \to$ 1
$2\beta^3 - 4\beta^2 + \beta - 1 \to$ 1 -1 -1 -1	$2\beta^3 - 4\beta^2 + \beta \to$ -1 -1 -1 -1 -1 1 0 1 1
$2\beta^3 - 4\beta^2 + 2\beta - 2 \to$ -1 -1 -1 0 1	$2\beta^3 - 3\beta^2 - 2\beta \to$ 1 1
$2\beta^3 - 3\beta^2 - \beta - 1 \to$ 0 1	$2\beta^3 - 3\beta^2 - \beta \to$ -1 -1 0 -1

De la même façon que précédemment, on déduit la stratégie pour l'autre moitié des points en considérant la suite de coups opposée de l'élément de $\mathbb{Z}[\beta]$ opposé.

En suivant cette stratégie, on aboutit à l'état 0 en partant de n'importe quel point du domaine $\mathbb{D}$. Il suffit donc de vérifier chacun des cas ci-dessus pour obtenir une preuve de l'exemple. Tout ceci a été vérifié par ordinateur. □

EXEMPLE 4.28. — *En suivant la stratégie ci-dessus, en partant de* $x = \beta^2 - 3$, *on obtient le chemin*

$$x = \beta^2 - 3 \xrightarrow{\text{-1 0 0}} \beta^2(\beta(\beta^2 - 3) - 1) = -\beta^2 + 3\beta - 2,$$

puisque $(\beta - 1)(\beta^2 - 3) \simeq 0.4826 \in [0.468990, 0.601232]$ *et* $\left|\beta^2 - 3\right|_0 \simeq 3.935 > 3.883201$. *L'opposé de l'élément* $-\beta^2 + 3\beta - 2$ *est alors dans la liste des* 38 *points (puisque* $\left|-\beta^2 + 3\beta - 2\right|_0 \simeq 3.75 < 3.883201$*), et on a successivement (en restant parmi ces* 38 *points ou leur opposé) :*

$$-\beta^2 + 3\beta - 2 \xrightarrow{\text{0 -1}} \beta^3 - \beta^2 - 2\beta \xrightarrow{\text{1 0 1 -1}} \beta^3 - 2\beta^2 \xrightarrow{\text{0 1}} -\beta^3 + 2\beta^2 - \beta + 1 \xrightarrow{\text{0 1 1 1 -1}} 0.$$

On peut vérifier que l'on a en effet l'égalité

$$(\beta^{15} + \beta^{11} - \beta^{10} - \beta^8 + \beta^7 - \beta^5 - \beta^3 - \beta^2 - \beta + 1)/\beta^{16} = \beta^2 - 3.$$

On obtient ainsi un chemin de $\beta^2 - 3$ *à* 0 *dans l'automate* $\mathcal{A}$. *Et on obtient aussi un chemin de* 0 *à* $((1/\beta)^2 - 3)/\beta = -2\beta^2 + 3\beta$, *par le lemme 4.19, étiqueté par le mot miroir et opposé.*

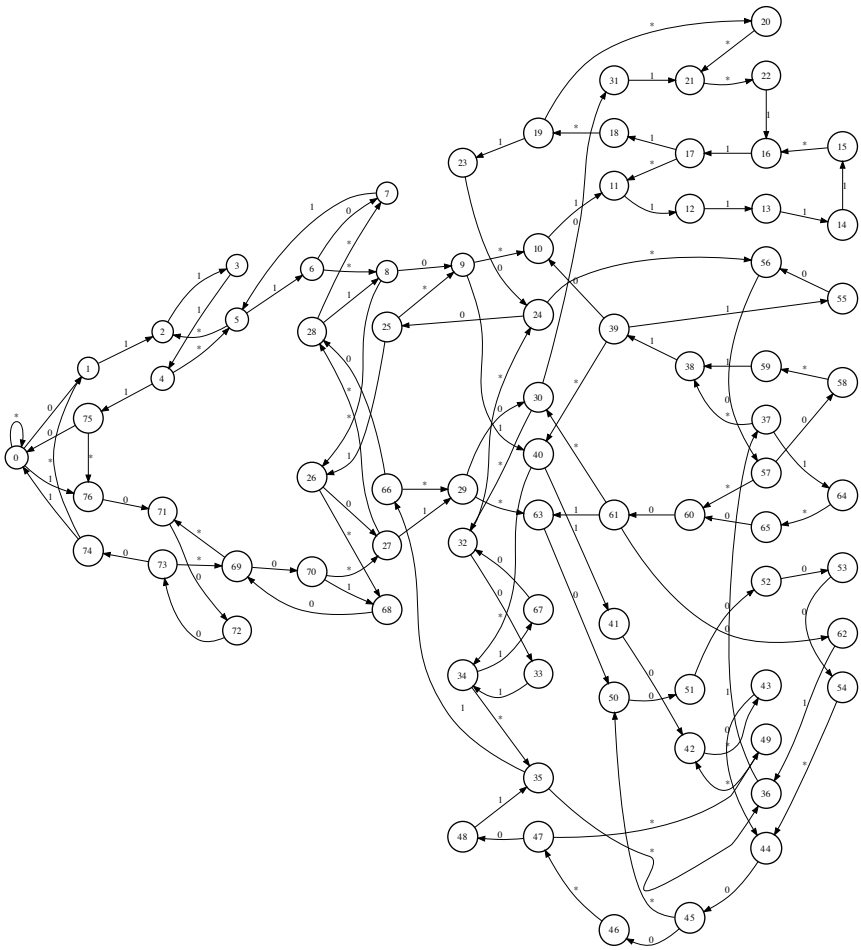


FIGURE 21. Portion de l'automate infini $\mathscr{A}^{\mathrm{rel}}$ des relations du semi-groupe de la proposition 4.23

Pour alléger les notations, sur la figure, on a remplacé les couples $(0,1)$ par 0, les couples $(1,0)$ par 1 et les paires de couples $(0,0)$ et $(1,1)$ par $*$.

REMARQUE 4.29. — *La preuve ci-dessus revient à démontrer le résultat suivant :*

Les restes dans la division euclidienne d'un polynôme $P \in \{-1,0,1\}[X]$ *par le polynôme* $\pi := X^4 - 2X^3 + X^2 - 2X + 1$ *sont exactement les polynômes*

$Q \in \mathbb{Z}[X]$ de degré au plus 3 tels que

$$|Q(\beta)| < \frac{1}{\beta - 1} \quad et \quad |Q(1/\beta)| < \frac{1}{1 - 1/\beta},$$

où $\beta > 1$ est la plus grande racine réelle de π.

La remarque suivante est due à Laurent Bartholdi.

REMARQUE 4.30. — *On peut montrer que le semi-groupe de l'exemple 4.23 n'est pas de présentation fini puisqu'il contient les relations $10^{4n}1 = 011(1001)^{n-1}110$ qui ne se déduisent pas de relations plus courtes.*

QUESTION . — *Le semi-groupe de l'exemple 4.23 est-il automatique ? A t'il un ensemble de mots réduits qui soit un langage rationnel ? Je conjecture une réponse négative à ces questions.*

4.4. Un exemple de semi-groupe fortement automatique et de présentation infinie. — Voici un exemple explicite de semi-groupe fortement automatique dont nous montrons qu'il n'est pas de présentation finie.

PROPOSITION 4.31. — *Soit $\beta \simeq 1.7924023578$ la racine réelle du polynôme $X^5 - X^4 - X^3 - X^2 + X - 1$. Alors, le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x \mapsto \beta x \\ 1 : x \mapsto \beta x + 1 \end{cases}$$

n'est pas de présentation finie.

Démonstration. — Le nombre β n'a pas de conjugué de module 1. D'après le théorème 4.2, le semi-groupe Γ est donc fortement automatique. Et de la preuve de ce théorème, on déduit que l'automate des relations du semi-groupe Γ est celui de la figure suivante.

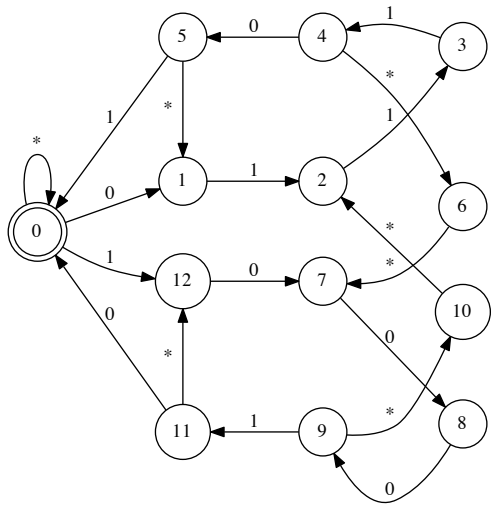


FIGURE 22. Automate $\mathscr{A}^{\mathrm{rel}}$ des relations du monoïde de la proposition 4.31

Pour alléger les notations, sur la figure, on a remplacé les couples $(0,1)$ par 0, les couples $(1,0)$ par 1 et les paires de couples $(0,0)$ et $(1,1)$ par $*$.

LEMME 4.32. — *On a les relations*

$$0111(00000011)^n01 = 1000(00110000)^n10$$

pour tout entier n.

Démonstration. — Cela se lit sur l'automate des relations ci-dessus. □

La proposition 4.31 se déduit alors du lemme suivant. □

LEMME 4.33. — *Les relations données par le lemme précédent sont minimales (c'est-à-dire qu'elles ne se déduisent pas de relations plus courtes).*

Démonstration. — On peut lire sur l'automate que pour toute relation minimale $u = v$, le mot u a un préfixe parmi $\begin{cases} 0111 \\ 1000**1 \\ 10001 \end{cases}$ (où les étoiles $*$ représentent chacune n'importe quelle lettre parmi 0 et 1) et a un suffixe parmi $\begin{cases} 010 \\ 101 \end{cases}$. Le mot u ne peut donc pas être un sous-mot strict du mot $0111(00000011)^n01$. □

5. Exemples

Cette section est consacrée à divers exemples qui rentrent dans la cadre du critère de forte automaticité des semi-groupes de développement en base β (théorème 4.2). Nous relions nos travaux à des travaux déjà existants, et donnons des automates des relations et des valeurs exactes d'exposants critiques que nous avons pu calculer grâce à notre preuve éffective du théorème 4.2.

Pour un semi-groupe Γ de développement en base β engendré par une partie finie G, on appellera *vitesse exponentielle de croissance* du semi-groupe le réel

$$\lambda := \limsup_{n\to\infty} \frac{1}{n} \log(\#G^n),$$

où G^n est l'ensemble des éléments de Γ de longueur n en les générateurs G.

Remarque 5.1. — *Pour un nombre $\beta \in \mathbb{C}$, si l'ensemble des générateurs G d'un semi-groupe Γ sont de la forme $x \mapsto \beta x + t$ pour $t \in \mathbb{C}$, alors l'exposant critique δ_Γ est relié à la vitesse exponentielle de croissance par*

$$\delta_\Gamma = \frac{\log(\lambda)}{|\log(\beta)|}.$$

5.1. Le cas où β est un nombre de Pisot. — On appelle *nombre de Pisot* un réel algébrique $\beta > 1$ qui a tous ses conjugués de modules strictement inférieurs à 1. Dans son article [7], Lalley s'intéresse aux semi-groupes engendrés par les transformations affines

$$x \mapsto \beta x + t$$

pout $t \in A \subset \mathbb{Z}[\beta]$, où $1/\beta$ est un nombre de Pisot et A est une partie finie de $\mathbb{Z}[\beta]$. D'après le théorème 4.2, le semi-groupe est fortement automatique. En particulier, il existe un automate des mots réduits pour l'ordre lexicographique, par la proposition 3.26. Lalley donne une construction de l'automate des mots réduits (mais sans parler d'automates), mais la construction que je propose dans cette thèse est différente. Il obtient ainsi la vitesse de croissance du semi-groupe, qu'il arrive à relier à la dimension de Hausdorff de l'ensemble limite.

5.2. L'exemple de Kenyon. — R. Kenyon étudie en détails dans son article [6] le semi-groupe engendré par les trois transformations

$$\begin{cases} 0 : x \mapsto x/3 \\ b : x \mapsto x/3 + t \\ 1 : x \mapsto x/3 + 1 \end{cases}$$

où $0 < t < 1$ est un réel.

D'après le théorème 4.2, ce semi-groupe est fortement automatique pour tout réel t. La proposition suivante permet de savoir si le semi-groupe Γ est libre ou non (et donc de savoir si l'automate des relations $\mathscr{A}^{\mathrm{rel}}$ est trivial ou non).

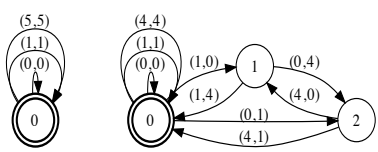
PROPOSITION 5.2 (Kenyon). — *Le semi-groupe* Γ *est libre si et seulement si le réel* t *n'est pas un rationnel de la forme* $\frac{p}{q}$ *avec* $p+q \not\equiv 0 \mod 3$, *pour* $p \wedge q = 1$.

Dans son article, Kenyon propose une construction d'automates qui est un cas particulier de la construction que je propose dans cet article. Il s'intéresse à la dimension de Hausdorff de l'ensemble limite du semi-groupe Γ. Il montre que celle-ci est reliée à la vitesse exponentielle de croissance du semi-groupe (que l'on peut calculer avec l'automate des mots réduits) quand le paramètre de translation t est rationnel. C'est encore une conjecture (connue sous le nom de conjecture de Furstenberg) que l'ensemble limite est de dimension de Hausdorff 1 quand le paramètre de translation t est irrationnel. Voir [6].

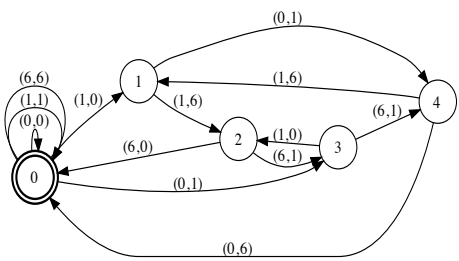
Voici quelques exemples d'automates des relations que l'on obtient pour le monoïde engendré par les 3 transformations

$$\begin{cases} 0 : x \mapsto x/3, \\ a : x \mapsto x/3 + a, \\ b : x \mapsto x/3 + b. \end{cases}$$

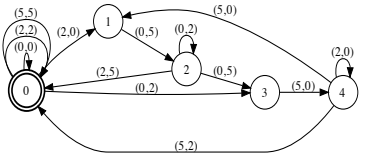
(Ce qui revient à considérer le semi-groupe de Kenyon avec $t = a/b$ et avec un élément neutre.) Cela permet de voir à quoi ressemble les premiers exemples d'automates correspondant aux semi-groupes de Kenyon.



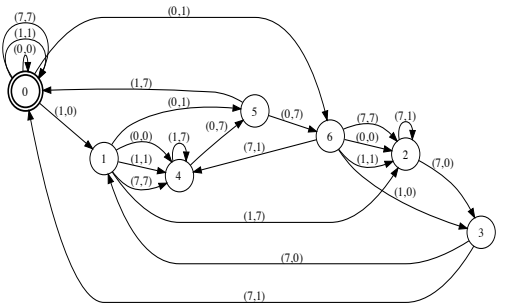
a=1 et b=5 a=1 et b=4



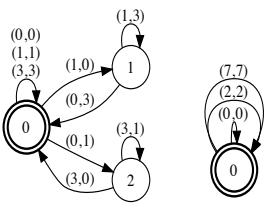
a=1 et b=6



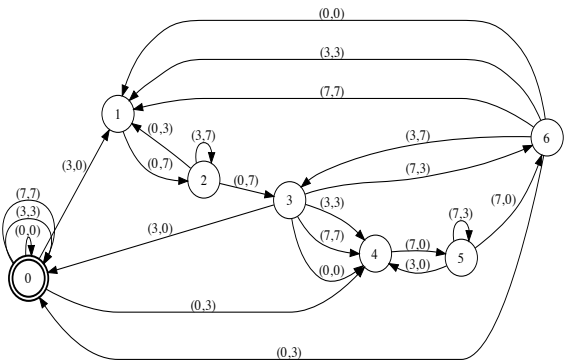
a=2 et b=5



a=1 et b=7

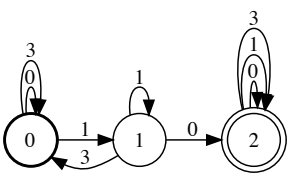


a=1 et b=3 a=2 et b=7

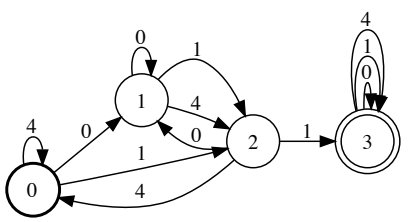


a=3 et b=7

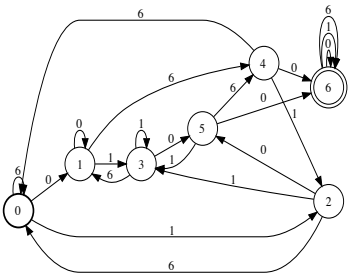
Et voici les automates minimaux des mots non réduits pour les même exemples (sauf pour $a/b = 1/5$ et $a/b = 2/7$ puisque les semi-groupes correspondant sont libres) :



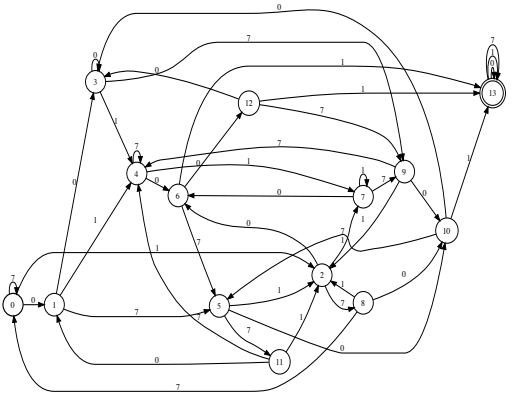
a=1 et b=3



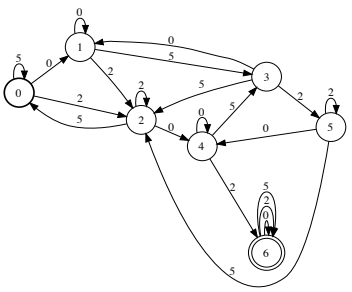
a=1 et b=4



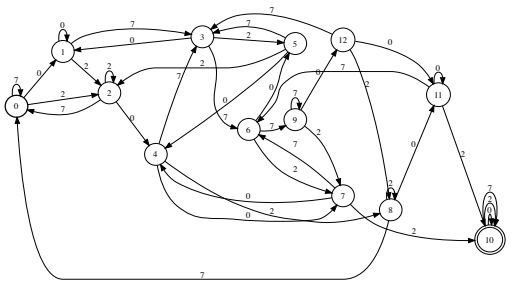
a=1 et b=6



a=1 et b=7



a=2 et b=5



a=3 et b=7

On en déduit facilement les automates des mots réduits et les vitesses de croissance de ces semi-groupes.

Voici la vitesse exponentielle de croissance λ du semi-groupe de Kenyon pour quelques valeurs du paramètre de translation t. On note π_λ le polynôme minimal de λ.

t	λ	π_λ
$1/3$	2.6180	x^2-3x+1
$1/4$	2.6180	x^2-3x+1
$2/5$	2.8019	x^3-4x^2+3x+1
$1/6$	2.7321	x^2-2x-2
$1/7$	2.7383	$x^5-3x^4+x^2+3x-1$
$3/7$	2.8794	x^3-3x^2+1
$3/8$	2.8136	x^3-2x^2-3x+2
$1/9$	2.6180	x^2-3x+1
$2/9$	2.7233	$x^6-3x^5+x^3+3x^2-1$
$4/9$	2.8794	x^3-3x^2+1
$1/10$	2.6180	x^2-3x+1
$3/10$	2.7699	$x^6-2x^5-4x^4+x^3+9x^2+6x+3$
$2/11$	2.7421	$x^5-4x^4+3x^3+x^2+x-1$
$3/11$	2.8073	$x^9-4x^8+x^7+7x^6-9x^3-x^2+3x-1$
$5/11$	2.9242	$x^{11}-5x^{10}+6x^9-7x^8+32x^7-32x^6+15x^5-49x^4+$ $20x^3-13x^2+3x-1$

J'ai donné ici tous les rationnels a/b dans l'intervalle $]0,1/2[$ ayant un dénominateur inférieur ou égal à 11, avec $a+b\not\equiv 0 \mod 3$. On en déduit facilement les valeurs des vitesses exponentielles de croissance pour tous les rationnels a/b ayant un dénominateur inférieur ou égal à 11. On constate que ces vitesses de croissance sont difficiles à prévoir. Il existe cependant des suites de valeurs de a/b pour lesquelles on connait la vitesse de croissance, comme par exemple les $1/3^n$ et $1/(3^n+1)$.

5.3. Développement β-adique avec ensemble de chiffres $\{0,1\}$. — Considérons le monoïde engendré par les deux transformations affines

$$\begin{cases} 0 : x \mapsto \beta x, \\ 1 : x \mapsto \beta x + 1, \end{cases}$$

où $\beta > 1$ est un réel. Si β est transcendant, le semi-groupe est libre, et donc sa structure automatique est triviale. Supposons que β soit algébrique.

DÉFINITION 5.3. — *On appelle* produit de Mahler *(ou mesure de Mahler) d'un nombre algébrique β le produit*

$$m_\beta := \prod_{\substack{v \text{ place de } \mathbb{Q}(\beta) \\ |\gamma|_v > 1}} |\gamma|_v ,$$

où l'on considère les valeurs absolues usuelles du corps de nombres $\mathbb{Q}(\beta)$.

Autrement dit, le produit de Mahler est le produit des modules des conjugués strictements supérieurs à 1 et du coefficient dominant du polynôme minimal de β.

On sait que le semi-groupe est libre quand le nombre algébrique β a un conjugué de module supérieur ou égal à 2 (puisque le semi-groupe avec $\beta > 2$ est de Schottky). Voici une réciproque :

PROPOSITION 5.4. — *Si le produit de Mahler m_β de β est strictement inférieur à 2, alors le semi-groupe n'est pas libre.*

Démonstration. — Toutes les valeurs absolues ultramétriques de β sont inférieure ou égales à 1, puisque sinon le produit de Mahler serait trop grand. Le réel β est donc un entier algébrique. On peut donc plonger l'anneau $\mathbb{Z}[\beta]$ dans $\mathbb{R}^d$, de tel façon qu'il y soit un réseau, où d est le degré du nombre algébrique β. Si l'on considère les 2^{n+1} polynômes en β de degré n et à coefficients dans $\{0,1\}$, on remarque qu'ils sont inclus dans un domaine de $\mathbb{R}^d$ qui est de volume majoré par $P(n)m_\beta^n$, pour un certain polynôme P. Comme l'anneau des entiers est un réseau de $\mathbb{R}^d$, ceci nous donne que le nombre d'éléments du semi-groupe de longueur n est majoré par $cP(n)m_\beta^n$, pour une constante $c > 0$, ce qui est strictement inférieur à 2^{n+1} pour n assez grand. D'où l'existence d'une relation non triviale dans le semi-groupe. □

La preuve ci-dessus montre que, sous les hypothèses de la proposition, l'exposant de croissance du semi-groupe est majoré par le produit de Mahler. Dans tous les exemples vérifiant les hypothèses de la proposition que j'ai pu voir, l'exposant de croissance du semi-groupe est même égal au produit de Mahler (i.e. $\delta_\Gamma = \frac{\log(m_\beta)}{\log(\beta)}$).

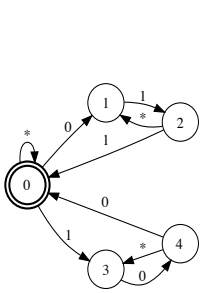
REMARQUE 5.5. — *Dans le cas particulier où le réel β est strictement inférieur à 2, l'étude du semi-groupe est liée à celle du système dynamique*

$$\begin{aligned} T : \mathbb{R}/\mathbb{Z} &\to \mathbb{R}/\mathbb{Z} \\ x &\mapsto \beta x \mod 1. \end{aligned}$$

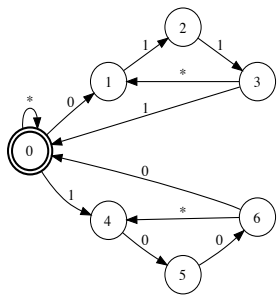
Voici quelques exemples d'automates des relations pour le monoïde engendré par les applications

$$\begin{cases} 0 : x \mapsto \beta x, \\ 1 : x \mapsto \beta x + 1, \end{cases}$$

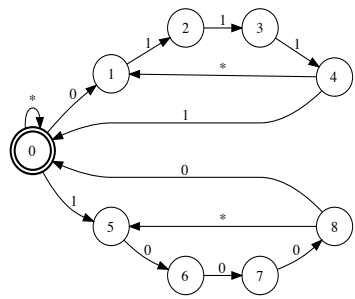
où l'étiquette 0 signifie $(0,1)$, l'étiquette 1 signifie $(1,0)$ et l'étiquette $*$ signifie que l'on a deux arêtes étiquetées respectivement par $(0,0)$ et $(1,1)$.



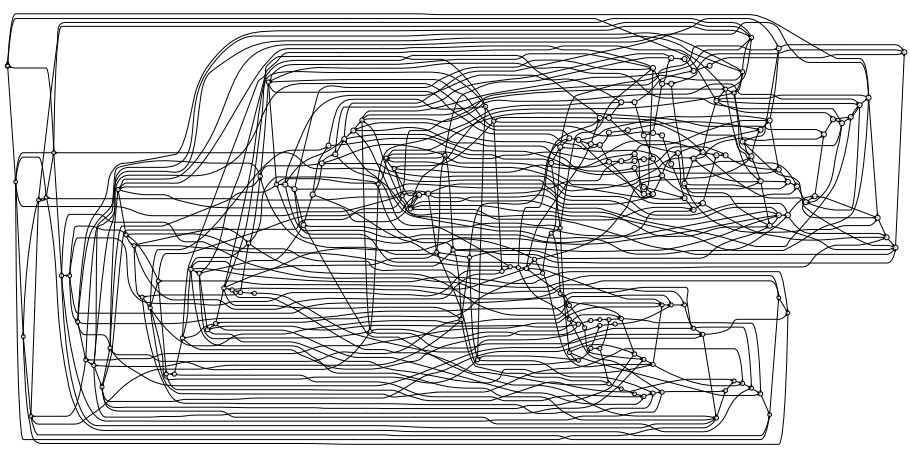
$\pi_\beta = x^2 - x - 1$



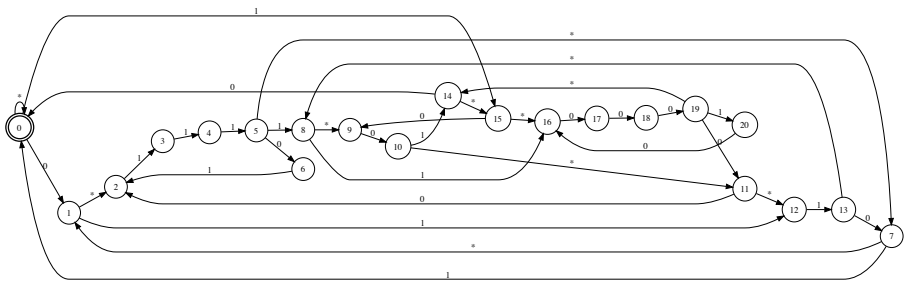
$\pi_\beta = x^3 - x^2 - x - 1$



$\pi_\beta = x^4 - x^3 - x^2 - x - 1$



$\pi_\beta = x^3 - x - 1$



$$\pi_\beta = x^4 - x^3 - x^2 + x - 1$$

Les trois premiers exemples d'automates des relations sont pour des nombres de Pisot, tandis que ce dernier exemple est pour un nombre qui n'est pas de Pisot. On peut voir que ces automates peuvent être très simples, mais aussi très compliqués même pour un des plus simples exemples de nombre de Pisot.

5.4. Un cas où β est un nombre transcendant. — Considérons le monoïde engendré par les 3 transformations

$$\begin{cases} 0 : x \mapsto \beta x, \\ p : x \mapsto \beta x + P(\beta), \\ q : x \mapsto \beta x + Q(\beta), \end{cases}$$

où β est un nombre transcendant, et P et Q sont deux polynômes à coefficients entiers.

REMARQUE 5.6. — *On peut supposer que l'on a* $\deg P < \deg Q$ *et* $\operatorname{pgcd}(P, Q) = 1$.

En effet, si l'on a $\deg Q < \deg P$, alors il suffit d'échanger P et Q, et si $\deg P = \deg Q$, alors le monoïde engendré par les transformations

$$\begin{cases} 0 : x \mapsto \beta x, \\ p : x \mapsto \beta x + (Q - P)(\beta), \\ q : x \mapsto \beta x + Q(\beta), \end{cases}$$

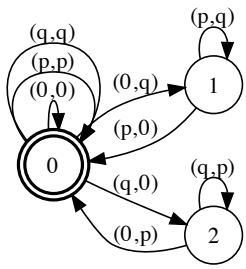
est le même. Si maintenant on a $\deg P = \deg Q = \deg (Q - P)$, alors le semi-groupe est libre, puisque l'on ne peut avoir d'égalité non triviale

$$\sum_{i=0}^{n} \epsilon_i \beta^i = 0,$$

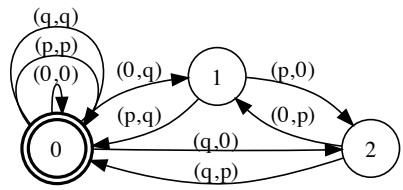
avec $\epsilon_i \in \{0, P, Q\} - \{0, P, Q\} = \{0, P, Q, -P, -Q, P - Q, Q - P\}$. On peut toujours supposer que les polynômes P et Q sont premiers entre eux quitte à tout diviser par le pgcd.

D'après la proposition 5.2 de Kenyon, le semi-groupe est libre dès que l'on a $P(3) + Q(3) \equiv 0 \mod 3$. Et d'après la preuve du théorème 4.2, déterminer si le semi-groupe est libre est toujours décidable, puisque la structure fortement automatique du semi-groupe est calculable. La remarque 5.8 donne un critère pour déterminer si le semi-groupe est libre. Mais existe-t'il un critère simple pour déterminer si le semi-groupe est libre à partir des polynômes P et Q ?

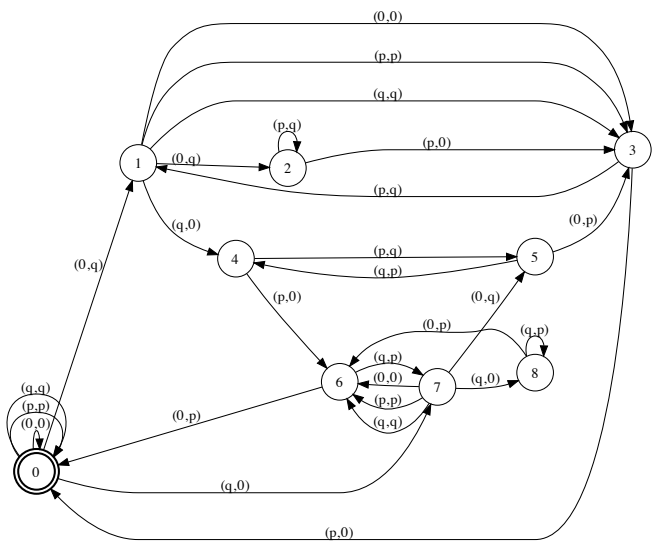
Voici quelques exemples d'automates des relations pour ce semi-groupe



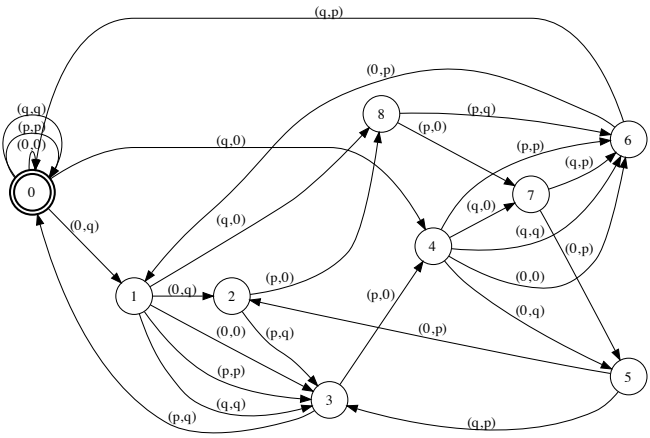
P=1 et Q=X



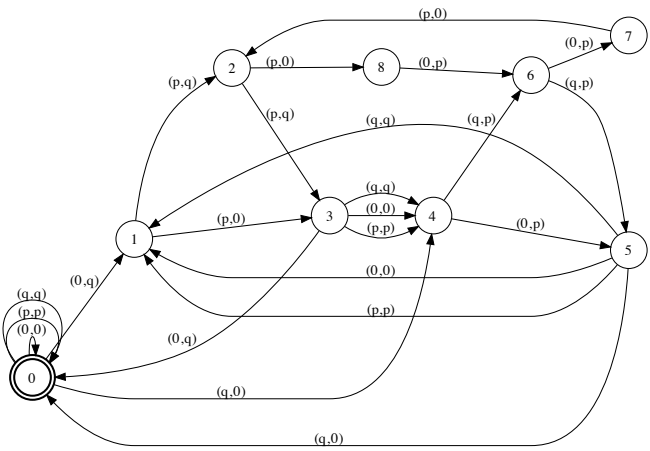
P=1 et Q=X+1



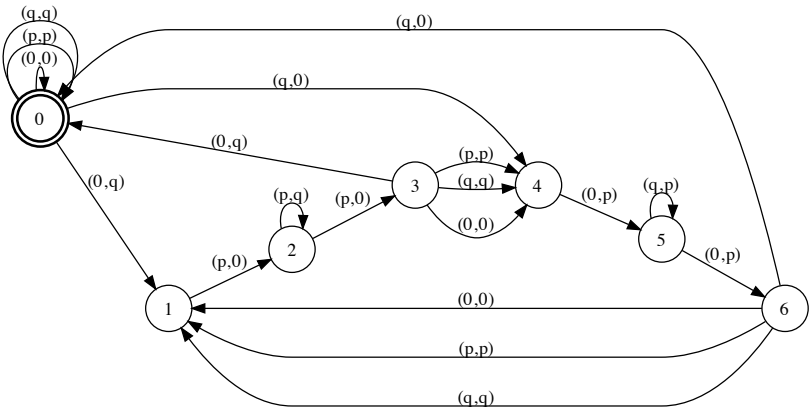
$P = 1$ et $Q = X^2$



$$P = 1 \text{ et } Q = X^2 + 1$$

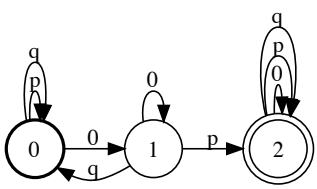


$$P = X \text{ et } Q = X^2 + 1$$

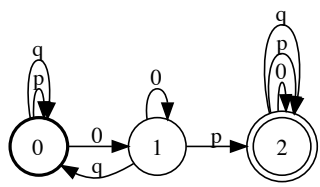


$P = X$ et $Q = X^2 - X + 1$

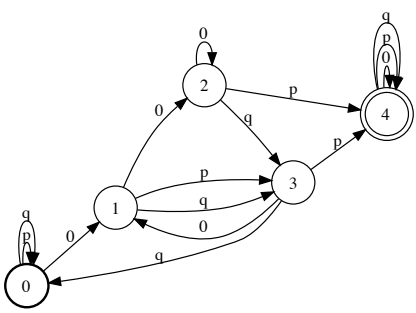
Et voici les automates des mots réduits pour les mêmes exemples :



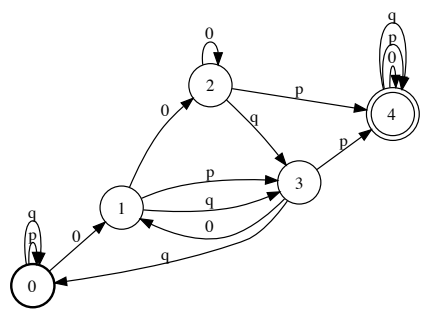
$P = 1$ et $Q = X$



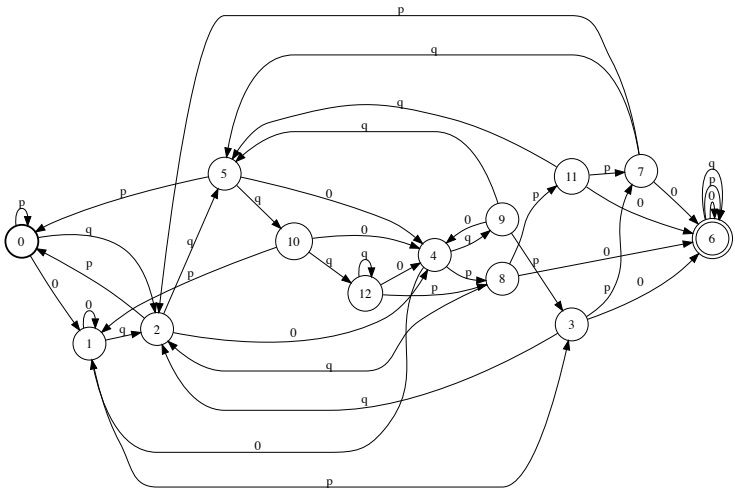
$P = 1$ et $Q = X + 1$



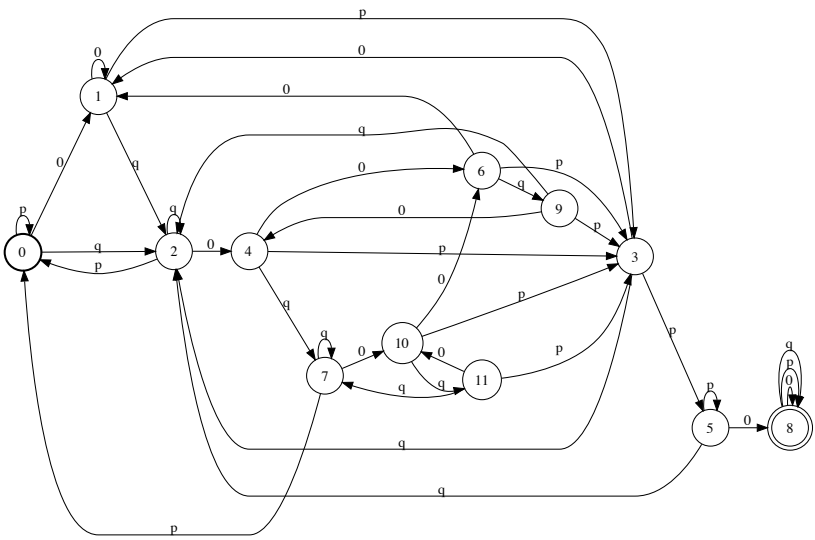
$P = 1$ et $Q = X^2$



$P = 1$ et $Q = X^2 + 1$



$P = X$ et $Q = X^2 + 1$



$P = X$ et $Q = X^2 - X + 1$

Voici les vitesses exponentielles de croissance λ pour quelques exemples, où π_λ est le polynôme minimal de λ :

P/Q	λ	π_λ
$1/X$	2.6180	x^2-3x+1
$1/(X+1)$	2.6180	x^2-3x+1
$1/(X^2-X)$	2.8794	x^3-3x^2+1
$1/(X^2-X+1)$	2.7971	$x^4-2x^3-2x^2-x+1$
$1/X^2$	2.6180	x^2-3x+1
$1/(X^2+1)$	2.6180	x^2-3x+1
$1/(X^2+X)$	2.8794	x^3-3x^2+1
$1/(X^2+X+1)$	2.7693	x^3-3x^2+x-1
$(X-1)/X^2$	2.7971	$x^4-2x^3-2x^2-x+1$
$(X-1)/(X^2+X-1)$	2.8794	x^3-3x^2+1
$1/(X^3-X^2-X)$	2.9615	x^4-3x^3+1
$1/(X^3-X^2)$	2.8584	$x^7-3x^6+3x^3+x^2-1$
$1/(X^3-X^2+1)$	2.8396	$x^{10}-3x^9+3x^6+x^5+4x^4-3x^3-3x^2+1$
$1/(X^3-X^2+X)$	2.8444	$x^{13}-3x^{12}-2x^{11}+7x^{10}-2x^9+7x^8-$ $16x^6+6x^5-6x^3+8x^2+x-2$

On remarque qu'à nouveau ces vitesses exponentielles de croissance sont difficiles à prévoir, mais qu'il y a tout de même des valeurs particulières pour lesquelles on les connait (par exemple les $1/X^n$).

REMARQUE 5.7. — *La vitesse exponentielle de croissance du semi-groupe pour β transcendant majore celle du semi-groupe pour β algébrique. Pour l'exemple de l'introduction (qui correspond aux polynômes $P=1$ et $Q=X$), le caractère algébrique de $1/3$ n'a aucun rôle : le semi-groupe est le même (d'un point de vue combinatoire) en prenant β transcendant plutôt que $\beta=1/3$. Cependant, les semi-groupes diffèrent quand on prend par exemple $P=X$ et $Q=X^2-X+1$ suivant que $\beta=1/3$ ou que β est transcendant.*

REMARQUE 5.8. — *Le semi-groupe n'est pas libre si et seulement si l'on a $P/Q=A/B$ pour deux polynômes $A,B\in\{-1,0,1\}[X]$ et avec $A-B\in\{-1,0,1\}[X]$. C'est pourquoi tous les exemples considérés ci-dessus sont de cette forme.*

BIBLIOGRAPHIE

[1] J. BERSTEL – *Transductions and context-free languages*, Leitfäden der Angewandten Mathematik und Mechanik, vol. 38, B. G. Teubner, 1979.

[2] A. CAIN – « Presentations for subsemigroups of groups », Thèse, University of St Andrews, 2005.

[3] O. Carton – *Langages formels, calculabilité et complexité*, Vuibert, 2008.

[4] J. Cassaigne & F. Nicolas – « On the decidability of semigroup freeness », *RAIRO Theor. Inform. Appl.* **46** (2012), p. 355–399.

[5] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson & W. P. Thurston – *Word processing in groups*, Jones and Bartlett Publishers, 1992.

[6] R. Kenyon – « Projecting the one-dimensional Sierpinski gasket », *Israel J. Math.* **97** (1997), p. 221–238.

[7] S. P. Lalley – « β-expansions with deleted digits for Pisot numbers β », *Trans. Amer. Math. Soc.* **349** (1997), p. 4355–4365.

[8] S. Lang – *Algebraic number theory*, second éd., Graduate Texts in Math., vol. 110, Springer, 1994.

[9] J. Sakarovitch – « Easy multiplications. I. The realm of Kleene's theorem », *Inform. and Comput.* **74** (1987), p. 173–197.