317

ASTÉRISQUE

2008

SÉMINAIRE BOURBAKI
VOLUME 2006/2007
EXPOSÉS 967-981

(971) *Groupes engendrés par les automates*

Andrzej ŻUK

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Séminaire BOURBAKI Novembre 2006
59e année, 2006-2007, no 971, p. 141 à 174

GROUPES ENGENDRÉS PAR LES AUTOMATES

par **Andrzej ŻUK**

INTRODUCTION

La classe des groupes d'automates contient plusieurs groupes infinis de type fini remarquables. Leur étude a permis de résoudre des problèmes importants de théorie des groupes. Des applications récentes s'étendent à l'algèbre, la géométrie, l'analyse et les probabilités.

Avec les groupes arithmétiques [**24**] et hyperboliques [**19**], les groupes d'automates dominent actuellement notre vision de la théorie des groupes infinis.

Les groupes présentés dans ce texte pourraient être rassemblés sous d'autres noms, comme groupes branchés ou groupes auto-similaires (les définitions précises de ces deux classes sont données plus loin). Nous avons choisi le nom « groupes d'automates » pour souligner l'importance de cette construction, qui produit des groupes aux propriétés intéressantes.

Comme exemples d'application de cette théorie, nous avons choisi les problèmes suivants.

- Problème de Burnside. Groupes infinis de type fini de torsion.
- Problème de Milnor. Constructions de groupes à croissance intermédiaire.
- Problème d'Atiyah. Calculs de nombres de Betti L^2.
- Problème de Day. Nouveaux exemples de groupes moyennables.
- Problème de Gromov. Groupes sans croissance uniforme.

Pour chacun d'entre eux, nous avons choisi les premiers exemples historiques de groupes d'automates considérés pour résoudre ces problèmes. Il s'agit du groupe d'Aleshin, du groupe d'allumeur de réverbères (qui peut être engendré par un automate à deux états), du groupe de Wilson et d'un groupe engendré par un automate à trois états.

Nous avons le sentiment que la classe des groupes d'automates est très riche et qu'on est loin d'une compréhension complète de ces groupes qui défient souvent notre intuition.

Nous espérons que cette introduction au monde des groupes engendrés par les automates pourrait stimuler les développements futurs.

1. GROUPES D'AUTOMATES

1.1. Définition du groupe engendré par un automate

Les automates qui nous intéressent sont finis, inversibles, avec le même alphabet à l'entrée et à la sortie, disons $D = \{0, 1, \dots, d-1\}$ pour un certain entier $d > 1$. À un tel automate A sont associés un ensemble fini d'états Q, une fonction de transition $\phi : Q \times D \to Q$ et une fonction de sortie : $\psi : Q \times D \to D$; l'automate A est caractérisé par le quadruplet (D, Q, ϕ, ψ).

L'automate A est dit inversible si, pour chaque $q \in Q$, la fonction $\psi(q, \cdot) : D \to D$ est une bijection. Dans ce cas, $\psi(q, \cdot)$ peut être identifiée avec l'élément correspondant σ_q du groupe symétrique S_d sur $d = |D|$ symboles.

Il existe un moyen convenable de représenter un automate fini par un graphe marqué $\Gamma(A)$ dont les sommets correspondent aux éléments de Q. Deux états $q, s \in Q$ sont liés par une arête orientée étiquetée par $i \in D$ si $\phi(q, i) = s$; chaque sommet $q \in Q$ est étiqueté par l'élément correspondant σ_q du groupe symétrique.

Les automates que l'on vient de définir sont les automates non initiaux. Pour les rendre initiaux, on doit pointer un état $q \in Q$ comme état initial. L'automate initial $A_q = (D, Q, \phi, \psi, q)$ agit à droite sur les suites finies et infinies sur D de la manière suivante. Pour chaque symbole $x \in D$, l'automate donne immédiatement la sortie $y = \psi(q, x)$ et change son état initial en $\phi(q, x)$.

En joignant la sortie de A_q avec l'entrée d'un autre automate $B_s = (S, \alpha, \beta, s)$, on obtient une application qui correspond à un automate appelé la composition de A_q et B_s et désigné par $A_q \star B_s$.

Cet automate est formellement décrit comme l'automate dont l'ensemble des états est $Q \times S$ et les fonctions de transition et de sortie Φ, Ψ sont définies par

$$\Phi((x, y), i) = (\phi(x, i), \alpha(y, \psi(x, i))),$$

$$\Psi((x, y), i) = \beta(y, \psi(x, i))$$

et avec l'état initial (q, s).

La composition $A \star B$ de deux automates non initiaux est définie par les mêmes formules pour les fonctions d'entrée et de sortie mais sans indiquer l'état initial.

Deux automates initiaux sont dits équivalents s'ils déterminent la même application sur l'ensemble des états. Il existe un algorithme pour minimiser le nombre d'états.

L'automate qui produit l'application identité sur l'ensemble des suites est appelé trivial. Si A est un automate inversible, alors pour chaque état q l'automate A_q admet un automate inverse A_q^{-1} tel que $A_q \star A_q^{-1}$, $A_q^{-1} \star A_q$ soient équivalents à l'automate trivial. L'automate inverse peut formellement être décrit comme l'automate $(Q, \widetilde{\phi}, \widetilde{\psi}, q)$ où $\widetilde{\phi}(s,i) = \phi(s, \sigma_s(i))$, $\widetilde{\psi}(s,i) = \sigma_s^{-1}(i)$ pour $s \in Q$. Les classes d'équivalence d'automates finis inversibles sur un alphabet D constituent un groupe qui est appelé le groupe des automates finis ; il dépend de D. Chaque ensemble d'automates initiaux engendre un sous-groupe de ce groupe.

Soit maintenant A un automate inversible non initial. Soit $Q = \{q_1, \ldots, q_t\}$ l'ensemble des états de A et soit $A_{q_1}, \ldots, A_{q_t}$ l'ensemble des automates initiaux que l'on peut obtenir à partir de A. Le groupe $G(A) = \langle A_{q_1}, \ldots, A_{q_t} \rangle$ est appelé le groupe déterminé ou engendré par A.

1.2. Groupes d'automates et produits en couronne

Il existe une relation entre les groupes d'automates et les produits en couronne. Pour un groupe de la forme $G(A)$, on a l'interprétation suivante.

Soit $q \in Q$ un état de A et soit $\sigma_q \in S_d$ la permutation associée à cet état. Pour chaque symbole $i \in D$, on note $A_{q,i}$ l'automate initial ayant pour état initial $\phi(q,i)$ (alors $A_{q,i}$ pour $i = 0, 1, \ldots, d-1$ parcourt l'ensemble des automates initiaux qui sont les voisins de A_q, i.e. tels que le graphe $\Gamma(A)$ admette une arête de A_q à $A_{q,i}$).

Soient G et F des groupes de type fini tels que F soit un groupe de permutations d'un ensemble X (nous nous intéressons au cas où F est le groupe symétrique S_d et X est l'ensemble $\{0, 1, \ldots, d-1\}$). On définit le produit en couronne $G \wr F$ de ces groupes comme suit. Les éléments de $G \wr F$ sont les couples (g, γ) où $g : X \to G$ est une fonction telle que $g(x)$ soit différente de l'élément neutre de G, noté Id, seulement pour un nombre fini d'éléments x de X, et où γ est un élément de F. La multiplication dans $G \wr F$ est définie par :

$$(g_1, \gamma_1)(g_2, \gamma_2) = (g_3, \gamma_1\gamma_2)$$

où

$$g_3(x) = g_1(x) g_2(\gamma_1^{-1}(x)) \quad \text{pour } x \in X.$$

On écrira les éléments du groupe $G \wr S_d$ sous la forme $(a_0, \ldots, a_{d-1})\sigma$, où $a_0, \ldots, a_{d-1} \in G$ et $\sigma \in S_d$.

Le groupe $G = G(A)$ admet un plongement dans le produit en couronne $G \wr S_d$ via l'application

$$A_q \to (A_{q,0}, \ldots, A_{q,d-1})\sigma_q,$$

où $q \in Q$. L'expression à droite est appelée décomposition en couronne de A. On écrira ainsi dans le texte $A_q = (A_{q,0}, \dots, A_{q,d-1})\sigma_q$.

Pour simplifier, on note a le générateur A_a du groupe engendré par l'automate A.

1.3. Action sur un arbre

Les suites finies sur l'alphabet $D = \{0, \dots, d-1\}$ sont en bijection avec les sommets d'un arbre enraciné T_d de degré d (dont la racine correspond à la suite vide).

Un automate initial A_q agit sur les suites sur D et agit aussi sur T_d par automorphismes. Ainsi pour chaque groupe engendré par un automate, en particulier pour un groupe de forme $G(A)$, il existe une action canonique correspondante sur un arbre (pour la théorie des actions sur les arbres sans racine, voir **[30]**).

Soit maintenant G un groupe agissant sur un arbre enraciné T. Le bord ∂T, constitué des rayons géodésiques infinis issus de la racine, admet une topologie naturelle qui le rend homéomorphe à l'ensemble de Cantor.

L'action de G sur T induit une action sur ∂T par homéomorphismes et admet une mesure canonique invariante μ sur ∂T qui est la mesure de Bernoulli sur $D^{\mathbb{N}}$ donnée par la distribution $\left\{\frac{1}{d}, \dots, \frac{1}{d}\right\}$.

Il existe un moyen canonique d'associer une représentation unitaire à un système dynamique muni d'une mesure invariante. Dans notre cas, on obtient la représentation régulière π sur $L^2(\partial T, \mu)$, définie par $(\pi(g)f)(x) = f(g^{-1}x)$.

1.4. Projections de stabilisateurs

Pour un groupe $G = G(A)$ agissant par automorphismes sur T, on note $\mathrm{St}_G(n)$ le sous-groupe de G constitué des éléments de G qui agissent trivialement sur le niveau n de l'arbre T. D'une manière analogue, pour un sommet $u \in T$, on note $\mathrm{St}_G(u)$ le sous-groupe de G constitué des éléments fixant u. Le plongement de G dans le produit en couronne $G \wr S_d$ induit un plongement $\phi : \mathrm{St}_G(1) \to G^d$ dans le groupe de base du produit en couronne. Celui-ci définit les projections canoniques $\psi_i : \mathrm{St}_G(1) \to G$ $(i = 1, \dots, d)$ données par $\psi_i(g) = \phi(g)|_i$ pour $g \in \mathrm{St}_G(1)$.

1.5. Groupes branchés et fractals

Le stabilisateur $\mathrm{St}_G(n)$ du n-ième niveau est l'intersection des stabilisateurs de tous les sommets de ce niveau. Pour tout sommet $u \in T$, on peut définir la projection $\psi_u : \mathrm{St}_G(u) \to G$.

DÉFINITION 1.1. — *Un groupe G est dit fractal si pour chaque sommet u, on a $\psi_u(\mathrm{St}_G(u)) = G$ après identification de l'arbre T avec le sous-arbre T_u issu de la racine u.*

Le stabilisateur rigide du sommet u est le sous-groupe, noté $\mathrm{Rist}_G(u)$, des automorphismes de G qui agissent trivialement sur le sous-arbre T_u. Le stabilisateur rigide du n-ième niveau $\mathrm{Rist}_G(n)$ est le groupe engendré par les stabilisateurs rigides des sommets sur ce niveau.

Un groupe G agissant sur un arbre enraciné T est dit sphériquement transitif s'il agit transitivement sur chaque niveau. Un groupe sphériquement transitif $G \subseteq \mathrm{Aut}(T)$ est dit branché si $\mathrm{Rist}_G(n)$ est un sous-groupe d'indice fini pour chaque $n \in \mathbb{N}$. Un groupe sphériquement transitif $G \subseteq \mathrm{Aut}(T)$ est dit faiblement branché si $|\mathrm{Rist}_G(n)| = \infty$ pour chaque $n \in \mathbb{N}$.

S'il n'y a pas de risque de confusion, on omettra l'indice G dans les notations $\mathrm{St}_G(u)$, $\mathrm{Rist}_G(u)$, etc.

Le plongement $G \to G \wr S_d$, $g \to (g_0, \ldots, g_{d-1})\sigma$ définit la restriction g_i de g au sommet i du premier niveau. L'itération de cette procédure conduit à une notion de restriction g_u de g à un sommet u.

DÉFINITION 1.2. — *On dit que le groupe G est régulièrement faiblement branché sur un sous-groupe $K \neq \{1\}$ si $K \supseteq K \times \ldots \times K$ (produit direct de d facteurs, chacun d'entre eux agissant sur le sous-arbre correspondant T_u, $|u| = 1$).*

On utilise les notations $x^y = y^{-1}xy, [x, y] = x^{-1}y^{-1}xy$ et on note $\langle X \rangle^Y$ la clôture normale de X dans Y. La longueur d'un mot w et d'un élément g est notée $|w|$ et $|g|$ respectivement.

1.6. Le problème des mots

Le problème des mots a une solution pour chaque groupe engendré par un automate, grâce à l'algorithme presenté ci-dessous :

PROPOSITION 1.3. — *Le problème des mots est résoluble pour les groupes d'automates.*

Preuve. — Soit w un mot sur l'alphabet consistant en les étiquettes des états de l'automate et leurs inverses.

1. Vérifier si $w \in \mathrm{St}_G(1)$ (sinon $w \neq 1$ dans G).
2. Calculer $w = (w_0, \ldots, w_{d-1})$. Alors

$$w = 1$$

dans G si et seulement si $w_i = 1$ dans G pour $i = 0, \ldots, d-1$. Aller à 1. en remplaçant w par w_i et procéder avec chaque w_i comme avec w.

Si, dans une étape, on obtient un mot qui n'est pas dans $\mathrm{St}_G(1)$, alors $w \neq 1$ dans G. Si dans une étape tous les mots $w_{i_1}, \ldots, w_{i_n}$ sont déjà apparus dans l'algorithme, alors $w = 1$ dans G.

Cet algorithme converge car les longueurs de $w_0, \ldots, w_{d-1}$ sont au plus la longueur de w et, après suffisamment d'étapes, les mots se répètent.

1.7. Classification des groupes d'automates à deux états sur l'alphabet $\{0,1\}$

Pour l'alphabet à deux lettres, les automates à un état produisent seulement le groupe trivial et le groupe d'ordre deux.

Certains automates à deux états sont déjà intéressants, par exemple le groupe d'allumeur de réverbères.

On se propose maintenant d'analyser tous les groupes engendrés par les automates à deux états avec un alphabet à deux lettres.

En plus du groupe d'allumeur de réverbères engendré par l'automate de la figure 2, il y a cinq autres groupes engendrés par les automates de la figure 1 (on note $\mathsf{1}$ ou Id l'identité de S_2 et e l'élément non trivial de S_2).

Les deux premiers automates engendrent le groupe trivial et le groupe d'ordre 2. Le groupe donné par le troisième automate est isomorphe au groupe de Klein $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$. Le quatrième automate définit le groupe diédral $\mathbb{D}_\infty$. Le dernier automate définit le groupe cyclique infini.

Ce sont les seules possibilités [**15**].

THÉORÈME 1.4. — *Les seuls groupes engendrés par les automates à deux états sur un alphabet à deux lettres sont :*

- *le groupe trivial* ;
- *le groupe d'ordre deux* $\mathbb{Z}/2\mathbb{Z}$;
- *le groupe de Klein* $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$;
- *le groupe cyclique inifini* $\mathbb{Z}$;
- *le groupe diédral infini* $\mathbb{D}_\infty$;
- *le groupe d'allumeur de réverbères* $(\oplus_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}$.

Preuve. — On note a et b les deux états de l'automate. Si les deux sont étiquetés par l'identité ou les deux par e, alors le groupe engendré par un tel automate est trivial ou bien $\mathbb{Z}/2\mathbb{Z}$.

Donc on peut supposer qu'un état, disons a, est étiqueté par l'identité et l'autre par e. En échangeant si nécessaire 0 avec 1, on peut supposer que $a = (a,a)$ ou $a = (b,b)$ ou $a = (a,b)$.

(i) Cas $a = (a,a)$.

Dans ce cas, a correspond à l'identité dans le groupe. L'échange de 0 et 1 (cela ne change pas a) réduit b à trois possibilités : $b = (b,b)\mathsf{e}$, $b = (a,b)\mathsf{e}$ ou $b = (a,a)\mathsf{e}$.

Le premier cas correspond à $\mathbb{Z}/2\mathbb{Z}$, le second à $\mathbb{Z}$ et le troisième à $\mathbb{Z}/2\mathbb{Z}$.

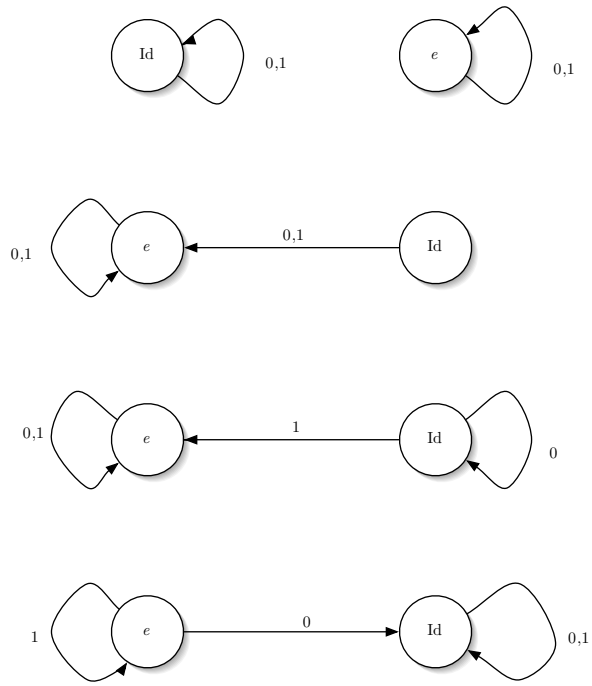

FIGURE 1. Les automates qui engendrent le groupe trivial, le groupe d'ordre deux, le groupe de Klein, le groupe diédral et le groupe cyclique infini.

(ii) Cas $a = (b, b)$.

L'échange de 0 et 1 (cela ne change pas a) réduit b à trois possibilités : $b = (b, b)\mathsf{e}$, $b = (b, b)\mathsf{e}$ ou $b = (a, b)\mathsf{e}$.

Les deux premières possibilités correspondent au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. En effet a et b sont d'ordre deux et commutent.

Le troisième cas correspond au groupe cyclique infini. En effet on a

$$ab = (ba, b^2)\mathsf{e},$$

$$ba = (ab, b^2)\mathsf{e},$$

donc a et b commutent. Deuxièmement,

$$b^2 a = (b^2 a, b^2 a),$$

ce qui implique la trivialité de $b^2 a$. Alors le groupe est cyclique. La relation précédente assure que l'ordre de a est deux fois l'ordre de b. Mais a et b ont le même ordre d'après

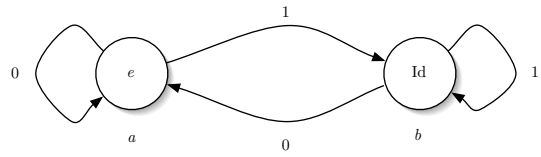

FIGURE 2. L'automate qui engendre le groupe d'allumeur de réverbères

la relation $a = (b, b)$. Comme a et b sont non triviaux, ceci implique que le groupe est $\mathbb{Z}$.

(iii) Cas $a = (a, b)$.

En considérant si nécessaire l'automate inverse (qui engendre le même groupe et ne change pas a) on peut supposer que b satisfait une des trois possibilités : $b = (b, b)\mathsf{e}$, $b = (a, b)\mathsf{e}$ ou bien $b = (a, a)\mathsf{e}$.

Dans le premier cas, $b^2 = (b^2, b^2)$ donc b est d'ordre 2. Comme $a^2 = (a^2, b^2)$, a aussi est d'ordre deux. La relation $a^{-1}b = (a^{-1}b, 1)\mathsf{e}$ et $(a^{-1}b)^2 = (a^{-1}b, a^{-1}b)$ implique que $a^{-1}b$ est d'ordre infini. Donc il s'agit du groupe diédral infini $\mathbb{D}_\infty$.

Le second cas correspond au groupe d'allumeur de réverbères (voir la section suivante).

Le troisième cas peut être analysé d'une manière similaire.

1.8. Exemples importants

Dans les sections suivantes, on présente les exemples importants de groupes engendrés par les automates. Il s'agit du groupe d'allumeur de réverbères (qui peut être engendré par un automate à deux états), du groupe d'Aleshin, d'un groupe engendré par un automate à trois états et du groupe de Wilson.

Il existe d'autres groupes d'automates dont l'étude a été importante pour le développement de la théorie. Mentionnons ici le groupe de Fabrykowski-Gupta [**9**], le groupe de Sushchansky [**31**] et le groupe de Gupta-Sidki [**20**].

Pour une théorie générale des automates et des groupes d'automates, on peut consulter [**11**], [**22**] et [**34**].

2. LE GROUPE D'ALLUMEUR DE RÉVERBÈRES COMME GROUPE D'AUTOMATE

L'automate de la figure 2 engendre le groupe d'allumeur de réverbères [**15**]. Ce groupe peut être défini comme le produit en couronne $(\mathbb{Z}/2\mathbb{Z}\wr\mathbb{Z})$ ou comme le produit semi-direct $(\oplus_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z})\rtimes\mathbb{Z}$ avec l'action de $\mathbb{Z}$ sur $\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ par translation.

Soient a et b les générateurs du groupe d'allumeur de réverbères $(\oplus_{\mathbb{Z}}\mathbb{Z}/2\mathbb{Z})\rtimes\mathbb{Z}$ tels que $a=(f_a,g_a)$, $b=(f_b,g_b)$, où $g_a=g_b\in\mathbb{Z}$ est un générateur de $\mathbb{Z}$, $f_a\in\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ est l'identité et $f_b=(\ldots,0,0,1,0,0,\ldots)\in\oplus_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z})$ est tel que 1 soit en position 1. Il existe un isomorphisme entre ce groupe et le groupe engendré par l'automate de la figure 2, où a et b correspondent aux états de cet automate.

L'étude de ce groupe, et de son action sur l'arbre enraciné de degré 2 correspondant à l'automate, a permis de répondre à une question d'Atiyah.

2.1. Récurrence d'opérateurs

Soit maintenant G le groupe engendré par l'automate de la figure 2. On note $\partial T=E_0\sqcup E_1$ la partition du bord ∂T associée aux sous-arbres T_0 et T_1 issus de chacun des deux sommets du premier niveau. On a un isomorphisme $L^2(\partial T,\mu)\simeq L^2(E_0,\mu_0)\oplus L^2(E_1,\mu_1)$ où μ_i est la restriction de μ à E_i, ainsi qu'un isomorphisme $L^2(\partial T,\mu)\simeq L^2(E_i,\mu_i)$, pour $i=0,1$, provenant de $T\simeq T_i$.

On obtient ainsi un isomorphisme entre $\mathcal{H}$ et $\mathcal{H}\oplus\mathcal{H}$, où $\mathcal{H}$ est un espace de Hilbert de dimension infinie. Grâce à cet isomorphisme, les opérateurs $\pi(a)$, $\pi(b)$ (encore notés a et b, respectivement), où π est une représentation comme dans la section 1.3, satisfont les relations d'opérateurs suivantes :

$$a=\begin{pmatrix}0&a\\b&0\end{pmatrix},\quad b=\begin{pmatrix}a&0\\0&b\end{pmatrix}$$

qui correspondent aux relations de type produit en couronne : $a=(a,b)\mathsf{e}$ et $b=(a,b)$.

Soit π_n une représentation par permutations du groupe G provenant de l'action de G sur le niveau n de l'arbre associé et soit $\mathcal{H}_n$ l'espace des fonctions sur le n-ième niveau. Soient a_n et b_n les matrices correspondant aux générateurs pour la représentation π_n. Alors $a_0=b_0=1$ et

$$a_n=\begin{pmatrix}0&a_{n-1}\\b_{n-1}&0\end{pmatrix},\quad b_n=\begin{pmatrix}a_{n-1}&0\\0&b_{n-1}\end{pmatrix}\tag{1}$$

en tenant compte de l'isomorphisme naturel $\mathcal{H}_n\simeq\mathcal{H}_{n-1}\oplus\mathcal{H}_{n-1}$.

2.2. Le groupe d'allumeur de réverbères et sa mesure spectrale

On s'intéresse au spectre et à la mesure spectrale correspondant à l'opérateur de Markov pour le groupe d'allumeur de réverbères.

Pour une partie génératrice S finie et symétrique ($S = S^{-1}$), on considère la marche aléatoire simple sur le graphe de Cayley $\mathrm{Cay}(G, S)$. Alors l'opérateur de marche aléatoire $A : \ell^2(G) \to \ell^2(G)$ est défini par

$$Af(g) = \frac{1}{|S|} \sum_{s \in S} f(sg),$$

où $f \in \ell^2(G)$ et $g \in G$.

Comme l'opérateur A est borné (on a $\|A\| \leq 1$) et auto-adjoint, il admet une décomposition spectrale

$$A = \int_{-1}^{1} \lambda \mathrm{d}E(\lambda),$$

où E est une mesure spectrale. Cette mesure est définie sur les sous-ensembles boréliens de l'intervalle $[-1, 1]$ et est à valeurs dans l'espace des projecteurs de l'espace de Hilbert $\ell^2(G)$. La mesure spectrale de Kesten μ sur l'intervalle $[-1, 1]$ est définie par

$$\mu(B) = \langle E(B)\delta_{\mathrm{Id}}, \delta_{\mathrm{Id}} \rangle,$$

où B est un sous-ensemble borélien de $[-1, 1]$ et $\delta_{\mathrm{Id}} \in \ell^2(G)$ est une fonction égale à 1 sur l'élément neutre et à 0 ailleurs.

Pour un sous-espace fermé et G-invariant H de $\ell^2(G)$, on définit sa dimension de von Neumann $\dim(H)$ comme étant

$$\dim(H) = \langle \mathrm{Pr}(H)\delta_{\mathrm{Id}}, \delta_{\mathrm{Id}} \rangle,$$

où $\mathrm{Pr}(H)$ est une projection de $\ell^2(G)$ sur H.

Pour le groupe d'allumeur de réverbères, on peut expliciter cette mesure **[15]** :

THÉORÈME 2.1. — *Soit G le groupe défini par l'automate de la figure 2, de générateurs a et b. L'opérateur de marche aléatoire A sur $\ell^2(G)$ possède les valeurs propres suivantes :*

$$\cos\left(\frac{l}{q}\pi\right)$$

où $q = 2, 3, 4, \ldots$ et $l = 1, \ldots, q-1$.

La dimension de von Neumann du sous-espace propre correspondant est égale à

$$\dim\left(\ker\left(A - \cos\left(\frac{l}{q}\pi\right)\right)\right) = \frac{1}{2^q - 1}$$

où $(l, q) = 1$.

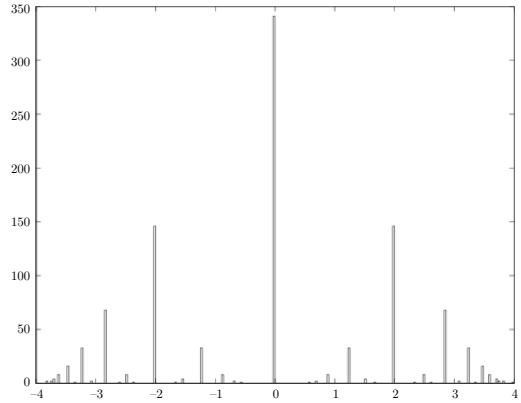

FIGURE 3. L'histogramme du spectre de $a_n + a_n^{-1} + b_n + b_n^{-1}$ pour $n = 10$

Pour démontrer ce théorème, on utilise les approximations de dimension finie π_n décrites précédemment.

Le calcul de la mesure spectrale a plusieurs applications aux marches aléatoires. Dans la section suivante, on présente une application de ce calcul à la conjecture d'Atiyah sur les nombres de Betti L^2 de variétés fermées.

2.3. Une question d'Atiyah

En 1976, Atiyah [**2**] a défini les nombres de Betti L^2 des variétés fermées. Il a conclu son article par une question concernant les valeurs de ces nombres. Plus tard cette question a donné lieu à une conjecture, dite d'Atiyah.

Pour un groupe Γ on note $\mathrm{fin}^{-1}(\Gamma)$ le sous-groupe de $\mathbb{Q}$ engendré par les inverses des ordres des sous-groupes finis de Γ. Pour une variété fermée M, on désigne par $b_i^{(2)}(M)$ son i-ième nombre de Betti L^2.

Conjecture. — *Soit M une variété fermée dont le groupe fondamental $\pi_1(M)$ est isomorphe à Γ. Alors on a*

$$b_i^{(2)}(M) \in \mathrm{fin}^{-1}(\Gamma)$$

pour tout nombre entier i.

Il existe plusieurs textes présentant les résultats obtenus sur cette conjecture, le plus récent étant un livre de Lück [**23**]. Plusieurs résultats confirment différentes formes de la conjecture d'Atiyah. On montre cependant que la version forte formulée ici est fausse [**14**].

THÉORÈME 2.2. — *Soit G le groupe donné par la présentation*

$$G = \langle a, t, s \mid a^2 = 1, [t, s] = 1, [t^{-1}at, a] = 1, s^{-1}as = at^{-1}at \rangle.$$

Chaque sous-groupe fini de G est un 2-groupe abélien élémentaire, en particulier l'ordre de chaque sous-groupe fini de G est une puissance de 2. Il existe une variété riemannienne fermée (M, g) de dimension 7 telle que $\pi_1(M) = G$ pour laquelle le troisième nombre de Betti L^2 est égal à

$$b_3^{(2)}(M, g) = \frac{1}{3}.$$

La preuve du théorème 2.2 repose sur les résultats décrits précédemment, sur le spectre et la mesure spectrale de l'opérateur de Markov A de la marche aléatoire simple sur le groupe de l'allumeur de réverbères, dont G est une extension HNN. Les résultats impliquent que

$$\dim\big(\ker(A)\big) = \frac{1}{3},$$

mais le dénominateur 3 ne divise pas les puissances de 2, qui sont les ordres des sous-groupes finis du groupe de l'allumeur de réverbères.

La conjecture d'Atiyah peut être formulée d'une manière équivalente en termes de dimension de sous-espaces propres des opérateurs dans $\mathbb{Z}[G]$ agissant sur $\ell^2(G)$ où $G = \pi_1(M)$. Si G est un groupe de présentation finie et A un opérateur de marche aléatoire sur G, il existe une construction d'une variété fermée M dont le groupe fondamental est G et telle que le troisième nombre de Betti L^2 de M soit égal à la dimension de von Neumann du noyau de l'opérateur A. Le groupe d'allumeur de réverbères n'est pas de présentation finie.

3. LE GROUPE D'ALESHIN

Considérons l'automate fini inversible représenté par la figure 4. Le groupe d'Aleshin [**1**] est le groupe G engendré par U et V.

Son étude a permis de donner une réponse particulièrement simple au problème de Burnside et de résoudre un problème de Milnor.

3.1. Une réponse au problème de Burnside

En 1902, Burnside a demandé s'il existe des groupes de type fini qui sont infinis et tels que chaque élément soit d'ordre fini. Le résultat le plus important concernant l'existence de tels groupes est le théorème d'Adyan-Novikov [**28**]. Le groupe d'Aleshin donne une réponse très simple à ce problème même si, contrairement aux groupes d'Adyan-Novikov, l'ordre des éléments n'est pas uniformément borné. Aleshin [**1**] démontre :

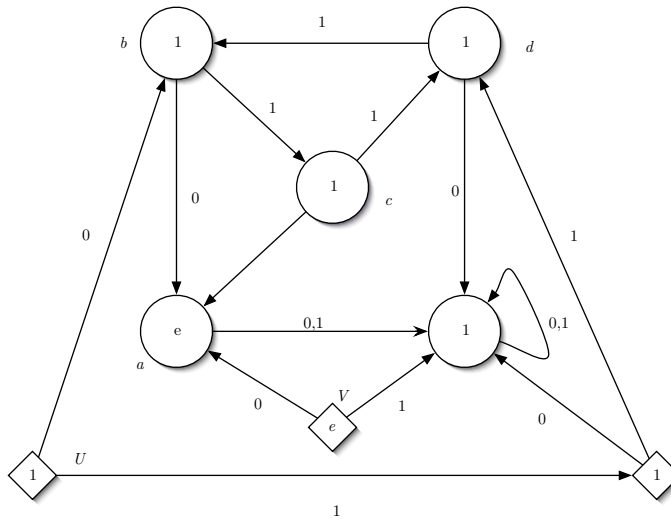

FIGURE 4. L'automate d'Aleshin de 1972

THÉORÈME 3.1. — *Le groupe $G = \langle U, V\rangle$ est de torsion et infini.*

Bien qu'il y ait des preuves plus directes de ce théorème, nous présentons la démonstration originale car elle permet la construction d'une quantité non dénombrable de p-groupes infinis pour tout nombre premier p.

Le groupe d'Aleshin est par définition de type fini. Les prochaines sous-sections donnent la preuve des deux assertions du théorème.

Préliminaires. —

Soit A un automate fini, δ un mot et q un état de $\Gamma(A)$. On note $q[\delta]$ la permutation que porte le sommet d'arrivée du chemin de $\Gamma(A)$ partant de q et suivant δ.

On constate :

PROPOSITION 3.2. — *Soit δ un mot de longueur l.*

i) *si $l \geq 3$, alors $V[\delta] = \mathrm{Id}$;*
ii) *si $U[\delta] = \mathsf{e}$, alors $l \geq 3$ et δ est de la forme $\xi, 1, 1, ..., 1, 0$ avec $\xi \in \{0, 1\}$;*
iii) *plus précisément,*

$m = 011...10$, $U[m] = \mathsf{e}$ si et seulement si m est de longueur $l \equiv 0$ ou 2 modulo 3

$m = 111...10$, $U[m] = \mathsf{e}$ si et seulement si m est de longueur $l \equiv 1$ ou 2 modulo 3.

LEMME 3.3. — *Les générateurs sont d'ordre fini* :

i) *U est d'ordre 2.*

ii) *V est d'ordre 4 et agit transitivement sur les 2 premières lettres des suites de $\{0,1\}$ et uniquement celles-ci.*

Preuve. — i) Soit δ un mot. Le second point de la proposition précédente indique que seule la lettre suivant un éventuel préfixe de δ de la forme $\xi, 0, 0, ..., 0, 1$ pourra être modifiée sous l'action de U. Il en va de même pour l'action de U sur la suite $U(\delta)$ et donc $U^2(\delta) = \delta$.

ii) Utilisons l'image de V dans le produit en couronne : $V = (\mathrm{Id}, a)\mathtt{e}$. Donc $V^2 = (a, a)$. Or $a = (\mathrm{Id}, \mathrm{Id})\mathtt{e}$ et donc $a^2 = (\mathrm{Id}, \mathrm{Id}) = \mathrm{Id}, a \neq \mathrm{Id}$. Finalement, V est exactement d'ordre 4.

Comme il n'y que 4 mots à 2 lettres, V agit bien transitivement sur les mots à 2 lettres. Le premier point de la proposition 3.2 achève la preuve de ce lemme.

Puisque U et V sont d'ordre fini, tout élément de G s'écrit $X = X_m X_{m-1} \dots X_1$, $X_i = U$ ou V. Pour tout mot δ, on note alors

$$X[\delta] = X_m[X_{m-1} \dots X_1(\delta)].$$

Nous allons associer à tout élément $X = X_m ... X_1 \in G$, avec $X_i = U$ ou V, une fonction

$$R_X : \{\text{mots de longueur } l \geq 3\} \longrightarrow \mathbb{N}\,.$$

Soit donc δ un mot de longueur $l \geq 3$. Soit d le plus petit entier tel que $X^d(\delta) = \delta$ (il existe car l'ensemble $\{X^i(\delta),\ i \in \mathbb{N}\}$ est fini).

On pose $\Gamma^1(X, \delta) = \delta_0^1, \delta_1^1, \dots, \delta_{m-1}^1, \delta_0^2, \dots, \delta_{m-1}^2, \dots, \delta_{m-1}^d$ avec pour $j \in \{0, ..., m-2\}$ et pour $i \in \{1, ..., d-1\}$

$$\delta_0^1 = \delta, \qquad \delta_{j+1}^i = X_{j+1}(\delta_j^i), \qquad \delta_0^{i+1} = X_m(\delta_{m-1}^i).$$

On note $\Gamma^2(X, \delta)$ la sous-suite de $\Gamma^1(X, \delta)$ qui consiste en les δ_j^i vérifiant

- $X_{j+1} = U$ (les mots δ_j^i en entrée de l'opérateur U)
- δ_j^i est de la forme $\xi, 1, 1, ..., 1, \nu$ avec ξ et ν égaux à 0 ou 1.

Dans cette suite, on remplace chaque δ_j^i par 0 s'il finit par 0 et par 1 sinon. On obtient ainsi une suite de la forme

$$0^{s_1^0} 1^{s_1^1} 0^{s_2^0} ... 1^{s_k^1}$$

avec $s_l^m > 0$ sauf peut-être pour s_1^0 ou s_k^1.
On remplace maintenant, pour $x = 0$ ou 1, chaque $x^{s_l^x}$ par x (la suite obtenue commence par 0 si $s_1^0 > 0$ et par 1 sinon ; de même, elle finit par 1 si et seulement si $s_k^1 > 0$).

Cette suite est notée $\Gamma^3(X, \delta)$.

DÉFINITION 3.4. — *On pose*

$$R_X(\delta) = \begin{cases} \max(k_0, k_1) & \text{si } k_0 \text{ et } k_1 \text{ sont non nuls} \\ 0 & \text{sinon} \end{cases}$$

où k_0 et k_1 sont respectivement le nombre de 0 et de 1 dans $\Gamma^3(X, \delta)$.

$R_X(\delta)$ est en fait le nombre d'alternances dans la suite $\Gamma^3(X, \delta)$.

Le groupe G est de torsion. —

Soit $X = X_m...X_1 \in G$. Il nous faut montrer l'existence de D tel que $X^D = 1$.

LEMME 3.5. — *Soit δ un mot de longueur $l \geq 3$ et d tel que $X^d(\delta) = \delta$.*

Si $R_X(\delta) = 0$, alors pour tout mot η, $X^{2d}(\delta\eta) = \delta\eta$.

Preuve. — Supposons que $R_X(\delta) = 0$. On distingue alors 3 cas :

1. $\Gamma^3(X, \delta) = \varnothing$.

Dans ce cas, la suite $\Gamma^1(X, \delta)$ ne possède pas de mot de la forme $\xi 11...0$ et donc, d'après la proposition 3.2, pour toute lettre x, on a $X^d(\delta x) = \delta x$. Comme $\Gamma^1(X, \delta)$ ne contient pas non plus de mot de la forme $\xi 11...1$, $\Gamma^3(X, \delta x) = \varnothing$ et ce premier cas est traité.

2. $\Gamma^3(X, \delta) = 0$.

Étant donné une lettre x, on a toujours $X^{2d}(\delta x) = X^{2d}(\delta)(X^d[\delta])^2(x) = \delta x$ (car $\mathrm{Id}^2 = \mathsf{e}^2 = \mathrm{Id}$). De plus, par hypothèse, la suite $\Gamma^1(X, \delta)$ ne contient pas de mots de la forme $\xi 11...1$ et ainsi la suite $\Gamma^3(X, \delta x)$ est vide : on est ramené au premier cas.

3. $\Gamma^3(X, \delta) = 1$.

On a $X^d[\delta] = \mathrm{Id}$ et donc, pour tout x, $X^d(\delta x) = \delta x$. De plus, $\Gamma^1(X, \delta x)$ est alors obtenu en ajoutant x à la fin de chaque mot de $\Gamma^1(X, \delta)$ et donc $\Gamma^3(X, \delta x)$ est égal à :

i) 0 si et seulement si $x = 0$. On est ramené au deuxième cas et donc, pour tout η, $X^{2d}(\delta x\eta) = \delta x\eta$.

ii) 1 sinon. On applique le raisonnement du troisième point à δx, jusqu'à ce que l'on soit dans le cas i) précédent.

LEMME 3.6. — *La fonction R_X est décroissante pour l'ordre partiel habituel sur les mots,* i.e.

$$R_X(\delta x) \leq R_X(\delta).$$

De plus, si d est le plus petit entier vérifiant $X^d(\delta) = \delta$, alors

$$X^d[\delta] = \mathrm{Id} \text{ et } R_X(\delta) > 0 \text{ implique } R_X(\delta x) < R_X(\delta).$$

Preuve. — Le cas $R_X(\delta) = 0$ a été traité dans la preuve du lemme précédent. On suppose donc $R_X(\delta) > 0$.

i) Cas $X^d[\delta] = \mathrm{Id}$. La suite $\Gamma^1(X, \delta x)$ est donc aussi de longueur md. De plus, les mots de la suite $\Gamma^2(X, \delta x)$ proviennent des mots de $\Gamma^2(X, \delta)$ de la forme $\xi 11...1$ et le nombre d'alternances entre les mots de $\Gamma^2(X, \delta x)$ finissant par 0 et ceux finissant par 1 est inférieur au nombre de 0 dans $\Gamma^3(X, \delta)$ (car seul un mot de la forme $\xi 11...0$ de $\Gamma^2(X, \delta)$ peut générer la permutation e). Finalement les nombres de 0 et de 1 dans la suite $\Gamma^3(X, \delta x)$ sont strictement plus petits que le maximum des nombres de 0 et de 1 dans $\Gamma^3(X, \delta)$: on a bien $R_X(\delta x) < R_X(\delta)$.

ii) Cas $X^d[\delta] = \mathsf{e}$. Ici la suite $\Gamma^1(X, \delta x)$ est de longueur $2md$. Si on note $\Gamma^1(X, \delta) = \delta_0^1, \delta_1^1, ..., \delta_{m-1}^1, \delta_0^2, ..., \delta_{m-1}^2, ...\delta_{m-1}^d$, alors $\Gamma^1(X, \delta x) =$

$$\begin{pmatrix} \delta_0^1 x & \delta_1^1 x_1^1 & ... & \delta_{m-1}^1 x_{m-1}^1 & \delta_0^2 x_0^2 & ... & \delta_{m-1}^2 x_{m-1}^2 & .... & \delta_{m-1}^d x_{m-1}^d \\ \delta_0^1 \mathsf{e}(x) & \delta_1^1 \mathsf{e}(x_1^1) & ... & \delta_{m-1}^1 \mathsf{e}(x_{m-1}^1) & \delta_0^2 \mathsf{e}(x_0^2) & ... & \delta_{m-1}^2 \mathsf{e}(x_{m-1}^2) & .... & \delta_{m-1}^d \mathsf{e}(x_{m-1}^d) \end{pmatrix}.$$

En raisonnant comme dans le premier cas, on voit que les mots de la suite $\Gamma^2(X, \delta x)$ proviennent des mots de $\Gamma^2(X, \delta)$ de la forme $\xi 11...1$ mais, cette fois-ci, sur les deux copies de $\Gamma^1(X, \delta)$ correspondant aux deux lignes de la matrice ci-dessus. Donc la longueur de la suite $\Gamma^3(X, \delta x)$ n'est pas plus grande que deux fois le nombre de 1 dans $\Gamma^3(X, \delta)$, ce nombre étant lui-même $\leq R_X(\delta)$. On remarque de plus que dans $\Gamma^2(X, \delta x)$ on a autant de mots finissant par 0 que de mots finissant par 1. On a bien $R_X(\delta x) \leq R_X(\delta)$.

LEMME 3.7. — *Soit δ un mot de longueur $l \geq 2$. Alors $R_X(\delta) = R_X(X(\delta))$.*

Preuve. — Il faut juste remarquer que la suite $\Gamma^1(X, X(\delta))$ est obtenue en mettant les m premiers mots de $\Gamma^1(X, \delta)$ à sa fin.

LEMME 3.8. — *Il existe $t_X \geq 3$ tel que pour tout δ mot de longueur $l \geq t_X$ et toute suite (finie ou infinie) η*

$$R_X(\delta) = R_X(\delta\eta).$$

Preuve. — L'élément X agit sur l'ensemble des mots à 3 lettres. Considérons alors une orbite B à laquelle nous pouvons d'après le lemme précédent associer un entier $R_X(B) = R_X(\delta)$, pour tout $\delta \in B$. Supposons ce nombre non nul.

Regardons alors l'ensemble B'^1 des mots de 4 lettres dont les 3 premières forment un mot de B. Soit $\eta x \in B'^1$, $\eta \in B$, $x = 0$ ou 1. Son orbite est nécessairement incluse dans B'^1 et deux cas se distinguent alors :

1. $X[\eta] = \mathsf{e}$ et dans ce cas l'orbite de ηx est B'^1.

2. $X[\eta] = \mathrm{Id}$ et dans ce cas B'^1 est la réunion disjointe $B_1^1 \sqcup B_2^1$ de deux orbites sur les mots à 4 lettres. Mais ici, d'après le lemme 3.6, $R_X(B_1^1)$ et $R_X(B_2^1)$ sont strictement inférieurs à $R_X(B)$.

Les descendants de B sont donc réunis en « blocs » B_q^p (correspondant à certaines orbites) que l'on peut représenter par les sommets d'un arbre enraciné tel que chaque sommet possède 1 ou 2 fils ; à chacun de ces blocs est associé un nombre $R_X(B_q^p)$ qui est strictement plus petit que celui du père de B_q^p si celui-ci a deux fils.

Le nombre de sommets ayant deux fils est donc nécessairement fini et il existe un niveau p tel que, pour tout bloc B_q^p, les blocs fils de B_q^p aient tous la même étiquette $R_X(B_q^p)$.

La preuve est achevée une fois remarqué qu'il n'existe qu'un nombre fini d'orbites B sur l'ensemble des mots à 3 lettres.

Nous allons maintenant montrer que, pour tout δ de longueur au moins t_X, $R_X(\delta) = 0$.

DÉFINITION 3.9. — *Soit δ un mot de longueur $l \geq 3$. Notons a_ξ le nombre d'occurrences du mot $\xi 11...10$ dans $\Gamma^2(X, \delta)$. Soit $\mathcal{A}$ un sous-alphabet de $\{0, 1\}$. On dit que $\Gamma^2(X, \delta)$ admet le type $\mathcal{A}$ si $\sum_{\xi \in \mathcal{A}} a_\xi$ est pair.*

Remarque 3.10. — Soit un des a_ξ est pair, soit c'est leur somme et donc $\Gamma^2(X, \delta)$ admet au moins un type.

LEMME 3.11. — *Supposons l'existence d'un mot δ et de deux lettres x_1 et x_2 tels que*

$$R_X(\delta) = R_X(\delta x_1) = R_X(\delta x_1 x_2) \neq 0.$$

Alors les suites $\Gamma^2(X, \delta x_1)$ et $\Gamma^2(X, \delta x_1 x_2)$ admettent les mêmes types.

Preuve. — Nécessairement, $X[\delta] = \mathsf{e}$. La preuve du lemme 3.6 indique alors que, si la suite $\Gamma^2(X, \delta x_1)$ contient le mot $\eta 0$, elle contient aussi le mot $\eta 1$ et donc les a_ξ de $\Gamma^2(X, \delta x_1)$ peuvent se lire aussi sur les mots de la forme $\xi 11...11$, lesquels vont donner les mots définissant les types de $\Gamma^2(X, \delta x_1 x_2)$.
En effet, $X[\delta x_1] = \mathsf{e}$ et l'ensemble des mots de $\Gamma^2(X, \delta x_1 x_2)$ de la forme $\xi 11...10$ est en bijection avec l'ensemble des mots de la forme $\xi 11...11$ (on modifie la dernière lettre), eux-mêmes en bijection avec l'ensemble des mots de la forme $\xi 11...1$ dans $\Gamma^2(X, \delta x_1)$ (on ôte la dernière lettre).
Ainsi les valeurs des a_ξ sont identiques dans $\Gamma^2(X, \delta x_1)$ et dans $\Gamma^2(X, \delta x_1 x_2)$ et le lemme est prouvé.

LEMME 3.12. — *Soit δ de longueur t_X. Alors $R_X(\delta) = 0$.*

Preuve. — Raisonnons par l'absurde. Nous sommes alors dans les conditions du lemme précédent et les types admis par les suites $\Gamma^2(X, \delta x_1)$, $\Gamma^2(X, \delta x_1 x_2)$,...,$\Gamma^2(X, \delta x_1 x_2 ... x_k)$ sont les mêmes. Soit donc $\mathcal{A}$ un tel type (qui existe grâce à la remarque 3.10). Il résulte du dernier point de la proposition 3.2 qu'il existe une longueur $l > t_X$ telle que les mots η de longueur l vérifiant $U[\eta] = \mathsf{e}$ soient exactement ceux de la forme

$\xi 11...10$ pour $\xi \in \mathcal{A}$. Mais alors pour le mot $m = \delta 11...1$ de longueur l et d tel que $X^d(m) = m$,

$$X^d[m] = \mathrm{e}^{\sum_{\xi \in \mathcal{A}} a_\xi} = \mathrm{Id}$$

et donc $R_X(m1) < R_X(m)$ ce qui contredit la propriété de t_X.

Soit maintenant

$$D = \mathrm{ppcm}\{\text{cardinal de l'orbite de } \delta | \delta \text{ de longueur } t_X\}.$$

Par définition de D, pour tout mot η de longueur au plus t_X, $X^{2D}(\eta) = \eta$. D'après le lemme précédent, pour tout mot η de longueur t_X, on a $R_X(\eta) = 0$ et donc pour toute suite γ finie ou infinie, $X^{2D}(\eta\gamma) = \eta\gamma$ (lemme 3.5). Finalement, $X^{2D} = 1$ et donc le groupe G est de torsion.

G est infini. —

LEMME 3.13. — *Pour tout $k \geq 0$, pour tout $\xi \in \{0,1\}$, il existe $X_{k,\xi} \in G$ et il existe $x_1, x_2, y_1, y_2 \in \{0,1\}$ tels que, pour tout mot γ, on ait*

$$X_{k,\xi}(x_1 x_2 \underbrace{0...0}_{k} \xi\gamma) = y_1 y_2 \underbrace{0...0}_{k+1} \gamma.$$

Preuve. — Par récurrence sur k.

Pour $k = 0$. On voit que $U^d(00\xi\gamma) = 00\mathrm{e}^d(\xi)\gamma$. Ici, $(x_1, x_2, y_1, y_2) = (0,0,0,0)$ convient. $X_{0,0} = \mathrm{Id}$ et $X_{0,1} = U$.

Supposons le résultat vrai pour tout $k \leq K$. Nous partons de $x_1 x_2 \underbrace{0...0}_{K+1} \xi\gamma$ et allons essayer d'arriver à $y_1 y_2 \underbrace{0...0}_{K+2} \gamma$.

Tout d'abord, une remarque : le lemme 3.3 nous indique que, en utilisant une puissance appropriée de V, on peut faire apparaître les deux premières lettres que l'on souhaite sur n'importe quel mot, sans modifier le reste de celui-ci. Cela est notamment utile pour utiliser les $X_{k,\xi}$ sur des mots dont les deux premières lettres ne sont pas celles requises par les hypothèses de récurrence.

Par hypothèse de récurrence, il existe $X_{K-1,1}$ tel que

$$X_{K-1,1}^{-1}(y_1' y_2' \underbrace{0...0}_{K} 0\gamma') = x_1' x_2' \underbrace{0...0}_{K-1} 10\gamma'.$$

On pose $\gamma' = \xi\gamma$ et on utilise une bonne puissance de V ; on obtient ainsi l'existence de T_1 tel que :

$$T_1(x_1 x_2 \underbrace{0...0}_{K+1} \xi\gamma) = x_1' x_2' \underbrace{0...0}_{K-1} 10\xi\gamma.$$

On itère ce procédé en utilisant successivement $X_{K-2,1}^{-1}$, $X_{K-3,1}^{-1}$,...,$X_{0,1}^{-1}$ et les bonnes puissances de V pour enfin obtenir un élément T_K vérifiant :

$$T_K(x_1x_2\underbrace{0...0}_{K+1}\xi\gamma) = y_1y_2\underbrace{1...1}_{K}0\xi\gamma.$$

D'après le dernier point de la proposition 3.2, il existe $\sigma \in \{0,1\}$ tel que $U[\sigma\underbrace{11..1}_{K+1}0] = \mathtt{e}$. On pose alors

$$T = UV^iT_K \text{ où } i \text{ est tel que } V^i(y_1y_2) = \sigma 1.$$

Cet élément vérifie

$$T(x_1x_2\underbrace{0...0}_{K+1}\xi\gamma) = \sigma\underbrace{1...1}_{K+1}00\gamma.$$

Maintenant on utilise successivement $X_{0,1}$, $X_{1,1}$,...,$X_{K-1,1}$ et les puissances appropriées de V pour, à chaque étape, faire apparaître les deux premières lettres requises à l'utilisation de $X_{i,1}$. On obtient alors la suite d'égalités

$$\begin{aligned}
T_1'(x_1x_2\underbrace{0...0}_{K+1}\xi\gamma) &= **0\underbrace{1.....1}_{K-1}00\gamma\\
T_2'(x_1x_2\underbrace{0...0}_{K+1}\xi\gamma) &= **00\underbrace{1..1}_{K-2}00\gamma\\
&\vdots\\
T_K'(x_1x_2\underbrace{0...0}_{K+1}\xi\gamma) &= **\underbrace{0.....0}_{K+2}\gamma
\end{aligned}$$

ce qui achève la preuve de l'hérédité et donc celle du lemme.

Le lemme précédent exhibe alors pour tout $k \in \mathbb{N}$ des éléments Z_k de G vérifiant

$$Z_k(\underbrace{1...1}_{k}111...) = \underbrace{0...0}_{k}111...$$

(on utilise les $X_{k,1}$ multipliés à droite et à gauche par des puissances adéquates de V).

Ces Z_k sont tous distincts et donc le groupe G est infini.

On remercie Jean-François Planchat qui nous a expliqué la preuve d'Aleshin [**29**].

3.2. Croissance

Pour un groupe G engendré par une partie S, finie et symétrique (i.e. telle que $S = S^{-1}$), on note $|g|_S$ le nombre minimal de générateurs requis pour représenter g. La croissance du groupe G décrit le comportement asymptotique de la fonction

$$b_G(n) = |\{g \in G : |g|_S \leq n\}|.$$

Ce type de croissance est indépendant de la partie génératrice. Par exemple, pour les groupes nilpotents, elle est polynomiale et, pour un groupe qui contient un sous-groupe ou même un semi-groupe libre, elle est exponentielle. Pour l'histoire de cette notion, voir [**18**]. Dans [**25**] il a été demandé s'il existe d'autres types de croissance. On présente la réponse donnée par Grigorchuk dans [**13**].

Soit G le groupe engendré par les états a, b, c et d de l'automate de la figure 4. Il est facile de voir que ce groupe est commensurable au groupe engendré par les états U et V et au groupe engendré par tous les états de cet automate (i.e. ces groupes ont des sous-groupes d'indice fini isomorphes).

PROPOSITION 3.14. — *Le groupe G n'est pas à croissance polynomiale.*

Preuve. — Un groupe à croissance polynomiale contient un sous-groupe d'indice fini nilpotent (Gromov) qui contient un sous-groupe d'indice fini sans torsion (Malcev). Or le théorème d'Aleshin (voir la section précédente) affirme que G est infini de torsion. On peut aussi vérifier cette proposition par un calcul simple.

Montrons que le groupe d'Aleshin est à croissance sous-exponentielle.

Nous avons les relations :

$$a = (1,1)\mathsf{e}$$

$$\begin{aligned} b &= (a,c) \\ c &= (a,d) \\ d &= (1,b) \end{aligned} \tag{2}$$

et aussi

$$\begin{aligned} aba &= (c,a) \\ aca &= (d,a) \\ ada &= (b,1). \end{aligned} \tag{3}$$

LEMME 3.15. — *Le groupe engendré par b, c et d est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Preuve. — Il s'agit d'une vérification simple.

Soit $\Gamma = \mathrm{St}_G(3)$. Alors $[G : \Gamma] < \infty$.

LEMME 3.16. — *Considérons pour $g \in \Gamma$ son image dans G^8 ; on note $g = (g_1, \dots, g_8)$. Alors*

$$\sum_{i=1}^{8} |g_i| \leq \frac{3}{4}|g| + 8, \tag{4}$$

pour la longueur par rapport aux générateurs a, b, c et d.

Preuve. — Sachant que a est d'ordre 2 et que b, c et d sont les éléments du groupe de Klein, chaque élément $g \in G$ s'écrit :

$$g = \overline{a}k_1ak_2a \dots ak_n\overline{a},$$

où $k_i \in \{b, c, d\}$ et le premier et le dernier a, notés $\overline{a}$, n'apparaissent pas forcément.

Considérons un bloc $\gamma = k_iak_{i+1}a$ ou $\gamma = ak_iak_{i+1}$. Grâce aux relations (2) et (3) son image $\gamma = (\gamma_1, \gamma_2)$ dans $G \times G$ vérifie

$$|\gamma_1| + |\gamma_2| \leq |\gamma|.$$

Si k_i ou k_{i+1} est égal à d, cette inégalité devient

$$|\gamma_1| + |\gamma_2| \leq \frac{3}{4}|\gamma|. \tag{5}$$

Les relations (2) et (3) montrent que l'image de k_i ou ak_ia dans $G \times G$ donne c si $k_i = b$ et donne d si $k_i = c$. Donc en itérant cette procédure 3 fois, on est sûr de se retrouver dans la situation (5). D'où l'inégalité (4) (le terme 8 est dû au fait que la longueur de $|g|$ n'est pas forcément divisible par 8).

PROPOSITION 3.17. — *Le groupe d'Aleshin est à croissance sous-exponentielle.*

Preuve. — L'inégalité (4) nous montre que

$$|b_\Gamma(k)| \leq \sum_{k_1+\dots+k_8 \leq \frac{3}{4}k+8} |b_G(k_1)| \times \dots \times |b_G(k_8)|. \tag{6}$$

Il est important de calculer la longueur des éléments par rapport aux générateurs a, b, c et d même si a n'appartient pas à Γ. Comme Γ est d'indice fini dans G, on a

$$\lim_{n\to\infty} \sqrt[n]{|b_G(n)|} = \lim_{n\to\infty} \sqrt[n]{|b_\Gamma(n)|} = \alpha. \tag{7}$$

Pour chaque $\varepsilon > 0$, il existe $c > 0$ tel que, pour n suffisamment grand, on ait

$$|b_G(n)| \leq c(\alpha + \varepsilon)^n.$$

La majoration (6) assure alors qu'il existe c' tel que

$$|b_\Gamma(n)| \leq c'n^8(\alpha + \varepsilon)^{\frac{3}{4}n+8}.$$

Donc $\lim_{n\to\infty} \sqrt[n]{|b_\Gamma(n)|} \leq \alpha^{\frac{3}{4}}$ ce qui, avec (7), implique

$$\lim_{n\to\infty} \sqrt[n]{|b_G(n)|} = 1.$$

Le groupe d'Aleshin est donc à croissance sous-exponentielle.

On ne connaît pas le comportement exact de la fonction de croissance du groupe d'Aleshin. Pour de meilleures estimations, voir **[5]**.

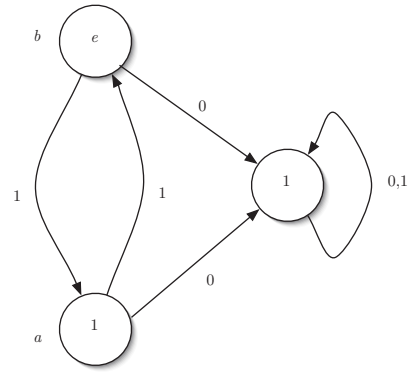

FIGURE 5. L'automate à trois états

4. GROUPE ENGENDRÉ PAR UN AUTOMATE À TROIS ÉTATS

On s'intéresse au groupe engendré par l'automate de la figure 5 introduit dans [**16**]. Ce groupe apparaît aussi comme le groupe de Galois des itérations du polynôme $x^2 - 1$ sur les corps finis (Pink) et comme le groupe de monodromie du revêtement ramifié de la sphère de Riemann donné par le polynôme $z^2 - 1$ (voir [**26**]).

Une des propriétés les plus remarquables de ce groupe est liée à la notion de moyennabilité.

4.1. Propriétés algébriques de G

THÉORÈME 4.1 ([**16**]). — *Soit G le groupe engendré par l'automate de la figure* 5.
Le groupe G possède les propriétés suivantes.

a) *Il est fractal*;
b) *il est régulièrement faiblement branché sur G'*;
c) *il est sans torsion*;
d) *le semi-groupe engendré par a et b est libre*;
e) *il admet la présentation :*

$$G = \langle a, b | \sigma^\varepsilon(\theta^m([a, a^b])) = 1, m = 0, 1, \ldots, \varepsilon = 0, 1 \rangle,$$

où

$$\sigma : \begin{cases} a & \mapsto & b^2 \\ b & \mapsto & a \end{cases} \qquad \theta : \begin{cases} a & \mapsto & a^{b^2+1} \\ b & \mapsto & b. \end{cases}$$

On présente ici les démonstrations de quelques propriétés algébriques de G mentionnées dans le théorème 4.1.

Pour $G = \langle a, b \rangle$, on a les relations $a = (1, b)$ et $b = (1, a)\mathsf{e}$.

PROPOSITION 4.2. — *Le groupe G est fractal.*

Preuve. — Nous avons

$$\mathrm{St}_G(1) = \langle a, a^b, b^2 \rangle.$$

Mais

$$\begin{aligned} a &= (1, b) \\ a^b &= \mathsf{e}(1, a^{-1})(1, b)(1, a)\mathsf{e} = (b^a, 1) \\ b^2 &= (a, a), \end{aligned} \tag{8}$$

et chacune des images des deux projections de $\mathrm{St}_G(1)$ est G, i.e. G est fractal.

PROPOSITION 4.3. — *Le groupe G est régulièrement faiblement branché sur G', i.e.*

$$G' \geq G' \times G'.$$

Preuve. — En effet, comme

$$[a, b^2] = (1, [b, a]),$$

en utilisant la fractalité de G, on obtient $G' \geq \langle [a, b^2] \rangle^G \geq 1 \times \langle [b, a] \rangle^G = 1 \times G'$ et $(1 \times G')^b = G' \times 1$. Donc G' contient $G' \times G'$ et comme $G' \neq 1$ le groupe G est régulièrement faiblement branché sur G'.

LEMME 4.4. — *Le semi-groupe engendré par a et b est libre.*

Preuve. — Considérons deux mots différents $U(a, b)$ et $V(a, b)$ qui représentent le même élément et tels que $\rho = \max\{|U|, |V|\}$ soit minimal. Une vérification directe montre que ρ ne peut valoir ni 0 ni 1.

Supposons que $|U|_b$, le nombre d'occurrences de b dans U, est pair (et donc $|V|_b$ également). Si ce n'est pas le cas, on peut considérer les mots bU et bV augmentant ainsi ρ par 1.

Maintenant U et V sont les produits de

$$a^m = (1, b^m)$$

et de

$$ba^m b = (1, a)\mathsf{e}(1, b^m)(1, a)\mathsf{e} = (b^m a, a).$$

Si, dans un de ces mots, il n'y a pas b, disons $U = a^m$, après avoir projeté U et V sur la première coordonnée, on obtient $1 = V_0$ où la projection V_0 est un mot non vide vérifiant $|V_0| < |V| \leq \rho$. Ceci contredit la minimalité de U et V.

On considère maintenant la situation où b apparaît dans les deux mots au moins deux fois. Si le nombre d'occurrences de b dans U et V était un, alors par minimalité ils doivent être égaux à ba^n et $a^m b$. Mais $ba^n = (b^n, a)\mathsf{e}$ et $a^m b = (1, b^m a)\mathsf{e}$, ce qui montre que, si ces mots sont différents, ils représentent des éléments différents.

Donc les deux mots contiennent deux b et $|U|, |V| \leq \rho$, ou l'un d'entre eux contient au moins quatre b et $|U|, |V| \leq \rho + 1$.

Si on considère les projections de U et V sur la seconde coordonnée, on obtient deux mots différents (à cause de la minimalité de U et V, ils doivent finir avec des lettres différentes) et de longueur strictement plus petite. Ceci contredit la minimalité de ρ.

LEMME 4.5. — *Nous avons la relation suivante* :

$$\gamma_3(G) = (\gamma_3(G) \times \gamma_3(G)) \rtimes \langle [[a,b],b] \rangle$$

où $\gamma_3(G) = [[G,G],G]$.

Preuve. — On part des relations

$$\gamma_3(G) = \langle [[a,b],a], [[a,b],b] \rangle^G,$$

$$[[a,b],a] = [(b^a, b^{-1}), (1,b)] = 1,$$

$$[[a,b],b] = (b^{-a},b)\mathsf{e}(1,a^{-1})(b^a,b^{-1})(1,a)\mathsf{e} = (b^{-a},b)(b^{-a},b^a) = (b^{-2a}, bb^a). \tag{9}$$

Les deux premières nous permettent de conclure que

$$\gamma_3(G) = \langle [[a,b],b] \rangle^G.$$

Grâce à la relation

$$[a,b^2] = (1,[a,b])$$

on a

$$[[a,b^2],a] = [(1,[a,b]),(1,b)] = (1,[[a,b],b]).$$

Soit $\xi = [[a,b],b]$. Des calculs directs montrent que $\xi^a, \xi^{a^{-1}}, \xi^b, \xi^{b^{-1}} \in \langle \xi \rangle$ mod $\gamma_3(G) \times \gamma_3(G)$ et $\langle \xi \rangle \cap (\gamma_3(G) \times \gamma_3(G)) = 1$ à cause de (9) et du fait que $(bb^a)^n \in G'$ si et seulement si $n = 0$ et $\gamma_3(G) \leq G'$.

LEMME 4.6. — *On a la relation suivante* :

$$G'' = \gamma_3(G) \times \gamma_3(G).$$

Preuve. — Soit $f = (1,c) \in G$ où $c = [a,b]$. On a pour $d = (b, b^{-1}) \in G'$

$$[f, d^{-1}] = [(1,[a,b]), (b^{-1},b)] = (1,[[a,b],b]) \in G''.$$

Ceci implique que $G'' \supseteq 1 \times \gamma_3(G)$ et alors $G'' \supseteq \gamma_3(G) \times \gamma_3(G)$. Comme $G'' \subseteq \gamma_3(G)$, d'après le lemme 4.5, il suffit de démontrer que $\langle \xi \rangle \cap G'' = 1$.

Il est facile de démontrer que

$$G' = (G' \times G') \rtimes \langle c \rangle. \tag{10}$$

En utilisant la relation (9) et la relation (10), on a

$$G'' = \langle [c, f] \rangle^G.$$

Mais

$$[c, f] = [(b^a, b^{-1}), (1, c)] = [1, [b^{-1}, [a, b]]] \in 1 \times \gamma_3(G).$$

Cela finit la démonstration.

Voici encore une propriété générale des groupes faiblement régulièrement branchés qui est facile à démontrer.

PROPOSITION 4.7. — *Soit G un groupe faiblement régulièrement branché sur K. Alors, pour tout sous-groupe distingué $N \triangleleft G$, il existe n tel que*

$$K_n' < N$$

où $K_n = K \times \ldots \times K$ (produit direct de d^n facteurs, chacun agissant sur le sous-arbre correspondant).

4.2. Moyennabilité

En 1929, von Neumann [**27**] a défini la notion de moyennablité qui est devenue fondamentale.

DÉFINITION 4.8. — *Le groupe G est dit moyennable s'il existe une mesure μ définie sur toutes les parties de G telle que*

- $\mu(G) = 1$
- $\mu(A \cup B) = \mu(A) + \mu(B) - \mu(A \cap B)$ *pour tous* $A, B \subset G$
- $\mu(gA) = \mu(A)$ *pour tout* $g \in G$ *et tout* $A \subset G$.

Il découle des travaux de von Neumann [**27**] que les groupes à croissance sous-exponentielle sont moyennables et que cette classe est fermée par rapport aux opérations élémentaires : extensions, quotients, sous-groupes et limites directes. Avant la construction du groupe engendré par l'automate de la figure 5, tous les groupes moyennables connus pouvaient être obtenus à partir de groupes à croissance sous-exponentielle en utilisant les opérations élémentaires décrites ci-dessus. Pour l'histoire des différentes conjectures concernant la classe des groupes moyennables, voir [**17**], la première référence étant l'article de Day [**6**].

Soit SG_0 la classe des groupes dont tous les sous-groupes de type fini sont à croissance sous-exponentielle. Supposons que $\alpha > 0$ est un ordinal et qu'on a défini SG_β pour chaque ordinal $\beta < \alpha$. Alors, si α est un ordinal limite, soit

$$SG_\alpha = \bigcup_{\beta < \alpha} SG_\beta.$$

Si α n'est pas un ordinal limite, soit SG_α la classe des groupes qui peuvent être obtenus à partir des groupes dans $SG_{\alpha-1}$ en utilisant soit des extensions soit des limites directes. Soit

$$SG = \bigcup_\alpha SG_\alpha.$$

Les groupes de cette classe sont dits sous-exponentiellement moyennables.

SG est la plus petite classe des groupes qui contient les groupes à croissance sous-exponentielle et qui est fermée par rapport aux opérations élémentaires. Les classes SG_α sont fermées par rapport aux sous-groupes et aux quotients.

PROPOSITION 4.9 ([**16**]). — *Le groupe G n'est pas sous-exponentiellement moyennable, i.e. $G \notin SG$.*

Preuve. — On commence par les lemmes suivants :

LEMME 4.10. — *Nous avons la relation*

$$\psi_1(\gamma_3(G)) = \langle \gamma_3(G), b^{2a} \rangle.$$

Preuve. — C'est une conséquence du lemme 4.5 et de la relation (9).

LEMME 4.11. — *On a*

$$\psi_1(\langle \gamma_3(G), b^{2a} \rangle) = \langle \gamma_3(G), b^{2a}, a \rangle.$$

Preuve. — Ceci est une conséquence du lemme précédent et de la relation $b^{2a} = (a, a^b)$.

LEMME 4.12. — *Pour la projection sur la seconde coordonnée, nous avons* :

$$\psi_2(\langle \gamma_3(G), b^{2a}, a \rangle) = G.$$

Preuve. — Ceci découle du lemme 4.5 et des relations $b^{2a} = (a, a^b)$ et $a = (1, b)$.

On peut maintenant démontrer la proposition 4.9. Supposons que $G \in SG_\alpha$ pour α minimal. Alors α ne peut pas être 0 puisque G est à croissance exponentielle (le semi-groupe engendré par a et b est libre d'après le lemme 4.4). En outre, α n'est pas un ordinal limite car, si $G \in SG_\alpha$ pour un ordinal limite, alors $G \in SG_\beta$ pour un ordinal $\beta < \alpha$. De plus G n'est pas limite directe (d'une suite croissante de groupes) car il est de type fini. Donc il existe N, $H \in SG_{\alpha-1}$ tels que la suite suivante soit exacte :

$$1 \to N \to G \to H \to 1.$$

Grâce à la proposition 4.7, il existe n tel que $N > (\mathrm{Rist}_G(n))' \geq G'' \times \ldots \times G''$ (2^n fois). Donc $G'' \in SG_{\alpha-1}$ et alors $\gamma_3(G) \in SG_{\alpha-1}$ d'après le lemme 4.6. Chaque classe SG_α est fermée par rapport aux quotients et passages aux sous-groupes. D'après les lemmes 4.10, 4.11, 4.12 on déduit que $G \in SG_{\alpha-1}$. Contradiction.

Pour démontrer la moyennabilité de G, on utilise un critère dû à Kesten [**21**] utilisant les marches aléatoires sur G.

Soit μ une mesure de probabilité symétrique dont le support est une partie génératrice symétrique S de G, i.e. $G = \langle S \rangle$, $\mu(s) = \mu(s^{-1})$ pour chaque $s \in S$ et $\mu(S) = 1$.

Soit p_n la probabilité de retour à l'identité après n pas pour la marche aléatoire donnée par μ, i.e.

$$p_n(\mathrm{Id}, \mathrm{Id}) = \mu^{*n}(\mathrm{Id})$$

où μ^{*n} est la n-ième puissance de convolution de μ sur G.

THÉORÈME 4.13 (Kesten [**21**]). — *Le groupe G est moyennable si et seulement si*

$$\lim_{n\to\infty} \sqrt[2n]{p_{2n}(\mathrm{Id}, \mathrm{Id})} = 1.$$

La moyennabilité de G a été démontrée par Virag [**32**]. Cette preuve a été publiée dans [**3**].

Sur G, considérons la marche aléatoire Z_n suivant la mesure symétrique μ sur $S = \{a, a^{-1}, b, b^{-1}\}$ avec les poids $\{1, 1, r, r\}$, i.e. $\mu(a^{-1}) = \mu(a) = \frac{1}{2r+2}$, $\mu(b^{-1}) = \mu(b) = \frac{r}{2r+2}$.

L'image de Z_n par le plongement de G dans $G \wr S_2$ est notée :

$$Z_n = (X_n, Y_n)\varepsilon_n$$

où $X_n, Y_n \in G$ et $\varepsilon_n \in S_2$.

On définit les temps d'arrêts σ et τ :

$$\begin{aligned}
\sigma(0) &= 0 \\
\sigma(m+1) &= \min\{n > \sigma(m) : \varepsilon_n = 1, X_n \neq X_{\sigma(m)}\} \\
\tau(0) &= \min\{n > 0 : \varepsilon_n = \mathsf{e}\} \\
\tau(m+1) &= \min\{n > \tau(m) : \varepsilon_n = \mathsf{e}, Y_n \neq Y_{\tau(m)}\}
\end{aligned}$$

Un calcul simple montre :

LEMME 4.14. — *$X_{\sigma(m)}$ et $Y_{\tau(m)}$ sont des marches aléatoires simples sur G suivant la distribution $\mu'(a^{-1}) = \mu'(a) = \frac{r}{2r+4}$, $\mu'(b^{-1}) = \mu'(b) = \frac{1}{r+2}$.*

On remarque que, pour $r = \sqrt{2}$, on obtient la même distribution sur Z_n, $X_{\sigma(n)}$ et $Y_{\tau(n)}$.

On vérifie aussi

LEMME 4.15. — *Presque sûrement*

$$\lim_{m\to\infty} \frac{m}{\sigma(m)} = \lim_{m\to\infty} \frac{m}{\tau(m)} = \frac{2+r}{4+4r} < \frac{1}{2}.$$

Pour conclure nous devons modifier la distance sur G, afin de pouvoir contrôler la norme de Z_n par les normes de X_n et Y_n.

Soit T_n le sous-arbre fini à n niveaux de T sur lequel agit G. Pour $g \in G$, on définit $|||\cdot|||_{T_n}$ par :

$$|||\, g \,|||_{T_n} = \sum_{\gamma \in \partial T_n} \left(|g_{|\gamma}| + 1\right) - 1.$$

Finalement on définit la distance $|||\ |||$ sur G :

$$|||\, g \,||| = \min_n |||\, g \,|||_{T_n}.$$

On vérifie que pour $g = (g_0, g_1)\mathsf{e}^{0,1}$

$$|||g_0||| + |||g_1||| \leq |||g||| \leq |||g_0||| + |||g_1||| + 1$$

et que la croissance par rapport à la métrique $|||\cdot|||$ est au plus exponentielle, i.e. il existe $a > 1$ tel que

$$|\{g : |||g||| \leq n\}| \leq a^n. \tag{11}$$

Nous avons

Proposition 4.16. — *Presque sûrement*

$$\lim_{n\to\infty} \frac{|||Z_n|||}{n} = 0.$$

Preuve. — L'existence de cette limite, qu'on note s, est une conséquence du théorème ergodique de Kingman. Maintenant

$$\frac{|||Z_n|||}{n} \leq \frac{|||X_n|||}{n} + \frac{|||Y_n|||}{n} + \frac{1}{n}.$$

Mais

$$\lim_{n\to\infty} \frac{|||X_n|||}{n} = \lim_{n\to\infty} \frac{|||X_{\sigma(n)}|||}{\sigma(n)} = \lim_{n\to\infty} \frac{|||X_{\sigma(n)}|||}{n} \lim_{n\to\infty} \frac{n}{\sigma(n)}$$

et similairement pour Y_n. Donc pour $r = \sqrt{2}$ si $s > 0$, d'après le lemme (4.15), $s < s\frac{1}{2} + s\frac{1}{2} = s$. Cette contradiction signifie que $s = 0$.

Proposition 4.17. — *La probabilité $p(Z_{2n} = \mathrm{Id})$ ne décroît pas exponentiellement.*

Preuve. — Pour chaque $\varepsilon > 0$, on a

$$p(|||Z_{2n}||| \leq \varepsilon n) = \sum_{g\in G, |||g||| \leq \varepsilon n} p(Z_{2n} = g) \leq p(Z_{2n} = \mathrm{Id}) \times |\{g \in G; |||g||| \leq \varepsilon n\}|.$$

Donc d'après (11)

$$p(Z_{2n} = \mathrm{Id}) \geq p\left(\frac{|||Z_n|||}{n} < \varepsilon\right) \cdot a^{-\varepsilon n}.$$

D'après la proposition 4.16 et le critère de Kesten, le groupe engendré par l'automate de la figure 5 est donc moyennable.

En utilisant des extensions HNN du groupe G, on peut construire des groupes moyennables de présentation finie qui ne sont pas sous-exponentiellement moyennables. Dans [**17**] on démontre que le groupe

$$\widetilde{G} = \langle b, t | [b^{tb}, b^t] = 1, b^{t^2} = b^2 \rangle$$

a ces propriétés.

5. GROUPE DE WILSON

On présente ici le groupe que Wilson a construit pour répondre à un problème de Gromov. Pour le définir, on utilise le langage des produits en couronne (voir la section 1.2).

5.1. Problème de Gromov

Pour les groupes à croissance exponentielle, la fonction de croissance dépend fortement de la partie génératrice. Il est naturel de demander si on peut associer un invariant lié à la croissance qui soit indépendant de la partie génératrice. Plus précisément, pour un groupe G engendré par une partie finie S, on définit

$$h(G,S) = \lim_{n\to\infty} \sqrt[n]{|\{g \in G : |g|_S \leq n\}|}.$$

L'entropie du groupe G est alors

$$h(G) = \inf_{S;\langle S\rangle = G} h(G,S).$$

En 1981, Gromov [**18**] a demandé si pour chaque G à croissance exponentielle

$$h(G) > 1,$$

i.e. s'il est à croissance exponentielle uniforme, ce qui signifie qu'il existe $a > 1$ tel que pour chaque partie génératrice

$$|\{g \in G : |g|_S \leq n\}| \geq a^n.$$

La réponse est positive pour plusieurs classes de groupes comme les groupes hyperboliques ou linéaires de type fini [**4**], [**8**].

Le premier groupe sans croissance exponentielle uniforme a été construit par Wilson en 2003 [**33**].

5.2. Construction de Wilson

Désignons par A_{31} le sous-groupe alterné du groupe symétrique à 31 éléments.

THÉORÈME 5.1. — *Soit H un groupe parfait de type fini vérifiant la propriété $H \simeq H \wr A_{31}$. Alors il existe une suite (x_n) d'éléments d'ordre 2 et une suite (y_n) d'éléments d'ordre 3 tels que*

1. $\langle x_n, y_n \rangle = H$ *pour chaque* n ;
2. $\lim_{n\to\infty} h(H, \{x_n, y_n\}) = 1$.

Construction de H. —

Soit T_{31} un arbre enraciné de degré 31. Soit $x \in \mathrm{Aut}(T_{31})$ qui agit non trivialement seulement sur le premier niveau. On définit $\overline{x} \in Aut(T_{31})$ par son image dans le produit en couronne

$$\overline{x} = (x, \overline{x}, \mathrm{Id}, \ldots, \mathrm{Id}).$$

Et finalement soit

$$H = \langle x, \overline{x} | x \in A_{31} \rangle.$$

Le groupe H est de type fini et H est parfait car A_{31} l'est.

PROPOSITION 5.2. — *On a*

$$H \simeq H \wr A_{31}.$$

Preuve. — Soit $\sigma = (2,3,4)$, $\rho = (1,3,2) \in A_{31}$; considérons $x, y \in A_{31}$. Alors $[\overline{x}, \sigma\overline{y}] = ([x,y], \mathrm{Id}, \ldots, \mathrm{Id})$. Comme H est parfait ceci montre que, pour chaque $x \in A_{31}$, on a $(x, \mathrm{Id}, \ldots, \mathrm{Id}) \in H$. Ensuite $\rho(x, \mathrm{Id}, \ldots, \mathrm{Id})^{-1}\overline{x} = (\overline{x}, \mathrm{Id}, \ldots, \mathrm{Id})$. Donc H contient $\{(h, \mathrm{Id}, \ldots, \mathrm{Id}) | h \in H\}$ e,t en utilisant $x \in A_{31}$, on a $H \wr A_{31} \subseteq H$.

Maintenant on va expliquer quelles sont les propriétés du groupe A_{31} dont on a besoin.

PROPOSITION 5.3. — *Le groupe A_{31} peut être engendré par un élément d'ordre 2 et un élément d'ordre 3.*

Comme $H \simeq H \wr A_{31}$ et H est parfait, ceci implique qu'il existe $u, v \in H$ tel que $u^2 = v^3 = \mathrm{Id}$ et $H = \langle u, v \rangle$.

PROPOSITION 5.4. — *Soit $H \simeq H \wr A_{31}$ un groupe parfait engendré par u et v tels que $u^2 = v^3 = id$. Alors il existe $x, y \in A_{31}$ tel que*

– *il existe $\alpha, \beta \in \{1, \ldots, 31\}$, $\alpha \neq \beta$*

$$\begin{aligned} x(\alpha) &= x^y(\alpha) = \alpha \\ y(\beta) &= \beta \end{aligned}$$

– *les élements*

$$\begin{aligned}\widehat{x} &= (\dots,u,\dots)x\\ \widehat{y} &= (\dots,v,\dots)y,\end{aligned}$$

où u est en position α et v en position β, satisfassent $\widehat{x}^2=\widehat{y}^3=id$ et $\langle\widehat{x},\widehat{y}\rangle=H$.

Preuve. — On vérifie facilement cette proposition avec x, y, α et β explicites **[33]**.

Maintenant soient

$$\begin{aligned}\gamma'(n) &= |\{w\in H : |w|_{\langle\widehat{x},\widehat{y}\rangle}\le n\}|,\\ \gamma(n) &= |\{w\in H : |w|_{\langle u,v\rangle}\le n\}|.\end{aligned}$$

PROPOSITION 5.5. — *Si on note $\lim_{n\to\infty}\sqrt[n]{\gamma(n)}=c$ et $\lim_{n\to\infty}\sqrt[n]{\gamma'(n)}=c'$, alors pour $s\ge 3$ on a*

$$c'\le \max\left(c^{1-\frac{1}{2c}},(1+2/s)(s+2)^{2/s}\right).$$

Preuve. — Commençons par expliquer le second terme. Considérons $\mathbb{Z}/3\mathbb{Z}*\mathbb{Z}/2\mathbb{Z}$. Soient

$$\rho_n=\{w\in\mathbb{Z}/3\mathbb{Z}*\mathbb{Z}/2\mathbb{Z};|w|_{\langle x,y\rangle}\le n \text{ et } |\{xy^{-1}xy\in w\}|\le[n/s]\}.$$

Alors $\lim_{n\to\infty}\sqrt[n]{\rho_n}\le(1+2/s)(s+2)^{2/s}$.

Maintenant soient

$$\begin{aligned}B(n) &= \{w\in\langle\widehat{x},\widehat{y}\rangle;|w|\le n\}\\ B_+(n) &= \{w\in B(n);|\{\widehat{x}\widehat{y}^{-1}\widehat{x}\widehat{y}\in w\}|\le[n/s]\}\\ B_-(n) &= B(n)\setminus B_+(n).\end{aligned}$$

On a

$$\widehat{x}\widehat{y}^{-1}\widehat{x}\widehat{y}\widehat{x}=(1,\dots,1,v^{-1},\dots,u,\dots,v)xy^{-1}xyx$$

où v^{-1} est en position $xyx(\beta)$, u est en $yx(\alpha)$ et v en $x(\beta)$.

Si $w\in B_+(n)$, alors $|\{\widehat{x}\widehat{y}^{-1}\widehat{x}\widehat{y}\widehat{x}\}|$ est au moins $\frac{1}{2}[n/s]=r$. Donc

$$|B_+(n)|\le|A_{31}|\sum_{n_1+\dots+n_{31}\le n-2r}\prod_{j=1}^{31}\gamma(n_i)\le K(n)(c+\varepsilon)^{n-2r}=K(n)(c+\varepsilon)^{n(1-1/2s)}$$

où $K(n)$ est un polynôme en n. On obtient donc l'estimation de la proposition.

La preuve du théorème se ramène donc à celle du lemme élémentaire :

LEMME 5.6. — *Il existe une suite $s_n\to\infty$ telle que*

$$c_n\to 1$$

où $c_1=2$ et $c_n=\max\left(c_{n-1}^{1-\frac{1}{2s_n}},(1+2/s_n)(s_n+2)^{2/s_n}\right)$ pour $n\ge 2$.

Finalement pour démontrer que H est à croissance exponentielle, on prouve qu'il admet un semi-groupe libre.

RÉFÉRENCES

[1] S. V. Alešin – Finite automata and the Burnside problem for periodic groups, *Mat. Zametki* **11** (1972), p. 319–328.

[2] M. F. Atiyah – Elliptic operators, discrete groups and von Neumann algebras, in *Colloque "Analyse et Topologie" en l'honneur de Henri Cartan (Orsay, 1974)*, Soc. Math. France, 1976, p. 43–72. Astérisque, No. 32–33.

[3] L. Bartholdi & B. Virág – Amenability via random walks, *Duke Math. J.* **130** (2005), p. 39–56.

[4] E. Breuillard & T. Gelander – Cheeger constant and algebraic entropy of linear groups, *International Mathematical Research Notices* **56** (2005), p. 3511–3523.

[5] J. Brieussel – Croissance et moyennabilité de certains groupes d'automorphismes d'un arbre enraciné, Thèse, Université Paris 7, 2008.

[6] M. M. Day – Amenable semigroups, *Illinois J. Math.* **1** (1957), p. 509–544.

[7] W. Dicks & T. Schick – The spectral measure of certain elements of the complex group ring of a wreath product, *Geom. Dedicata* **93** (2002), p. 121–137.

[8] A. Eskin, S. Mozes & H. Oh – On uniform exponential growth for linear groups, *Invent. Math.* **160** (2005), p. 1–30.

[9] J. Fabrykowski & N. Gupta – On groups with sub-exponential growth functions, *J. Indian Math. Soc. (N.S.)* **49** (1985), p. 249–256 (1987).

[10] ———, On groups with sub-exponential growth functions. II, *J. Indian Math. Soc. (N.S.)* **56** (1991), p. 217–228.

[11] F. Gecseg & I. Peák – *Algebraic theory of automata*, Akadémiai Kiadó, 1972, Disquisitiones Mathematicae Hungaricae, 2.

[12] Y. Glasner & S. Mozes – Automata and square complexes, *Geom. Dedicata* **111** (2005), p. 43–64.

[13] R. Grigorchuk – Degrees of growth of finitely generated groups and the theory of invariant means, *Izv. Akad. Nauk SSSR Ser. Mat.* **48** (1984), p. 939–985.

[14] R. Grigorchuk, P. Linnell, T. Schick & A. Żuk – On a question of Atiyah, *C. R. Acad. Sci. Paris Sér. I Math.* **331** (2000), p. 663–668.

[15] R. Grigorchuk & A. Żuk – The lamplighter group as a group generated by a 2-state automaton, and its spectrum, *Geom. Dedicata* **87** (2001), p. 209–244.

[16] ———, On a torsion-free weakly branch group defined by a three state automaton, *Internat. J. Algebra Comput.* **12** (2002), p. 223–246, International Conference on Geometric and Combinatorial Methods in Group Theory and Semigroup Theory (Lincoln, NE, 2000).

[17] ———, Spectral properties of a torsion-free weakly branch group defined by a three state automaton, in *Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001)*, Contemp. Math., vol. 298, Amer. Math. Soc., 2002, p. 57–82.

[18] M. Gromov – *Structures métriques pour les variétés riemanniennes*, Textes Mathématiques, vol. 1, CEDIC, 1981, Edited by J. Lafontaine and P. Pansu.

[19] ———, Hyperbolic groups, in *Essays in group theory*, Math. Sci. Res. Inst. Publ., vol. 8, Springer, 1987, p. 75–263.

[20] N. Gupta & S. Sidki – Some infinite p-groups, *Algebra i Logika* **22** (1983), p. 584–589.

[21] H. Kesten – Full Banach mean values on countable groups, *Math. Scand.* **7** (1959), p. 146–156.

[22] V. B. Kudryavtsev, S. V. Aleshin & A. S. Podkolzin – B*vedenie v teoriyu avtomatov (Introduction to automata theory)*, "Nauka", 1985.

[23] W. Lück – *L^2-invariants : theory and applications to geometry and K-theory*, Ergebnisse Math. Grenzg.. 3. Folge, vol. 44, Springer, 2002.

[24] G. A. Margulis – *Discrete subgroups of semisimple Lie groups*, Ergebnisse Math. Grenzg.. 3. Folge, vol. 17, Springer, 1991.

[25] J. Milnor – Problems and Solutions : Advanced Problems : 5600-5609, *Amer. Math. Monthly* **75** (1968), p. 685–687.

[26] V. Nekrashevych – *Self-similar groups*, Mathematical Surveys and Monographs, vol. 117, Amer. Math. Soc., 2005.

[27] J. von Neumann – Zur allgemeinen Theorie des Maßes, *Fundamenta Mathematica* **13** (1929), p. 73–116.

[28] P. S. Novikov & S. I. Adjan – Infinite periodic groups. I, *Izv. Akad. Nauk SSSR Ser. Mat.* **32** (1968), p. 212–244, 251–524, 709–731.

[29] J.-F. Planchat – Groupe d'Aleshin, mémoire de DEA, Paris VII, 2005.

[30] J-P. Serre – *Arbres, amalgames,* SL_2, Soc. Math. France, 1977, Astérisque, No. 46.

[31] V. Ī. Suščans′kiĭ – Periodic p-groups of permutations and the unrestricted Burnside problem, *Dokl. Akad. Nauk SSSR* **247** (1979), p. 557–561.

[32] B. Virag – Self-similar walk on a self-similar group, prépublication, 2003.

[33] J. S. Wilson – On exponential growth and uniformly exponential growth for groups, *Invent. Math.* **155** (2004), p. 287–303.

[34] A. Żuk – Automata groups, livre à paraître.

Andrzej ŻUK

Université Paris VII
Institut de Mathématiques de Jussieu
UMR 7586 du CNRS
Boîte 7012
2 place Jussieu
75251 Paris Cedex 05
E-mail : zuk@math.jussieu.fr