A brief and biased introduction to combinatorial group theory

Burnside problem, growth of groups and Mealy automata

Thibault Godin

May 21, 2019

Contents

Chapter 1

Words and Groups

In this section, we give a short introduction to group theory. We focus on basic properties and definitions which will be of direct interest to us in the next sections. More complete and advanced introductions can be found in [dlH00, CSC10, LS01, Löh17] for instance.

Definition 1.0.0.1 (Group)**.** *A group is set G with an internal law $* : G^2 \to G$ such that:*

1. *$*$ is associative: $\forall x, y, z \in G, (x * y) * z = x * (y * z)$.*
2. *There exists a neutral element $\mathbb{1}$ for $*$: $\forall x \in G, e * x = x * e = x$.*
3. *All elements admit an inverse: $\forall x \in G, \exists y \in G, x * y = y * x = e$. In this case we write $y = x^{-1}$.*

In a lot of situation the internal law will be clear from the context and we will omit it, writing G instead of $(G, *)$.

Example 1.0.0.2. *We give a few examples and non-examples. Proofs are left as exercises. We start with some infinite groups used in everyday's math:*

- *The set of integer $\mathbb{Z}$ with addition $+$ is a group, whose identity is 0. So is the set of even integer with addition, however the set of odd integer is not since 1) the sum of two odd is even, and 2) there is no odd neutral element for the addition.*
- *The set of integer $\mathbb{Z}$ with multiplication $\times$ is a not a group since inverses are not defined in general. The set of rational numbers $(\mathbb{Q}, \times)$ is not either because 0 has no inverse, $(\mathbb{Q}^*, \times) = (\mathbb{Q} \setminus \{0\}, \times)$ is a group. So are $(\mathbb{R}^*, \times)$ and $(\mathbb{R}^*, \times)$*
- *The set of invertible matrices over any field $GL_n(\mathbb{K})$ is a group for matrix multiplication. So is the set of bijections of some set with the function composition.*
- *The set of words other some alphabet Σ with concatenation is not a group because of lack of inverses. The set of words other some alphabet Σ and its formal inverse Σ^{-1} is a group, called the* free group

and denoted $\mathbb{F}_\Sigma$. In addition all the free groups of alphabet of size n are isomorphic, and we denote $\mathbb{F}_n$ this group.

Now here are some finite groups and non-groups

- *The set of integer modulo n $\mathbb{Z}/n\mathbb{Z}$ with addition $+$ is a group, whose identity is 0. The set of integer non 0 modulo n $(\mathbb{Z}/n\mathbb{Z})^*$ with multiplication $\times$ is a group if and only if n is prime.*
- *So is the set of bijections of some finite set E of size n with the function composition is a group called the* symmetric group *and denoted S_E. Moreover all the symmetric groups of sets of size n are isomorphic, and we denote S_n the canonical representative, i.e. the set of bijection of $[\![1 : n]\!]$ whose elements are* permutations.
- *The set $V = \{(0,0),(0,1),(1,0),(1,1)\}$ with addition modulo 2 is a group called Klein 4-group or Klein Vierergruppe.*

Exercise 1.0.0.3. *Show that the identity element of a group is unique, and that an element admits a unique inverse.*

Proof. Let $\mathbb{1}, \mathbb{1}'$ be identity elements in a group G. Then we have $\mathbb{1} * \mathbb{1}' = \mathbb{1}'$ as $\mathbb{1}$ is an identity but also$\mathbb{1} * \mathbb{1}' = \mathbb{1}$, hence $\mathbb{1} = \mathbb{1}'$.
Let $x \in G$ and y, z be inverses of x. Then $y * (x * z) = y$ and$(y * x) * z = z$. By associativity we conclude that $y = z$. □

Once a group is defined, it is natural to consider smaller parts of it, as we have done with even and odd integer. The following notion formalize this idea:

Definition 1.0.0.4 (Subgroup)**.** *Let $(G, *)$ be a group. Then $(H, *)$ is a subgroup of $(G, *)$ (denoted $(H, *) \leq (G, *)$) if H is a non empty subset of G and :*

1. $\forall x, y \in H, x * y \in H$,
2. $\forall x \in H, x^{-1} \in H$.

Notice that in particular this definition forces the identity element of G to belong to the subgroup H and be its identity element as well.
A group always have at least 2 subgroups: itsefl and the trivial group $(\{\mathbb{1}\}, *)$.

Exercise 1.0.0.5. *Prove that no subgroup of $(\mathbb{Z}, +)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}, +)$. Hints: pick any non-zero element and consider its powers.*

It can be interesting to know the relative size of a subgroup compared to the original group. This is achieved by the index:

Definition 1.0.0.6. *Given a group G and a subgroup $H \leq G$, the* index *of H in G is*

$$[G : H] = \min_{\#\{g_i\} \subset G} \bigcup_i g_i H = G \, .$$

Example 1.0.0.7. *The index of the even integer in $(\mathbb{Z}, +)$ is two. The index of $(\mathbb{Z}, +)$ in $(Q, +)$ is infinite and so is the index of $(Q, +)$ in $(\mathbb{R}, +)$.*

More generally, the size of a subgroup is not totally uncorrelated with the size of the original group. More precisely:

Theorem 1.0.0.8 (Lagrange, Index formula)**.** *Let $G \geq H \geq K$ be groups. Then*

$$[G : K] = [G : H] \, [H : K] \ .$$

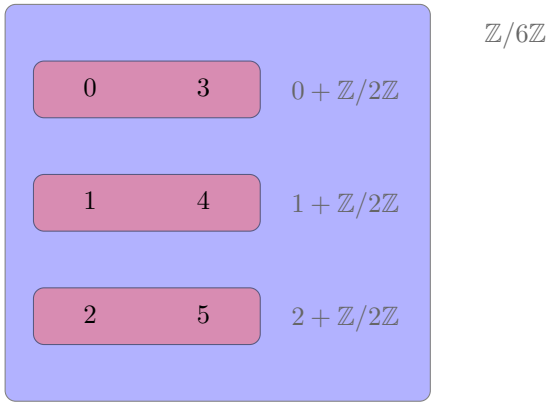
In particular, if G is finite, then the size of any subgroup H of G divides the size of G.

Proof. By definition, $[G : K] = \min_{\#\{g_i\} \subset G} \bigcup_i g_i K = G$ and accordingly for the other indices. Now, we have

$$\begin{aligned} \bigcup_i g_i' K = G &= \bigcup_i g_i H \\ &= \bigcup_i g_i \left(\bigcup_j h_j K \right) \\ &= \bigcup_i \left(\bigcup_j g_i h_j K \right) \end{aligned}$$

and as $g_i h_j \in G$ and the unions are disjoint, taking the minimum on both side leads us to the required formula. □

Example 1.0.0.9. *We have $[\mathbb{Z}/6\mathbb{Z} : \mathbb{Z}/2\mathbb{Z}] = 3$:*



The concept of subgroup can be extremely useful. for instance, it can allow to prove general result by focusing on a single group. The following is central in the theory of finite groups.

Theorem 1.0.0.10 (Cayley)**.** *Every finite group is isomorphic to a subgroup of a symmetric group.*

Proof. Let G be a finite group of size n. One can define group of functions $\Phi_G = \{\varphi_g : G \to G, h \mapsto gh | g \in G\}$. As $\varphi_g = \varphi_{g'} \Rightarrow \forall h, gh = g'h \Rightarrow ghh^{-1}g'hh^{-1} \Rightarrow g = g'$, the two groups are isomorphic. Moreover, each φ_g induces a permutation on the finite set G, because $gh = gh' \Rightarrow g^{-1}gh = g^{-1}gh \Rightarrow h = h'$, so $\Phi_G \leq S_G \simeq S_n$. □

We finish this section with two important definitions:

Definition 1.0.0.11 (Normal subgroup)**.** *Let G be a group and $nN \leq G$ be a subgroup. Then N is called* normal *if we have $\forall g \in G, gN = Ng$. In other words:*

$$N \lhd G \Leftrightarrow \forall g \in G, \forall n \in N, gng^{-1} \in N \ .$$

A subgroup may not be normal. However, given a subgroup (and more generally a subset) R of G, one may always construct the smallest normal subgroup containing R by considering the closure of the set $\{grg^{-1}\}$ of conjugate of R under the group operation.

Definition 1.0.0.12 (Quotient)**.** *Let G be a group and $N \lhd G$ be a normal subgroup. Then the set of coset $\{gN, g \in G\}$ is a group with identity N and the law induced by the law on G.*

Notice that, in general, if N is only a subgroup the the set of coset gN is not a group. This notation of quotient is coherent with the cyclic groups: $d\mathbb{Z}$ is normal is $\mathbb{Z}$ and the cyclic group of order d is indeed isomorphic to the quotient $\mathbb{Z}/d\mathbb{Z}$. In the same spirit the group of complex units (*resp.* complex unit of finite order) can be seen as $\mathbb{R}/2\pi\mathbb{Z}$ (*resp.* $\mathbb{Q}/2\pi\mathbb{Z}$).

1.1 Finitely generated groups

As we saw with the odd integers, a subset does not always form a group, whence the idea of

Definition 1.1.0.1 (Generating set)**.** *Let $(G, *)$ be a group. A* generating set *of G is a set $S \subset G$ such that any element of G can be written as a combination of elements of S:*

$$\forall g \in G, \exists s_1, \ldots, s_j, \ldots \in S, \ g = s_1 * s_2 * \ldots * s_j * \ldots \ .$$

The whole group is always a generating set for itself, but one is usually interested in smaller generating sets. One say that a generating set is *symmetric* if the inverse of each element also belong to the set, usually but not always the generating sets are supposed to be symmetric.

Example 1.1.0.2.
- $\{\pm 1\}$ *is a generating set for* $(\mathbb{Z}, +)$. *So are* $\{+2, -3\}$ *or* $\{-5, -3, -1, +8, +10\}$ *for instance.*
- $\{(0, \pm 1), (\pm 1, 0)\}$ *is a generating set for* $(\mathbb{Z}^2, +)$.
- $\{a^{\pm 1}, b^{\pm 1}\}$ *is a generating set for the free group* $\mathbb{F}_{\{a,b\}}$.
- $\{+1\}$ *is a generating set of* $\mathbb{Z}/n\mathbb{Z}$.
- $\{(1, 2), (1, 2, \ldots, n)\}$ *is a generating set of* S_n.

A group is called *monogenic* if there exists a generating set of size 2 consisting in exactly one element and its inverse.
A group is called *finitely generated* if there exists a generating set of finite size. These group are of particular interest in combinatorial group theory because each element can be understood as a word on a finite alphabet. Despite the strong requirement, the of finitely generated group already include many interesting examples and behaviour while providing numerous tools to be analysed. Quoting Gromov:

"A statement that holds for all finitely generated groups has to be either trivial or wrong."

Example 1.1.0.3.
- $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ *are monogenic.*
- $\mathbb{Z}^2, V, S_n, \mathbb{F}_n$ *are finitely generated.*
- $Q^*, \mathbb{R}^*$ *are not finitely generated.*
- $GL_n(\mathbb{K})$ *is finitely generated if and only if* $\mathbb{K}^*$ *is finitely generated.*

Definition 1.1.0.4 (Order)**.** *The* order *of an element* g *of a group* G *is the least (strictly positive) integer* α *such that* $g^\alpha = \mathbb{1}$. *When such an integer exists we say that* g *has* ***finite order****, infinite otherwise.*

In other words, the order of g is the cardinality of the monogenic subgroup $\langle g \rangle$ it generates.

Example 1.1.0.5. *In* $(\mathbb{Z}/12\mathbb{Z}, +)$, 5 *has order* 12 *because* $5+5 = 10, 10+5 = 3, 3+5 = 8, 8+5 = 1, 1+5 = 6, 6+5 = 11, 11+5 = 4, 4+5 = 9, 9+5 = 2, 2+5 = 7, 7+5 = 0 = e$. *In the same fashion* 2 *has order 6 and* 8 *has order* 3.

On the other hand, for the group of integers $\mathbb{Z}$, *zero is the only element of finite order since the repeated sum of the same integer goes to plus or minus infinity.*

One can also have mixed behaviour: for instance take the direct product of $\mathbb{Z}/2\mathbb{Z}$ *with* $\mathbb{Z}$ *(*$(x, \mathbb{1}_\mathbb{Z})$ *has finite order,* $\left(\mathbb{1}_{\mathbb{Z}/2\mathbb{Z}}, y\right), \quad y \neq \mathbb{1}_\mathbb{Z}$ *has infinite order) or the continuous group of roots of the unit* $\{e^{i\theta} | \quad \theta \in [0\,, 2\pi[\}$ *(the elements of* $Q/\mathbb{Z}2\pi$ *have finite order, the element in complement all have infinite order).*

Exercise 1.1.0.6. *1. Prove that the Klein group is the smallest non-monogenic group.*

2. *A group is called* Abelian *if every elements commutes, i.e.* $\forall x, y, \quad x * y = y * x$. *Prove that the symmetric group on* 3 *elements is the smallest non-abelian group.*

3. *Prove that every finite monogenic group is isomorphic to* $\mathbb{Z}/n\mathbb{Z}$ *for some* n *and that every infinite monogenic group is isomorphic to* $\mathbb{Z}$.

Exercise 1.1.0.7. *Let* G *be a group and define* $Z_G = \{x \in G | \forall y \in G, xy = yx\}$ *its centre. Prove that* Z_G *is Abelian. Prove that* $[G : Z_G] \geq 4$ *if* G *is non-Abelian.*

Proof. The first claim is clear from the definition. For the second, notice that for all $g \in G, gZ_G = Z_G g$ (the subgroup is called *normal*). Denote $\bar{g} = \{g' \in G | g' Z_G = gZ_G\}$. This is a group noted G/Z_G called *quotient* of G by Z_G whose order is $[G : Z_G]$. Now this quotient group cannot be cyclic if G is not Abelian: if it were then $G/Z_G = \langle \bar{x} \rangle$. This means that $\exists x \in G, x \notin Z_G$, hence $\exists y \in G, xy \neq yx$. By definition of the centre $y \notin Z_G$ hence one can consider $G/Z_G \ni yZ_G \neq \mathbb{1}_{G/Z_G}$. Since we assumed G/Z_G is cyclic $\bar{y} = \bar{x}^k$ for some k, and using the properties of G/Z_G we obtain $yZ_G = x^k Z_G$ so $y = x^k g$ with $g \in Z_G$. Now $xy = x(x^k g) = x^k xg = x^k gx = yx$, contradiction. We conclude using the fact that the smallest non-Abelian group has order 4. □

Exercise 1.1.0.8 (Fibonacci mod d, the Pisano periods)**.** *Prove that* $GL_n(\mathbb{Z}/d\mathbb{Z})$ *is a finite group. Use this to prove that the sequence of residues of Fibonacci number* mod d *is periodic.* hint: *use the powers of the matrix* $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ *to describe the couple of Fibonacci number* $\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix}$

This is used in [Dia18] to perform a small "mathe-magic trick": draw a table of 16 cells ; put two numbers of between 0 *and* 6 *in the two first cells, then complete the table by adding the two predecessors of a cell* mod 7 *; then add up (normally) all cells. The total number is* 49.

We now give an informal definition of the presentation of a group: if S is a set of letter and R a set of words on S, then the group $\langle S|R \rangle$ is the biggest group in which elements of R are trivial. More precesely

Definition 1.1.0.9 (Presentation)**.** *Let* S *be a set and* R *be a set of words on* S. *The group* $\langle S|R \rangle$ *is the quotient* $\mathbb{F}_S/N(R)$ *of the free group on* S *by the normal closure of* R *in* $\mathbb{F}_S$.

The notation $\langle S \rangle$ of a subgroup generated by a subset and $\langle S|R \rangle$ are quite ambiguous, in particular when one consider the free group $\mathbb{F}_S = \langle S| \rangle$ which is often written $\mathbb{F}_S = \langle S \rangle$. Nevertheless the signification is generally clear from the context.

Groups are well-known to encode symmetries, hence it is natural to try to use on geometrical object.

Definition 1.1.0.10 (Action)**.** *Let* G *be a group and* X *be a set. An action of* G *on* X *is a fucntion* $\varphi : G \times X \to X$ *which is compatible with the law on* G, *i.e.* $\forall x \in X, \varphi(e, x) = x$ *and* $\forall g, h \in \forall x \in X, \varphi(gh, x) = \varphi(g, \varphi(h, x))$.

In general, we will say that G act on X and write $G \curvearrowright X$ and denote the action with a simple point $(\varphi(g, x) = g.x)$.

The action of a group is a powerful way to understand its structure. In fact, it is often the case that a group and its "natural" action are used indeferentially, for instance the group of permutations of $[\![1 : n]\!]$ and its action on $[\![1 : n]\!]$.

We now provide three classical ways of increasing complexity for creating new groups from existing.

Definition 1.1.0.11 (Direct product)**.** *Let $(G, .)$ and $(H, *)$ be groups. The direct product $G \times H$ of G with H is the group whose elements are $(g, h) \in G \times H$ and whose law is given by:*

$$(g, h)(g', h') = (g.g', h * h')$$

Definition 1.1.0.12 (Semi-direct product)**.** *Let $(G, .)$ and $(H, *)$ be groups such that H acts on G by φ. The semidirect product $G \rtimes_\varphi H$ of G with H is the group whose elements are $(g, h) \in G \times H$ and whose law is given by:*

$$(g, h)(g', h') = (g.\varphi(h, g'), h * h')$$

In particular the direct product is a special case of the semi-direct product where the action is trivial.

Definition 1.1.0.13 (Wreath product)**.** *Let $(G, .)$ and $(H, *)$ be groups. The wreath product $G \rtimes_\varphi H$ of G with H is the group whose elements are $\langle g_{|h_1}, \ldots, g_{|h_d}, \ldots \rangle h \in G^H \times H$ and whose law is given by:*

$$\langle g_{|h_1}, \ldots, g_{|h_d}, \ldots \rangle h.\langle g_{|h_1}, \ldots, g_{|h_d}, \ldots \rangle h' = \left\langle g_{|h_1} {g'}_{|h*h_1}, \ldots, g_{|h_d} {g'}_{|h*h_d}, \ldots \right\rangle h * h'$$

A equivalent definition is $G \wr H \simeq \prod_H G \rtimes H$. Usually, we will have $H = S_d$ so the action will just be permutation of the indices of the tuple.

We finish this introduction with a nice theorem of independent interest which proof uses several of the notions we introduced. Beside its own striking result, it suggest us several directions of research such as randomness and groups, decision problems ,and links between algebraic and combinatorial properties that we will develop along this course.

Theorem 1.1.0.14 (Proportion of commuting elements, Gustafson 1973 [Gus73])**.** *Let G be a finite group. If the proportion of commuting pairs*

$$dc(G) = \frac{1}{|G|^2} \#\{(x, y) \in G^2 | \quad xy = yx\}$$

is greater than $5/8$ then the group is Abelian.

Proof. Assume G is not Abelian. Let $C(x) = \#\{y \in G | xy = yx\}$.

$$\begin{aligned} dc(G) &= \frac{1}{|G|^2} \#\{(x, y) \in G^2 | \quad xy = yx\} \\ &= \frac{1}{|G|^2} \sum_{x \in G} |C(x)| \end{aligned}$$

Denoting $Z_G = \{x | \forall y \in G, xy = yx\}$ the centre (Zentrum) of G with have

$$= \frac{1}{|G|^2} \left(\sum_{x \in Z_G} |C(x)| + \sum_{x \notin Z_G} |C(x)| \right)$$

Since $C(x)$ is a proper subgroup and by Lagrange formula

$$\begin{aligned}
&\leq \frac{1}{|G|^2} \left(\sum_{x \in Z_G} |G| + \sum_{x \notin Z_G} |G|/2 \right) \\
&\leq \frac{1}{|G|^2} \left(|Z_G||G| + (|G| - |Z_G|)\frac{|G|}{2} \right) \\
&\leq \frac{1}{|G|^2} \left(|G| \left(|Z_G| + \frac{1}{2}(|G| - |Z_G|) \right) \right) \\
&\leq \frac{1}{|G|^2} \left(|G| \left(\frac{1}{2}(|G| + |Z_G|) \right) \right)
\end{aligned}$$

As it is proven in Exercise 1.1.0.7, the centre has index at least 4 in G, hence

$$\begin{aligned}
&\leq \frac{1}{|G|^2} \left(|G| \left(\frac{1}{2}(|G| + |G|/4) \right) \right) \\
&\leq \frac{5}{8}
\end{aligned}$$

Notice that the equality is obtained when $Z_G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ as for example for the quaternion group. One also can see that:

- If $Z_G \neq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ then $[G : Z_G] \geq 6$, whence $dc(G) \leq \frac{7}{12}$
- If the order of G is odd then $[G : Z_G] \geq 9$, so $dc(G) \leq \frac{11}{27}$

□

Amazingly enough, this result remains true in an infinite group: it is proven in [AMV17] that the proportion of commuting element in an infinite group is:

- greater than 5/8 if and only if the group is Abelian,
- greater than 0 if and only if the group is virtually Abelian.

Chapter 2

Burnside Problem

Historically, when people considered example of finitely generated groups, they were always either finite, or infinite with an element of infinite order.

It is quite clear that if a group has an element of infinite order (and hence contains a copy of $\mathbb{Z}$ has a subgroup), then it has to be infinite (if g has infinite order, then $\{g^k,\ k \in \mathbb{Z}\}$ is infinite). The reciprocal gives that a finite group has only elements of finite order.

Hence the question of Burnside:

Question 2.0.0.1 (Burnside 1902 [Bur02])**.** *Can a finitely generated group have all elements of finite order and be infinite?*

We stress that, in Burnside problem, all elements are supposed to be of finite order, and not only the generators.

This question became central in group theory and was solved for several classes of groups (for instance it is not hard to see that when the group is commutative the answer is no).

Remark 2.0.0.2. *The requirement for the group to be finitely generated is needed to avoid easy counter-examples that do not really concern combinatorial group theory. Otherwise groups such as* $\prod_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ *(the direct product of infinitely many groups of size* 2*) is indeed infinite with all elements of order* 2*.*

We can prove that some classes do not contain infinite Burnside group

Lemma 2.0.0.3. *If a group is Abelian, then it cannot be infinite Burnside.*

Proof. We prove the result for a 2-generated Abelian group, the general result is not harder. Assume that $G = \langle a, b\rangle$ is an Abelian group such that all elements are of finite order. Put α (*resp.* β) the order of a (*resp.* b). Consider now an element $g \in G$, by commutativity we can write $g = a^i b^j$,and using the integer

division, we get $g = a^{q\alpha+r}b^{q'\beta+r'} = a^r b^{r'}$. So all elements of G can be written $a^r b^{r'}$, $r \in [\![0 : \alpha]\!]$, $r' \in [\![0 : \beta]\!]$, which is a finite set.

□

More involved theorems highlight the difficulty of the conjecture, for instance:

Theorem 2.0.0.4 (Burnside 1905)**.** *Let G be a subgroup of $GL_n(\mathbb{C})$. If there exists $N > 0$ such that for all g in G, $g^N = \mathbb{1}$ then G is finite*

The solution was found in 1964 by Golod and Shafarevich, who gave an explicit example of a finitely generated group with all elements of finite order and infinite (henceforth called **infinite Burnside group**).

Theorem 2.0.0.5 (Golod and Shafarevich 1964 [GS64, Gol64])**.** *There exists infinite Burnside groups, that is infinite finitely generated groups such that every element has finite order.*

Remark 2.0.0.6. *In fact, the result of Golod is even stronger: namely, for every $d \geq 2$ there exists an infinite d-generated group such that every $d-1$-generated subgroup is finite. See [Ers12].*

However this example is very complicated and requires deep results in field theory, and, as these groups are on the edge between finiteness and infiniteness, people continued to look for examples.

In fact, the Burnside problem can be strengthen to:

Question 2.0.0.7 (Burnside 1902 [Bur02])**.** *Can a finitely generated group have all elements of finite order uniformly bounded and be infinite?*

This question reduces to: *"Is there a group $B(n, M) = \langle a_1 \dots a_n | \mathbf{w}^M, \forall \mathbf{w} \in \{a_1^{\pm 1}, a_n^{\pm 1}\}^* \rangle$ which is infinite?"*.

The answer is yes and was given by Adian and Novikov for certain large odd M and by Ivanov and Lysenok for (very) large even number:

Theorem 2.0.0.8 (Adian-Novikov 1968, Ivanov 1996, Lysenko 1996 [NA68, IO96])**.** *The free Burnside group $B(n, N)$ is infinite for $n > 1$ and sufficiently large N.*

You will not give any detail on the proofs (each of them is longer that 200 pages) nor on the actual meaning of "sufficiently large", as this vary strongly with the proofs and is anyhow believed to be quite far from the optimal.
On the other hand, for small exponents very few is known: the groups $B(n, 2), B(n, 3), B(n, 4)$, and $B(n, 6)$ are all finite [Hal58]. We prove the easiest case, which is a remark due to Burnside :

Exercise 2.0.0.9. *The Free Burnside groups $B(n, 2)$ are all finite.*

Proof. take a, b two generators of the group. Then $a^2 = \mathbb{1} = b^2 = (ab)^2$, whence $abab = a^2b^2$ so $ba = ab$, the group is Abelian. We conclude using Lemma 2.0.0.3. □

In fact we proved a slightly stronger result that announced: any group such that words of size less or equal than 2 are of order 2 is Abelian and finite (so is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some m).

Chapter 3

Mealy automata

In this chapter we describe how Mealy automata can be used to generate (interesting) groups. We start with an explicit example before giving the full formal explanations.

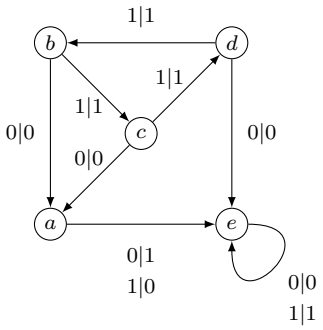


Figure 3.1: The Grigorchuk automaton.

3.1 The Grigorchuk automaton

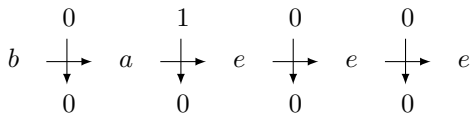
We see that the graph Figure 3.1 has vertices labelled by letters and edges (called transitions) of the form $x|y$ with $x, y \in \{0, 1\}$. We are going to call a, b, c, d, e the *states* of the automaton, {0,1} its *alphabet*, x the *input* letter of the transition, and y the *output* letter of the transition.

As for a classical automaton, the main move is, from a state, to read a letter. For instance reading 0 from the state b leads us to a outputting 0, because the transition is $b \xrightarrow{0|0} a$. This action can be easily extended, and from a state we can read a word of letter. For instance if we want to read, from the state b, the word 0100, we start as before by following the transition $b \xrightarrow{0|0} a$, outputting 0. What left to do is to read the word 100, now from a, so we follow the transition $a \xrightarrow{1|0} e$, and we iterate this process until there is no more

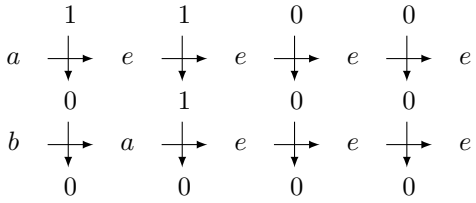
letter to be read. To summarise we have went through the states b, a, e and e, outputting 0000. This can be read as a path in the automaton:

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

or equivalently

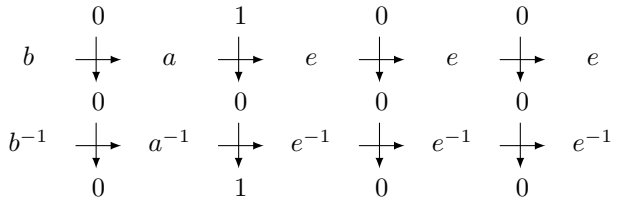


As we see, b transforms 0100 into 0000. As we can do this for any word, we can say that b induces a transformation ρ_b from $\{0,1\}^*$ to itself. Hence we get one function from word to word per state. Moreover, since these functions have the same domain and codomain, we can *compose* them as we want. Note that the composition corresponds in the automaton to the plug-in of the output of a run to the input of another. Namely $\rho_{ab} = \rho_b \circ \rho_a$ can be seen as



This structure where object can be compose together is called a semigroup. The most well known semigroup is certainly the set of positive integer (because the addition of two such number is always a positive integer), but in computer science we also use quite often the semigroup of words (the concatenation of two words is also a word), and we can think to many other examples. The theory of semigroups is a wide area intertangling math and informatics, but one is generally more familiar with group theory, where the elements can always be inversed.

In our setting, generating a group means that each function has to be bijective, *i.e.* that every state induces a function that can be inverted.



This can be easily verified on the automaton: it is equivalent to require that every state induces a permutation on the alphabet. This is the case for the Grigorchuk automaton (for instance a flips 0 and 1), so we can study the *group generated by the Grigorchuk automaton*, henceforth called the **Grigorchuk group**.

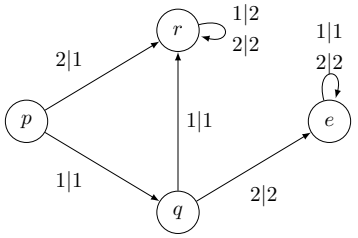


Figure 3.2: A Mealy automaton which cannot generate a group. For instance p sends 1 and 2 onto 1 and thus cannot be inverted

3.2 Automaton groups

We briefly review definitions and elementary facts about Mealy automata and self-similar group. A more complete reference is [Nek05, Zuk06].

3.2.1 Mealy automata

A *Mealy automaton* is a complete deterministic letter-to-letter transducer $\mathcal{A} = (Q, \Sigma, \delta, \rho)$, where Q and Σ are finite sets respectively called the the *stateset* and the *alphabet*, and $\delta = (\delta_i : Q \to Q)_{i\in\Sigma}$, $\rho = (\rho_q : \Sigma \to \Sigma)_{q\in Q}$ are respectively called the *transition* and *production* functions. Examples of such Mealy automata are depicted Figure 3.1. The transition and production functions can be extended to words as follows: see $\mathcal{A}$ as an automaton with input and output tapes, thus defining mappings from input words over Σ to output words over Σ. Formally, for $q \in Q$, the map $\rho_q \colon \Sigma^* \to \Sigma^*$, extending $\rho_q \colon \Sigma \to \Sigma$, is defined recursively by:

$$\forall i \in \Sigma,\ \forall \mathbf{s} \in \Sigma^*, \qquad \rho_q(i\mathbf{s}) = \rho_q(i)\rho_{\delta_i(q)}(\mathbf{s})\,. \tag{3.1}$$

Observe that ρ_q preserves the length of words in Σ^*. We can also extend the map ρ to words of states $\mathbf{u} \in Q^*$ by composing the production functions associated with the letters of $\mathbf{u}$:

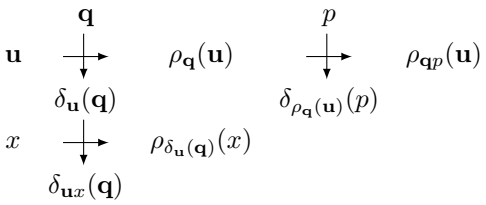
$$\forall q \in Q,\ \forall \mathbf{u} \in Q^*, \qquad \rho_{q\mathbf{u}} = \rho_{\mathbf{u}} \circ \rho_q\,. \tag{3.2}$$

For all $x \in \Sigma$, $\mathbf{u} \in \Sigma^*$, $p \in Q$, $\mathbf{q} \in Q^*$, we have, using *cross diagrams* from [AKL+12]:

$$\rho_{\mathbf{q}}((\mathbf{u}x)) = \rho_{\mathbf{q}}(\mathbf{u})\rho_{\delta_{\mathbf{u}}(\mathbf{q})}(x)$$

and

$$\delta_{\mathbf{u}}((\mathbf{q}p)) = \delta_{\mathbf{u}}(\mathbf{q}) \cdot \delta_{\rho_{\mathbf{q}}(\mathbf{u})}(p)\ .$$



Therefore the production functions $\rho_q : \Sigma^* \to \Sigma^*$ of an automaton $\mathcal{A}$ generate a semigroup $\langle\mathcal{A}\rangle_+ := \{\rho_{\mathbf{u}} : \Sigma^* \to \Sigma^* | \mathbf{u} \in Q^*\}$, all of which elements preserve the length of words in Σ^*.

A Mealy automaton is said to be *invertible* whenever ρ_q is a permutation of the alphabet for every $q \in Q$. In this case, all functions $\rho_q : \Sigma^* \to \Sigma^*$ are invertible and the automaton actually generates a group:

$$\langle\mathcal{A}\rangle := \langle\rho_q^{\pm 1} : \Sigma^* \to \Sigma^* | q \in Q\rangle = \left\{\rho_{\mathbf{u}} : \Sigma^* \to \Sigma^* | \mathbf{u} \in \left(Q \cup Q^{-1}\right)^*\right\}\ .$$

It is not difficult to find another (symmetrized) Mealy automaton generating this group as a semigroup. Its stateset can be taken as $Q \cup Q^{-1}$ such that $\rho_q^{-1} = \rho_{q^{-1}}$. A group of the form $\langle\mathcal{A}\rangle$ for an invertible automaton is called an *automaton group*. Such a group acts naturally on the set Σ^*.

Observe that given an integer k and a Mealy automaton $\mathcal{A} = (Q, \Sigma, \delta, \rho)$ with alphabet Σ, one can associate to it a Mealy automaton $(Q, \Sigma^k, \delta, \rho)$ where we identify the function ρ_q acting on Σ with the same function acting on Σ^k via (3.1). This just amounts to replacing the alphabet by the set of syllables of length k. With a slight abuse of language, we call the latter automaton the level k of $\mathcal{A}$. Notice that this level k automaton generates the same group as the original automaton.

3.2.2 Self-similar groups

One can describe the automaton group through this action via *wreath recursion* and obtain a so-called *self-similar* group. First let us recall a few definitions. Let us write $\Gamma \curvearrowright X$ the action of a group Γ on a set X and $\gamma.x \in X$ the transformation of $x \in X$ induced by $\gamma \in \Gamma$. The *permutational wreath product* $G \wr_\Sigma \mathrm{Sym}(\Sigma)$ of a group G over a set Σ is the set $G^\Sigma \times \mathrm{Sym}(\Sigma)$ together with the operation

$$\left\langle g_{|x_1}, \ldots, g_{|x_d}\right\rangle\pi(g).\left\langle h_{|x_1}, \ldots, h_{|x_d}\right\rangle\pi(h) = \left\langle g_{|x_1}h_{|\pi(g)^{-1}.x_1}, \ldots, g_{|x_d}h_{|\pi(g)^{-1}.x_d}\right\rangle\pi(g)\pi(h)$$

for the obvious action of $\mathrm{Sym}(\Sigma)$ on $\Sigma = \{x_1, x_2, \ldots, x_d\}$.

Assume we are given a group G together with an injective homomorphism $\psi : G \hookrightarrow G \wr_\Sigma \mathrm{Sym}(\Sigma)$. Then one can describe the group elements with a recursive formula, where we canonically identify g and $\psi(g)$

$$g = \psi(g) = \left\langle g_{|x_1}, \ldots, g_{|x_d}\right\rangle\pi(g)\ . \tag{3.3}$$

The group element $g_{|x_i}$ is called the *section* of g in x_i and $\pi(g)$ is the *action* of g. One can extend the section to words : $\forall \mathbf{u}x \in \Sigma^*, g_{|\mathbf{u}x} = g_{|\mathbf{u}|_x}$.

One can also extend the action of G to Σ^* by $\forall x\mathbf{u} \in \Sigma^*, g.x\mathbf{u} = (\pi(g).x)g_{|x}.\mathbf{u}$. The action of G on Σ^*, is called *self-similar* if

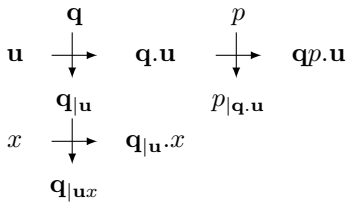
$$\forall g \in G, \forall \mathbf{u} \in \Sigma^*, \forall x \in \Sigma, \exists h \in G, \exists y \in \Sigma, g.x\mathbf{u} = yh.\mathbf{u}\,.$$

For all $x \in \Sigma$, $\mathbf{u} \in \Sigma^*$, $p \in Q$, $\mathbf{q} \in Q^*$, we have, using the same cross diagrams as for the automaton computations:

$$\mathbf{q}.(\mathbf{u}x) = \mathbf{q}.\mathbf{u}\mathbf{q}_{|\mathbf{u}}.x$$

and

$$(\mathbf{q}p)_{|\mathbf{u}} = \mathbf{q}_{|\mathbf{u}} \cdot p_{|\mathbf{q}.\mathbf{u}}\,.$$



If, for every element g of G the set $\{g_{|\mathbf{u}}, \mathbf{u} \in {}^*\}$ is finite, the action is said to be *finite state*. It is easy to see that such a finite state self-similar action corresponds to exactly one automaton group, possibly with infinite stateset. A quick way to describe an automaton group is to give the section decomposition (3.3) of all elements of the stateset.

The correspondence between Mealy automata and self-similar groups can be summarized as:

$$\rho_q(x) = y \text{ and } \delta_x(q) = p \quad \Longleftrightarrow \quad q_{|x} = p \text{ and } \pi(q).x = y\,,$$

which we represent by the arrow notation $q \xrightarrow{x|y} p \ \in \mathcal{A}$. The stateset of the automaton corresponds to a generating set of the self-similar group.

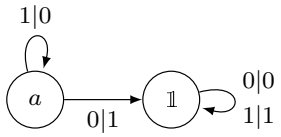


Figure 3.3: The adding machine, generating $\mathbb{Z}$

Example 3.2.2.1. *The self-similar group $a = \langle \mathbb{1}, a\rangle(0,1)$ depicted Figure 3.3 generates a group isomorphic to $\mathbb{Z}$.*
Indeed one easily sees that the state $\mathbb{1}$ indeed induces the identity function other Σ^*. Now we show that a has infinite order: notice that one sees a word $\mathbf{u}$ in Σ^ℓ as a binary digit written from right to left, then the action of a corresponds to adding $1 \mod 2^\ell$ to the digit represented by $\mathbf{u}$, so the order of a can be arbitrary large, hence is infinite. Finally, since $\langle\mathcal{A}\rangle$ is an infinite monogenic group, it is isomorphic to $\mathbb{Z}$.

3.3 An example of an infinite Burnside (automaton) group

3.3.1 Infiniteness of the Grigorchuk group

For the **Grigorchuk group** lots of properties are known. For instance we can prove that it is **infinite** :

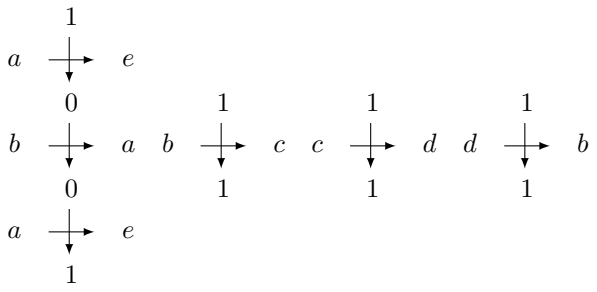
First, we can see that $e = \mathbb{1}_{\Sigma^*}$ is the identity function, because e is a sink state which copies the input word on th output.

We are going to construct an infinite number of elements via a morphism η defined by:

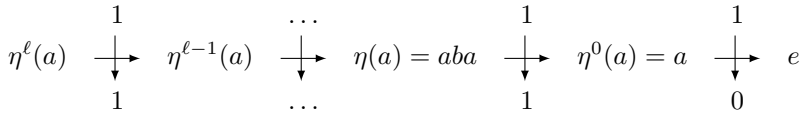
$$\begin{aligned} \eta : \{a,b,c,d\}^* &\to \{a,b,c,d\}^* \\ a &\mapsto aba \\ b &\mapsto d \\ c &\mapsto b \\ d &\mapsto c \end{aligned}$$

Lemma 3.3.1.1. *The elements $\eta^\ell(a)$ are pairwise different in the Grigorchuk group.*

Proof. We show that the $\eta^\ell(a)$ act differently on 1^ω. We have:



So, as e acts like the identity in the group, it can be ignored when it appears in a word, we have:



hence every $\eta^\ell(a)$ acts differently on 1^ω, so they represent different elements in the group. □

We have proved:

Proposition 3.3.1.2. *The Grigorchuk group is infinite*

Another way to prove this result is through a very interesting property of the action:

Proposition 3.3.1.3 (Fractal action)**.** *The action of the Grigorchuk group is* fractal*, i.e.:*

$$\forall g \in \langle \mathcal{G} \rangle, \forall \mathbf{u} \in \Sigma^*, \exists h \in \langle \mathcal{G} \rangle \cup St_{\langle \mathcal{G} \rangle}(\mathbf{u}),\ \ h \ \begin{array}{c}\mathbf{u}\\ \downarrow \\ \mathbf{u}\end{array}\ g = h_{|\mathbf{u}}$$

Proof. Consider the subgroup of elements of $\langle \mathcal{G} \rangle$ that leave the first letter invariant, then this subgroup contains b, c, d, aba, aca, ada. Now the images of this subset after reading the letter 0 (*resp.* 1) is a, b, c, d, which is a generating set for $\langle \mathcal{G} \rangle$, hence one can obtain any element of $\langle \mathcal{G} \rangle$ after reading and stabilizing any word of size 1. We conclude using an induction on the size of the word $\mathbf{u}$. □

Now this can be used to show that the action of $\langle \mathcal{G} \rangle$ is *level transitive*, i.e. that given any pair of words $(\mathbf{u}, \mathbf{v}) \in (\Sigma^\ell)^2$, there exists an element $g \in \langle \mathcal{G} \rangle$ such that $g.\mathbf{u} = \mathbf{v}$:

Proposition 3.3.1.4 (Level transitive)**.** *The Grigorchuk group is level transitive.*

Proof. Let $(u_1 \dots u_\ell, v_0 \dots v_\ell) = (\mathbf{u}, \mathbf{v}) \in (\Sigma^\ell)^2$, we are going to construct explicitly an element that changes $\mathbf{u}$ to $\mathbf{v}$. If $u_j = v_j$ then we have nothing to do on the j-th level, so we can take $g_j = \mathbb{1}$. Otherwise, we use fractalness to find an element of $\langle \mathcal{G} \rangle$ which acts like a after reading $u_1 \dots u_{j-1}$. Hence the action of g_j on $\mathbf{u}$ consist exactly in flipping the j-th bit, leaving the rest of the word unchanged. Now $g_\ell \dots g_1.\mathbf{u} = g_j \dots g_1.u_1 \dots u_j v_{j+1} \dots v_\ell = \mathbf{v}$.

$$\begin{array}{lccccccc}
 & u_1 & & u_2 & & u_3 & & u_4 \\
g_4 & \downarrow & . & \downarrow & . & \downarrow & \delta_{u_4,v_4}a & \downarrow & e \\
 & u_1 & & u_2 & & u_3 & & v_4 \\
g_3 & \downarrow & . & \downarrow & \delta_{u_4,v_4}a & \downarrow & e & \downarrow & e \\
 & u_1 & & u_2 & & v_3 & & v_4 \\
g_2 & \downarrow & \delta_{u_4,v_4}a & \downarrow & e & \downarrow & e & \downarrow & e \\
 & u_1 & & v_2 & & v_3 & & v_4 \\
g_1 = \delta_{u_4,v_4}a & \downarrow & e & \downarrow & e & \downarrow & e & \downarrow & e \\
 & v_1 & & v_2 & & v_3 & & v_4 &
\end{array}$$

□

Finally, as the group is transitive on a set of arbitrary large size, it must be infinite.

3.3.2 Order of elements in the Grigorchuk group

We are now going to prove that the group generated by the Grigorchuk automaton is an infinite Burnside group.

One of the crucial observation for our proof is that the subgroup generated by b, c, d is finite: $\langle b, c, d\rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The relations are:

$$bc = cb = d \; ; \; bd = db = c \; ; \; cd = dc = b \, . \tag{3.4}$$

The proof is a simple verification and can be done with cross diagrams or via computer assisted computations.

This and the fact that a is of order 2 means that we can write all elements in the Grigorchuk group in a simple fashion: all element can be written as

$$a^{\varepsilon_0} x_1 a x_2 a \dots a x_i a \dots a x_\ell a^{\varepsilon_\ell} \, , \tag{NF}$$

with $\varepsilon_0, \varepsilon_\ell \in \{0, 1\}$ and $x_j \in \{b, c, d\}$.

Let us recall that the *conjugate* of g by h is the group element $h^{-1}gh$.
We need the small lemma:

Lemma 3.3.2.1. *If g has finite order n, then so does each of its conjugates.*

Proof. we compute $(h^{-1}gh)^n = h^{-1}ghh^{-1}gh \dots h^{-1}gh = h^{-1}g^n h = h^{-1}eh = e$. So $h^{-1}gh$ has order less than n, we get the other inequality by symmetry: g is conjugate to $h^{-1}gh$ by h^{-1}. □

We now have all the tools we need to prove

Theorem 3.3.2.2. *The group $\langle \mathcal{G}\rangle$ has every element of finite order.*

Proof. Let $g \in \langle \mathcal{G}\rangle$. We are going to do an induction on the length of the shortest representative of g on Q^*. Let ℓ be this shortest length and $\mathbf{w}$ be a word on Q of length ℓ representing g in $\langle \mathcal{G}\rangle$. As the product of two element of $S := Q \setminus \{a\}$ is an element of S (3.4), we can assume that $\mathbf{w}$ is written as an alternation of an a and a letter of S. On can show[1] for initialisation, that if $\ell < 3$, then g has finite order.

Assume ℓ is *odd*. If $\mathbf{w}$ starts with an a, then $\mathbf{w} = a\mathbf{u}a = \mathbf{u}^a$ (since $a^{-1} = a$), with $\mathbf{u}$ a word on Q of length $\ell - 2$. Hence we can use the induction of u, and since conjugation does not change the order (Lemma 3.3.2.1), g has finite order.
If $\mathbf{w}$ starts with $p \in S$, then $\mathbf{w} = p\mathbf{u}q$, $q \in S$. We can conjugate by p^-1 : $g^{p^{-1}} = p^{-1}p\mathbf{u}qp$. The word $\mathbf{u}r$ has length at most $\ell - 1$ (since $q.p = r \in S$, (3.4)), whence the order of g (which is equal to the order of $\mathbf{u}r$) is finite order using the induction hypothesis.

Now is ℓ is *even*. By conjugation we can assume that $\mathbf{w}$ starts with an a.
We are going to split the analysis into sub-cases depending on the length of $\mathbf{w}$.
If 4 divides ℓ, then $\mathbf{w} = aw_1au_1aw_2a \dots aw_{\ell/4}au_{\ell/4}$ and we can group the letters of w into blocks aw_ia and w_j. As $\mathbf{w}$ has an even number of a, $\mathbf{w}$, can be decomposed as $(\mathbf{w_0}, \mathbf{w_1})()$[2], where $\mathbf{w}_\epsilon$ ($\epsilon \in \{0, 1\}$) have length

[1] Using computer or by hand
[2] *i.e.* $\mathbf{w}$ acts like $\mathbf{w}_0$ after reading a 0 and as $\mathbf{w}_1$ after reading a 1, And that the first letter read is not modified by $\mathbf{w}$.

at most $\ell/2$, since blocks aw_ia can be decomposed as $aw_ia = (s,t)$ with $s,t \in Q$. So, the order of g is the lowest common multiple of the orders of $\mathbf{w}_\epsilon$, finite by the induction.
Finally, if $\ell = 4j-2$, we consider g^2, represented by $\mathbf{ww}$.

1. if $\mathbf{w}$ contains a letter d, then the length of $(\mathbf{w}_\epsilon)$ is lesser or equal to $4j-3$ and we can conclude.
2. if $\mathbf{w}$contains a letter c then the words $\mathbf{w}_\epsilon$ are either of size lesser or equal to $4j-3$, or contain a d, and we conclude using the previous case on $\mathbf{w}_\epsilon$.
3. otherwise, the word $\mathbf{w}$ is a power ab, hence of finite order.

□

Using Corollary 3.3.1.2, we get:

Theorem 3.3.2.3 (Grigorchuk 1980 [Gri80])**.** *The group $\langle \mathcal{G} \rangle$ generated by the Grigorchuk automaton $\mathcal{G}$ is an infinite Burnside group.*

Remark 3.3.2.4.
- *The Grigorchuk group is not the only infinite Burnside automaton group, indeed several generalization led to a countable number of examples.*
- *Automaton groups such as in Remark 2.0.0.6 are not known.*

Chapter 4

Growth of groups

4.1 Cayley graph

A very nice way to describe a group goes through a geometrization called the Cayley graph:

Definition 4.1.0.1 (Cayley graph)**.** *Let G be a group with (finite) generating set S. The* Cayley graph $\Gamma_{G,S}$ *of G, S is the graph whose vertices are the element of the group and edges are*

$$g \xrightarrow{s} g.s \quad g \in G,\ s \in S\,.$$

This graph provides a fresh view on the properties of the group. For instance, if the Cayley graph (seen as a continuous metric space) is δ-hyperbolic then the group (which will be called word-hyperbolic, Gromov-hyperbolic or simply hyperbolic) has many interesting algebraic properties [CEH+92]. It also motivates the study of the group through geometry and combinatorics.

This vision also induce a natural metric on the group: for any $w = s_1 \dots s_n$ in S^*, we call *length* of w with respect to S is

$$|w| = |s_1 \dots s_n| = n.$$

By convention the empty word as length zero. For any g in G, we call *norm* of G with respect to S the number

$$\|g\|_S := \inf\{|w| : w \in S, w =_G g\}\,.$$

The terminology is justified by the

Proposition 4.1.0.2. *The function $\|\cdot\|_S : G \to \mathbb{R}_{\geq 0}$ satisfies*

1. $\forall g, h \in G, \|gh\|_S \leq \|g\|_S + \|h\|_S$,
2. $\|g\|_S = 0$ *if and only if* $g = \mathbb{1}$ *is the neutral element.*

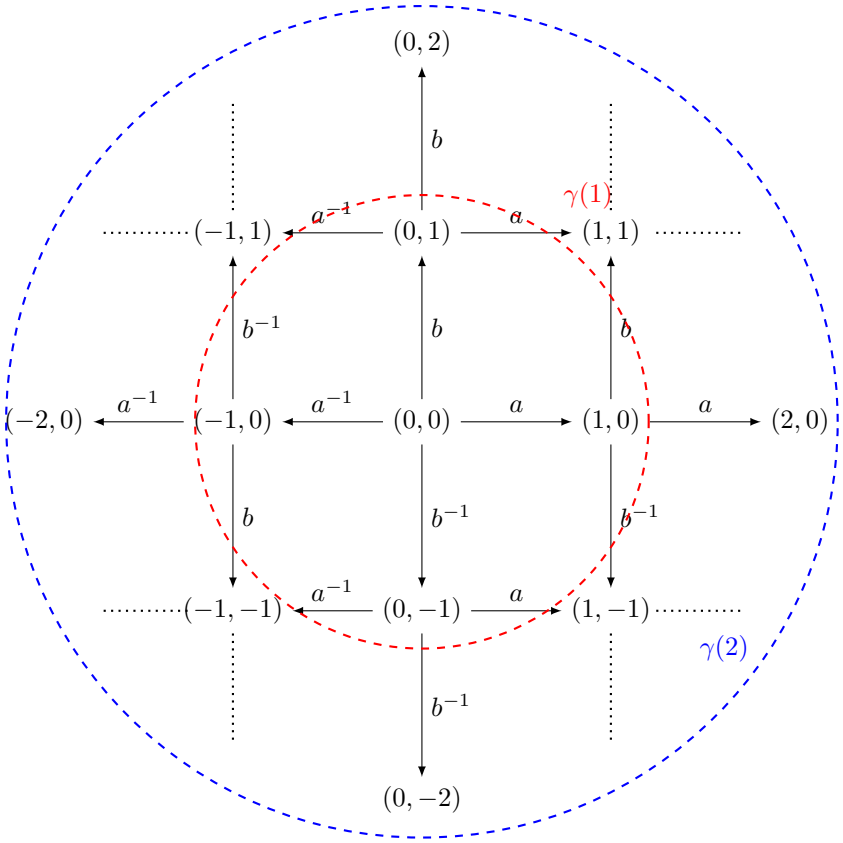


Figure 4.1: The Cayley graph of $\mathbb{Z}^2$ with generators $S = \{a^{\pm 1} = (0, \pm 1), b^{\pm 1} = (\pm 1, 0)\}$, along with the balls of radii 1 (red) and 2 (blue)

Moreover, the infimum is in fact a minimum.

A word w is a *minimal representative* of a group element g if $|w|_S = \|g\|_S$. It always exists but may not be unique. Observe that a subword of a minimal word is also minimal.

Proof. Let $g \neq e$. By assumption there is a word w in S representing g, so $\|g\|_S$ is finite. Since there are only finitely many words in S^* of length less than $|w|_w$, so the infimum is a minimum. Moreover only the empty word (representing the neutral element) has zero length. This prove second point. Finally let w_g and w_h be minimal representative words of g and h, then $w_g w_h$ represents gh, the first assertion follows. □

This word norm induces a metric $d_S(x, y) := \|x^{-1}y\|_S$ on G. Recall that a metric is a function $d : G \times G \to \mathbb{R}_{\geq 0}$ such that for all $x, y, z \in G$, we have $d(x, z) \leq d(x, y) + d(y, z)$ and that $d(x, y) = 0$ if and only if $x = y$. This metric is left-invariant under the group action in the sense that $d_S(gx, gy) = d_S(x, y)$ for all g, x, y in G. Observe that this metric is symmetric, which means $d_S(x, y) = d_s(y, x)$ for all x, y, if and

only if S is symmetric.

When we identify the group G with the vertices of its Cayley graph $\Gamma_{G,S}$, the metric d_S coincides with the metric inherited by the vertex set when we declare that each oriented edge labelled by s has length 1. It implies that the path in $\Gamma_{G,S}$ defined by following edges labelled by the letters of a minimal word w is a geodesic (i.e. shortest) path from the starting point x to the end point $y = xw$.

4.2 Growth function

Definition 4.2.0.1. *The* ball *of radius ℓ and centre x in (G, d_S) is the set*

$$B_{G,S}(x, \ell) := \{y \in G : d_S(x, y) \leq \ell\}.$$

The growth *function of G with respect to (S) counts the sizes of the balls*

$$\gamma_{G,S}(\ell) = \#B_{G,S}(x, \ell)\,.$$

By left-invariance, the size of a ball in a group depends only on the radius ℓ and not on the centre x. To fix ideas, one may choose $x = e$.

Let us say that two functions f, g are *equivalent* when there exists $c > 0$ such that $g(\frac{1}{c}\ell) \leq f(\ell) \leq g(c\ell)$ for all $\ell \geq 0$. The next lemma ensures that the equivalence class of $\gamma_{G,S}(\ell)$ does not depend on S. This class is called the growth *rate* of G, and denoted by abuse of notation $\gamma_G(\ell)$.

Lemma 4.2.0.2. *Let (S) and (T) be two finite weighted generating sets of the group G, then there exists $c > 0$ such that $\gamma_{G,S}(\ell) \leq \gamma_{G,T}(c\ell)$ for all ℓ.*

Proof. Let $c := \max\{\, \frac{\|s\|_T}{\|s\|_S} \,|s \in S\} \in]0\,, \infty[$. If $g \in B_{G,S}(\ell)$ then there exists a minimal representative word $w = s_1 \dots s_n$ in S^* we have

$$\|g\|_T \leq \sum_{i=1}^{n} \|s_i\|_T \leq c \sum_{i=1}^{n} \|s_i\|_S \leq c\ell.$$

□

Definition 4.2.0.3. *A group G has*

- polynomial *growth if $\gamma_G(\ell)$ is bounded above by a polynomial function,*
- exponential *growth if there is $c > 0$ such that $\gamma_G(\ell) \geq \exp(c\ell)$ for all ℓ,*
- intermediate *growth if $\gamma_G(\ell)$ is greater than any polynomial function and lesser than any exponential function:*

$$\forall d \in \mathbb{Z}, \alpha \in \mathbb{R}_{>0}, \exists N, \forall \ell \geq N, \ell^d \leq \gamma_G(\ell) \leq \exp(\alpha\ell).$$

Another, equivalent, way to describe the type of growth is to consider $\alpha = \lim_{\ell\to\infty} \sqrt[\ell]{\gamma_G(\ell)}$ the *exponential growth rate*[1]. One can show by direct computation that $\alpha > 1$ if ad only if G has exponential growth rate.

Proposition 4.2.0.4. *The growth function of $\mathbb{Z}^2$ with generators $S = \{a^{\pm 1} = (0, \pm 1), b^{\pm 1} = (\pm 1, 0)$ satisfies*

$$\gamma_{\mathbb{Z}^2,S}(\ell) = 2\ell^2 + 2\ell + 1$$

Proof. We proceed by induction on the radius of the ball. For $\ell = 0, 1$ the formula holds. Assume it is true for $\ell - 1 > 0$. The sphere of radius ℓ in the Cayley graph corresponds to a discrete square of diagonal $2\ell + 1$, hence is of size $4(\ell + 1) - 4 = 4\ell$. We get

$$\begin{aligned}\gamma_{\mathbb{Z}^2,S} &= 2(\ell-1)^2 + 2(\ell-1) + 1 \ + \ (4\ell) \\ &= 2\ell^2 - 4\ell + 2 + 2\ell - 2 + 1 \ + \ (4\ell) \\ &= 2\ell^2 + 2\ell + 1\end{aligned}$$

□

Accordingly we can show, *e.g.* by induction on the dimension d, that $\mathbb{Z}^d$ with the standard set of generators, has growth a polynomial of degree d (*hint*: fix one coordinate on the sphere on the Cayley graph.)

Proposition 4.2.0.5. *The growth function of $\mathbb{F}_d$ with generators $S = \{a_1^{\pm 1}, \dots, a_d^{\pm 1})$ satisfies*

$$\gamma_{\mathbb{F}_d,S}(\ell) = \frac{2d(2d-1)^{\ell+1}}{2(d-1)}$$

Proof. We carry the proof for $d = 2$, the other cases are treated similarly. Since the group is free, if g is an element of length $\ell \geq 1$, then gs has length $\ell + 1$ for all but one of the $2d$ elements of S. Hence the size of the sphere of radius $\ell + 1$ is $2d - 1$ the size of the one of radius ℓ, and the growth is a geometric sequence of common ration $2d - 1$. Hence the result. □

Proposition 4.2.0.6. *The growth function of the Heisenberg group $\mathbb{H} = \langle \begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&1&1\\0&0&1 \end{pmatrix} \rangle$ has growth function equivalent to a polynomial of degree 4.*

Proof. Let $x = \begin{pmatrix} 1&1&0\\0&1&0\\0&0&1 \end{pmatrix}, y = \begin{pmatrix} 1&0&0\\0&1&1\\0&0&1 \end{pmatrix}, z = \begin{pmatrix} 1&0&1\\0&1&0\\0&0&1 \end{pmatrix}$. Since the degree of the polynomial does not depend on the generating set, we carry the proof for $S = \{x, y, z\}^{\pm 1}$

First notice $[x, y] = z$ (so $[y, x] = z^{-1}$ and $yxz^{-1} = xy$) and that z commutes with x and y (Hence we can put any word of $\mathbb{H}$ under a normal form $x^a y^b z^c$). Moreover $x^a y^b = \begin{pmatrix} 1&a&ab\\0&1&b\\0&0&1 \end{pmatrix}$ and $\left[x^a, y^b\right] = \begin{pmatrix} 1&0&ab\\0&1&0\\0&0&1 \end{pmatrix}$ (generally $\begin{pmatrix} 1&a&c\\0&1&b\\0&0&1 \end{pmatrix} \times \begin{pmatrix} 1&\alpha&\gamma\\0&1&\beta\\0&0&1 \end{pmatrix} = \begin{pmatrix} 1&a+\alpha&c+\gamma+a\beta\\0&1&c+\gamma\\0&0&1 \end{pmatrix}$). Hence $\|x^a y^b z^c\| \leq |a| + |b| + 4\lfloor\sqrt{|c|}\rfloor + (c - \lfloor\sqrt{|c|}\rfloor^2) \leq |a| + |b| + 4\lfloor\sqrt{|c|}\rfloor + (c^2 - (\sqrt{c} - 1)^2) \leq |a| + |b| + 6\lfloor\sqrt{|c|}\rfloor \leq |a| + |b| + 6\sqrt{|c|}$.

[1] This limit exists because the log of the growth is a subadditive function, hence $\log \gamma_{G,S}(\ell + m)/\ell + m$ converges by Fekete lemma and so does $\sqrt[\ell]{\gamma_{G,S}(\ell)} = \exp \log \gamma_{G,S}(\ell)/\ell$

On the other hand we have that $\|x^a y^b z^c\| \geq |a| + |b|$, because the a and c coordinate behave like additive groups.
In addition $\|x^a y^b z^c\| \geq \sqrt{|c|} - 1$, because one need at least $\lfloor\sqrt{|c|}\rfloor + c - (\lfloor\sqrt{|c|}\rfloor)^2$ elements which is greater or equal than $\lfloor\sqrt{|c|}\rfloor + c - (\lfloor\sqrt{|c|}\rfloor)^2 \geq \sqrt{|c|} - 1$.

Hence

$$\frac{1}{2}\left(|a| + |b| + \sqrt{|c|} - 1\right) \leq \|x^a y^b z^c\| \leq |a| + |b| + 6\sqrt{|c|}$$

We are now able to conclude by counting the number of possible (pairwise different) $x^a y^b z^c \in \mathbb{H}$ in balls of radii ℓ. □

Lemma 4.2.0.7. *If $H \leq G$ is a subgroup of finite index, then*

$$\gamma_H(\ell) \asymp \gamma_G(\ell)$$

Proof. Assume $G = \langle S \rangle$ and $H = \langle T \rangle$. Since changing the generating set does not change the asymptotic behaviour of the growth function, we can take $G = \langle S \cup T \rangle$. This immediately gives $\#B_G(\ell) = \gamma_H(\ell) \geq \gamma_G(\ell)$. Now to get the other direction, since H is of finite index, there exists $g_1, \ldots, g_k$ such that $G = \bigcup_i g_i H$. In particular, for each element $g \in G$ there exists a unique i such that $g_i g \in H$. Moreover as $g = s_1 \ldots g_k | s_i \in S$, we can write $g g_i = s_1 t_1 . (t_1^{-1} s_2) t_2 \ldots (t_{k-1}^{-1} s_k) g_i$, such that each $t_j^{-1} s_{j+1} t_{j+1}$ belong to H. Let $K = \max_i \|t_j^{-1} s_{j+1} t_{j+1}\|_H$, we get $\gamma_G(\ell) \leq \gamma_H(K\ell)$. □

4.3 Milnor problem

As we saw, the growth function of a group is a nice way to classify groups, since it is invariant from the generating set set. A first obvious observation is:

Proposition 4.3.0.1. *A group has finite growth if and only if it is finite.*

But a more interesting question is to know if the growth somehow characterize an algebraic property. As for Burnside problem in 1902, the examples of growth of infinite growth showed until the eighties a dichotomy: it was either polynomial or exponential. Whence the question of Milnor:

Question 4.3.0.2 (Milnor 1968 [Mil68])**.**
1. *Are there groups of intermediate growth between polynomial and exponential?*
2. *What are the groups with polynomial growth?*

The first question was solved by Gromov, who showed sec:poly

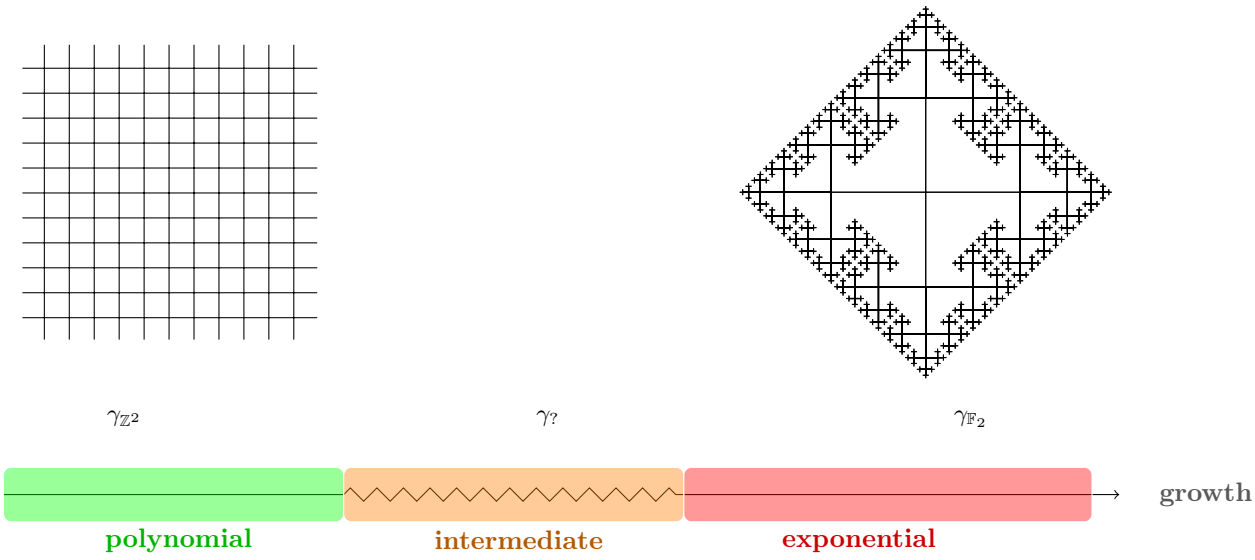


Figure 4.2: A (very) rough summarize of Milnor problem.

4.4 Gromov theorem on polynomial growth

We state here a deep result of Gromov without giving a proof. Yet it worth mentioning it for it completes the picture of growth of group and is probably one of the most important theorem in geometric group theory

Definition 4.4.0.1 ((virtually) nilpotent group)**.** *A group G is called* nilpotent *if the sequence*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$

where $G_{i+1} = [G_i, G]$, ends in finitely many steps.
A group G is called virtually nilpotent *if it has a subgroup of finite index which is nilpotent.*

Notice that Abelian groups are 1-step nilpotent, and in some sense, nilpotency is a generalization of commutativity.

We saw that Abelian groups have polynomial growth. The following is the natural generalization:

Theorem 4.4.0.2. *Bass, Guivarc'h 1972-73 A nilpotent group as polynomial growth.*

The proof of this theorem is mostly tedious but does not involve any really new construction. However the reciprocal lead to numerous innovations and remains a very deep and difficult theorem whose proof would be itself a full course.

Theorem 4.4.0.3 (Gromov 1981 [Gro81])**.** *A group has polynomial growth if and only if it is virtually nilpotent.*

This theorem has multiple consequences in geometric and combinatorial group theory. For instance, with the following:

Lemma 4.4.0.4. *Let $G \triangleright H$ be groups. For each element $g \in G$, the order of gH in G/H divides the order of g in G*

Proof. Let $\gamma > 0$ be the order of g in G. We have in G/H that $(gH)^\gamma = g^\gamma H = \mathbb{1}H = H$, so the order of gH in G/H divides γ □

and

Lemma 4.4.0.5. *An infinite nilpotent group has elements of infinite order*

Proof. We prove the reciprocal, by induction on the nilpotency class. If it is 1 (i.e. the group is Abelian), we already proved the result in Lemma 2.0.0.3. Otherwise, let G be a Burnside group of nilpotency class d. The group $[G, G]$ is torsion free (for it is a subgroup of G), and is $d-1$ step nilpotent, hence finite by the induction hypothesis. Moreover $G/[G, G]$ is Abelian and torsion (Lemma 4.4.0.4), hence finite, since $|G| = |G/[G, G]| \times |[G, G]|$, G is finite. □

We get:

Corollary 4.4.0.6. *An infinite Burnside group has super-polynomial growth.*

And indeed, as we are going to show, the Grigorchuk group, studied Section 3.3, grows faster than any polynomial.

4.5 A group of intermediate growth

As we saw Proposition 3.3.1.2, the Grigorchuk group is infinite. Since it is also Burnside, we know that is as super polynomial growth (see Corollary 4.4.0.6, but this will be proven explicitly later in Section 4.5.1). Beside being the first example of such a group, Grigorchuk group (and more generally automaton groups) are of the highest importance in the study of groups of intermediate growth: indeed all[2] known examples of groups of intermediate growth are based on automaton groups. Here we give an (hopefully) self-contained proof that the Grigorchuk group is of intermediate growth. Our proofs and plan is based on several articles with the same purpose [GP08, dlH00, Zuk06], simplify the original proof [Gri84].

[2] In a recent preprint [Nek18], Nekrashevych constructs simple groups of intermediate growth. This construction does not involve directly automaton groups but is based on a dynamical system inspired by the Grigorchuk group.

4.5.1 The Grigorchuk group has superpolynomial growth

In order to prove that the Grigorchuk group has superpolynomial growth, we are going to apply a two-fold strategy: first we are going to focus to a group, the stabilizer of the first level, and show that it is of finite index ; then we will show that this group surjects on two copy of itself, thus cannot have polynomial growth.

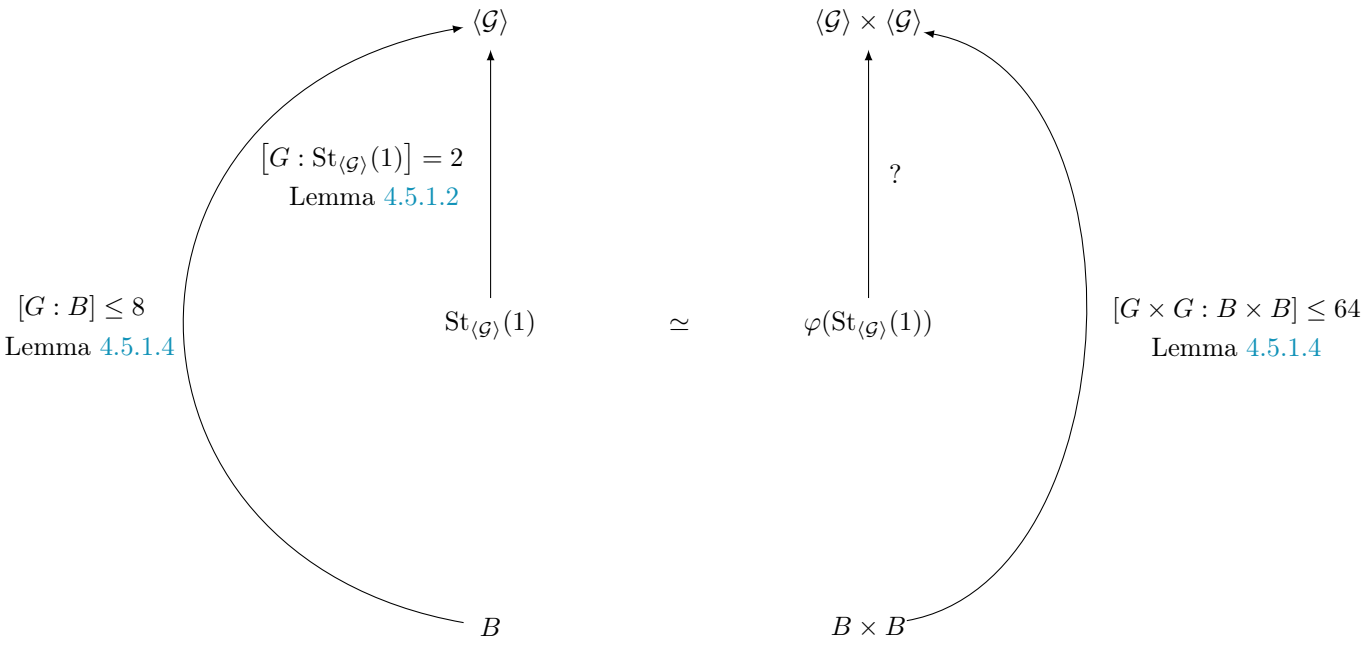


Figure 4.3: General strategy of the proof of superpolynomiality of the Grigorchuk group.

Definition 4.5.1.1 (Stabilizer)**.** *Let G be an automaton group on alphabet Σ. The* stabilizer *of the n-th level is the subgroup of elements g of G that leave words of size at most n invariant.*

$$St_{\langle \mathcal{G} \rangle}(n) = \{g \in G | \forall \mathbf{u} \in \Sigma^n, g.\mathbf{u} = \mathbf{u}\} .$$

This set is always a subgroup of G, but in the case of the Grigorchuk group we can elaborate, using the normal form (NF):

Lemma 4.5.1.2. *The stabilizer of the first level of the Grigorchuk group is generated by $\{b, c, d, aba, aca, ada\}$. Moreover it has finite index 2.*

Proof. Using (NF), we know that all elements of the Grigorchuk group can be written $a^{\varepsilon_0} x_1 a x_2 a \dots a x_i a \dots a x_\ell a^{\varepsilon_\ell}$ with $\varepsilon_0, \varepsilon_\ell \in \{0, 1\}$ and $x_j \in \{b, c, d\}$. We can check that $b, c, d \in \mathrm{St}_{\langle \mathcal{G} \rangle}(1)$ and so do aba, aca and ada, but $a \notin \mathrm{St}_{\langle \mathcal{G} \rangle}(1)$ (because a flips the first letter). More precisely we can show, by induction on the length of

the element, that an element is in $\mathrm{St}_{\langle\mathcal{G}\rangle}(1)$ if and only if it can be written with an even number of a. This plus (NF) gives that $\mathrm{St}_{\langle\mathcal{G}\rangle}(1) = \langle b, c, d, aba, aca, ada\rangle$. Moreover this also means that $\langle\mathcal{G}\rangle = \mathrm{St}_{\langle\mathcal{G}\rangle}(1) \cup a\mathrm{St}_{\langle\mathcal{G}\rangle}(1)$, thus that $\mathrm{St}_{\langle\mathcal{G}\rangle}(1)$ is a subgroup of index 2. □

More generally, we can prove a result that will be important to prove subexponentiality:

Lemma 4.5.1.3. *The n-th level stabilizer has finite index bounded by* 2^{2^n-1}.

Proof. Going back to the definition of index, we are looking for the minimal number of element of G such that $\langle\mathcal{G}\rangle = \bigcup_g g\mathrm{St}_{\langle\mathcal{G}\rangle}(n)$. Consider the subgroup T_n of automorphisms acting only on the first n level of the tree. Then $\langle\mathcal{G}\rangle = \bigcup_{g\in T_n} g\mathrm{St}_{\langle\mathcal{G}\rangle}(n)$, and using fractalness of the action (Proposition 3.3.1.3) and the transitivity of $\langle\mathcal{G}\rangle$ on the first level we get $T_n \leq \langle\mathcal{G}\rangle$. The result follows since $|T_n| = 2^{2^n-1}$. □

Define the morphism $\varphi : \mathrm{St}_{\langle\mathcal{G}\rangle}(1) \to \langle\mathcal{G}\rangle \times \langle\mathcal{G}\rangle, g \mapsto (g_{|0}, g_{|1})$. This is a surjection componentwise, because:

- $\varphi(b) = (a, c)$
- $\varphi(c) = (a, d)$
- $\varphi(d) = (\mathbb{1}, b)$
- $\varphi(aba) = (c, a)$
- $\varphi(aca) = (d, a)$
- $\varphi(ada) = (b, \mathbb{1})$

whence $\varphi(\mathrm{St}_{\langle\mathcal{G}\rangle}(1)) \simeq \mathrm{St}_{\langle\mathcal{G}\rangle}(1)$.

Proposition 4.5.1.4. *The group* $St_{\langle\mathcal{G}\rangle}(1) \simeq \varphi(St_{\langle\mathcal{G}\rangle}(1)) \leq \langle\mathcal{G}\rangle \times \langle\mathcal{G}\rangle$ *is of finite index.*

Proof. Define $B = \langle b\rangle^{\langle\langle\mathcal{G}\rangle\rangle} = \langle g^{-1}1bg, g \in \langle\mathcal{G}\rangle\rangle$. Since $\langle\mathcal{G}\rangle = \langle a, b, d\rangle$), $\langle\mathcal{G}\rangle/\langle B\rangle$ is a quotient of $\langle a, d\rangle$ which is of order 8 (since $a^2 = d^2 = (ad)^4 = \mathbb{1}$). Hence $[\langle\mathcal{G}\rangle : B] \leq 8$.
Now consider $\varphi(\mathrm{St}_{\langle\mathcal{G}\rangle}(1))$. We have $\varphi(\mathrm{St}_{\langle\mathcal{G}\rangle}(1)) \supset \langle\varphi(d), \varphi(ada)\rangle = \langle(b, \mathbb{1}), (d, \mathbb{1})\rangle$. Then for any $\mathrm{St}_{\langle\mathcal{G}\rangle}(1) \ni x$ with $\varphi(x) = x_0, x_1$ we have $\varphi(d^x) = (x_0^{-1}, x_1^{-1})(\mathbb{1}, b)(x_0, x_1) = (\mathbb{1}, b^x)$, whence $1 \times B \subset \varphi H$. The same reasoning using ada gives $B \times 1 \subset \varphi H$ so $B \times B \subset \varphi H$. We obtain $B \times B \subset \varphi\mathrm{St}_{\langle\mathcal{G}\rangle}(1) \simeq \mathrm{St}_{\langle\mathcal{G}\rangle}(1) \times \mathrm{St}_{\langle\mathcal{G}\rangle}(1) \subset \langle\mathcal{G}\rangle \times \langle\mathcal{G}\rangle$. We get that $\left[\langle\mathcal{G}\rangle \times \langle\mathcal{G}\rangle : \mathrm{St}_{\langle\mathcal{G}\rangle}(1) \times \mathrm{St}_{\langle\mathcal{G}\rangle}(1)\right] \leq [\langle\mathcal{G}\rangle \times \langle\mathcal{G}\rangle : B \times B] = [\langle\mathcal{G}\rangle : B] \leq 8^2 = 64$. □

Using the former and Lemma 4.2.0.7 we get

$$\gamma_G(\ell) \asymp \gamma_{G\times G}(\ell)\,,$$

whence the growth function cannot be a polynomial.

4.5.2 The Grigorchuk group has subexponential growth

The basic idea in this section is to consider the subgroup of stabilizer of the first level, in order to apply φ three times. In this process we are going to get 8 words for each element of $\mathrm{St}_{\langle\mathcal{G}\rangle}(3)$, and the key property will be that the sum of these words will be shorter than the length of the original word. Using this and the fact that stabilizers have finite index in the Grigorchuk group, we will prove subexponential growth.

Lemma 4.5.2.1. *Let $g \in St_{\langle\mathcal{G}\rangle}(3)$ and $(g_{000}, \dots, g_{111}) = \varphi^3(g)$. Then*

$$|g| \leq 3/4 \sum_{i=000}^{111} |g_i| + 8\,.$$

Proof. Let l_s be the number of $s \in \{b, c, d\}$ in g. We are going to apply a strategy analogous to the last part of the proof of Theorem 3.3.2.2. Using the normal form (NF), reductions, and φ, we get that

$$\begin{aligned} |g_0| + |g_1| &\leq |g| - l_d + 1 \\ |g_0 0| + |g_1 1| &\leq |g_0| + |g_1| - l_c + 2 \\ |g_0 0| + |g_1 1| &\leq |g_0| + |g_1| - l_c + 4 \end{aligned}$$

Moreover, from the normal form, $\sum_{i\in\{b,c,d\}} l_i \geq (|g| - 1)/2$, so there exists a generator $s \in \{b, c, d\}$ such that $l_s \geq |g|/6 - 1$. We can now conclude.

□

We are now able to prove the sub exponentiality of $\mathrm{St}_{\langle\mathcal{G}\rangle}(3)$, which is of finite index in $\langle\mathcal{G}\rangle$:

Proposition 4.5.2.2. *The group $St_{\langle\mathcal{G}\rangle}(3)$ has subexponential growth.*

Proof. From Lemma 4.5.2.1, we get that

$$B_{\mathrm{St}_{\langle\mathcal{G}\rangle}(1)}(\ell) \subset \prod_{k_{000}+\dots+k_{111}\leq 3/4\ell+8} B_{\langle\mathcal{G}\rangle}(k_i))$$

Since $\mathrm{St}_{\langle\mathcal{G}\rangle}(3)$ has finite index in $\langle\mathcal{G}\rangle$, the number of element in $\langle\mathcal{G}\rangle$ that actually belong to $\mathrm{St}_{\langle\mathcal{G}\rangle}(3)$ can be pretty well understood, as we have done in the proof of Lemma 4.2.0.7. Hence the exponential growth rates (with respect to the chosen generating sets) $\alpha = \lim_{\ell\to\infty} \sqrt[\ell]{B_G(\ell)} = \lim_{\ell\to\infty} \sqrt[\ell]{B_G(\ell)}$ are equal.

Now, by definition of exponential growth rate, for any $\varepsilon > 0$ there exists a constant C such that, for ℓ large enough, $\gamma_G(\ell) \leq C(\alpha + \varepsilon)^\ell$. We get that

$$\gamma_{\langle\mathcal{G}\rangle}(\ell) \leq C(\alpha + \varepsilon)^\ell$$

Using the upper bound of Lemma 4.5.2.1,we get

$$\gamma_{\mathrm{St}_{\langle\mathcal{G}\rangle}(3)}(\ell) \leq C(\alpha+\varepsilon)^{3/4\ell+8}$$

Now, taking the ℓ-th root and the limit when ℓ goes to infinity and ϵ goes to 0, we obtain

$$\alpha = \alpha^{3/4}$$

Hence $\mathrm{St}_{\langle\mathcal{G}\rangle}(3)$ has subexponential growth. □

We have now every tool to prove:

Theorem 4.5.2.3 (Grigorchuk 1983, [Gri84])**.** *The Grigorchuk group has intermediate growth.*

4.5.3 The exact growth of the Grigorchuk group

This section goes far beyond the scope of this course and is mostly a survey of the research that led Erschler and Zheng, together with Bartholdi, to give an (almost) exact growth estimate for the Grigorchuk group.

In the previous section we proved the Grigorchuk group has intermediate growth, without providing any actual bound. However, it is possible to do so, even if the better the bound the more subbtle the proof. The seminal result is

Theorem 4.5.3.1. *Grigorchuk 1983 [Gri84] The growth of the Grigorchuk group is intermediate and bounded by*

$$e^{\sqrt{\ell}} \preccurlyeq \gamma_{\langle\mathcal{G}\rangle}(\ell) \preccurlyeq e^{\alpha\ell}\,,$$

for some $\alpha = \log_{32} 31 \approx .9908$.

This upper bound has been later improved by Bartholdi:

Theorem 4.5.3.2. *Bartholdi 1998 [Bar98] Let* η *be the real root of* X^3-X^2-2X-4 *and let* $\alpha = \frac{\log 2}{\log 2-\log \eta} \approx .7674$. *Then The growth of the Grigorchuk group is bounded by*

$$\gamma_{\langle\mathcal{G}\rangle}(\ell) \preccurlyeq e^{\alpha\ell}\,.$$

This was reproved by Muchnik and Pak in [MP01] using similar method. Notice that one can get very good upper bounds, approximating this value, using computer [BGM18].

On the lower bound hand, the first improvement is due to Leonov:

Theorem 4.5.3.3. *Leonov 2001 [Leo01] Let* $\alpha = \log_{87/22}(2) \approx .504$. *Then The growth of the Grigorchuk group is bounded by*

$$e^{\alpha\ell} \preccurlyeq \gamma_{\langle\mathcal{G}\rangle}(\ell)\,,$$

This was rapidly improved by Bartholdi using the same method and computer-assisted computations:

Theorem 4.5.3.4. *Bartholdi 2001 [Bar01] Let $\alpha = .5157$. Then The growth of the Grigorchuk group is bounded by*

$$e^{\alpha\ell} \preccurlyeq \gamma_{\langle \mathcal{G} \rangle}(\ell) \, .$$

In his thesis, Brieussel gave a sharper estimate using the same technique as Leonov

Theorem 4.5.3.5. *Brieussel 2008 [Bri08] Let $\alpha = \min_{\delta+\gamma+\beta=0} \max\left\{\frac{\log 2}{\log(4-3/2\delta)}, \frac{\log 4}{\log(16-6\delta-3\beta)}, \frac{\log 8}{\log(56+2\delta-4\gamma)}\right\} \approx .5207$. Then the growth of the Grigorchuk group is bounded by*

$$e^{\alpha\ell} \preccurlyeq \gamma_{\langle \mathcal{G} \rangle}(\ell) \, .$$

In a recent preprint, Erschler and Zheng gave a somewhat definitive answer by giving a lower bound matching the upper bound up to an $o(1)$ constant:

Theorem 4.5.3.6. *Erschler–Zheng 2018 [EZ18] The growth of the Grigorchuk group is intermediate and bounded by*

$$e^{\alpha\ell+o(\ell)} \preccurlyeq \gamma_{\langle \mathcal{G} \rangle}(\ell) \preccurlyeq e^{\alpha\ell} \, ,$$

for $\alpha = \frac{\log 2}{\log 2 - \log \eta} \approx .7674$ where η is the real root of $X^3 - X^2 - 2X - 4$.

Their proof does not use a direct combinatorics analysis of the growth but rather some deep results in random walks.

Chapter 5

Conclusion

We showed that finitely generated groups form an easy to define set where many counter-intuitive things can occur. On the other hand, Mealy automata are powerful sources of interesting groups. Moreover, the underlying automaton (hence combinatorial) structure allow some proof to be rather short and elementary: we have not used any theorem that goes further a first lecture in group theory.Now consider

These groups generated by Mealy automata have given several other interesting examples, in particular regarding amenability, by giving an example of amenable but not exponentially amenable group (solving **Day Problem**) ; and continue to provide candidates to test conjectures.

Beside, the general classes of Mealy automata remains rather badly understand, and the mere question *"what are the group that can or cannot be realised as automaton group?"* is still widely opens apart from trivial remarks (an automation group has to be finitely generated, residually finite and with decidable word problem, all finite groups can be realised as automaton groups, the class of automation group is closed under direct product).
This goal is (very) partially reached if one consider subclasses of Mealy automata, yet even very restricted classes can contain groups of high complexity.

Bibliography

[AKL+12] A. Akhavi, I. Klimann, S. Lombardy, J. Mairesse, and M. Picantin. On the finiteness problem for automaton (semi)groups. *International Journal of Algebra and Computation*, 22(6):1–26, 2012.

[AMV17] Y. Antolín, A. Martino, and E. Ventura. Degree of commutativity of infinite groups. *Proceedings of the American Mathematical Society*, 145(2):479–485, 2017.

[Bar98] L. Bartholdi. The growth of Grigorchuk's torsion group. *Internat. Math. Res. Notices*, pages 1049–1054, 1998.

[Bar01] L. Bartholdi. Lower bounds on the growth of a group acting on the binary rooted tree. *International Journal of Algebra and Computation*, 11(01):73–88, 2001.

[BGM18] J. Brieussel, Th. Godin, and B. Mohammadi. Numerical upper bounds on growth of automata groups. *CoRR*, abs/1810.00544, 2018.

[Bri08] J. Brieussel. *Croissance et moyennabilité de certains groupes d'automorphismes d'un arbre enraciné*. PhD thesis, 2008. Thèse de doctorat dirigée par Zuk, Andrzej Mathématiques Paris 7 2008.

[Bur02] W. Burnside. On an unsettled question in the theory of discontinuous groups. *Quart. J. Math.*, 33:230–238, 1902.

[CEH+92] J. W. Cannon, D. B.A. Epstein, D. F. Holt, S. V.F. Levy, M. S. Paterson, and W. P. Thurston. Word processing in groups. *Jones and Barlett Publ., Boston, MA*, 1992.

[CSC10] T. Ceccherini-Silberstein and M. Coornaert. *Cellular automata and groups*. Springer Science & Business Media, 2010.

[Dia18] P. Diaconis. *Probabilizing Fibonacci Numbers*, page 1–12. Cambridge University Press, 2018.

[dlH00] P. de la Harpe. *Topics in Geometric Group Theory*. Chicago Lectures in Mathematics. University of Chicago Press, 2000.

[Ers12] M. Ershov. Golod-shafarevich groups: a survey. *IJAC*, 22(5), 2012.

[EZ18] A. Erschler and T. Zheng. Growth of periodic Grigorchuk groups. *ArXiv e-prints*, February 2018.

[Gol64] E. S. Golod. On nil-algebras and finitely residual groups. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 28:273–276, 1964.

[GP08] R. I. Grigorchuk and I. Pak. Groups of intermediate growth: an introduction. In *Enseign. Math.* Citeseer, 2008.

[Gri80] R. I. Grigorchuk. On Burnside's problem on periodic groups. *Akademiya Nauk SSSR. Funktsional′nyĭ Analiz i ego Prilozheniya*, 14-1:53–54, 1980.

[Gri84] R. I. Grigorchuk. Degrees of growth of finitely generated groups and the theory of invariant means. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 48-5(5):939–985, 1984.

[Gro81] M. Gromov. Groups of polynomial growth and expanding maps. *Publ. Math., Inst. Hautes Étud. Sci*, pages 53–73, 1981.

[GS64] E. S. Golod and I. Shafarevich. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

[Gus73] W. H. Gustafson. What is the probability that two group elements commute? *The American Mathematical Monthly*, 80(9):1031–1034, 1973.

[Hal58] M. Hall. Solution of the Burnside problem for exponent six. *Illinois J. Math.*, 2(4B):764–786, 12 1958.

[IO96] S. V. Ivanov and A. Y. Ol'Shanskii. Hyperbolic groups and their quotients of bounded exponents. *Trans. Amer. Math. Soc*, pages 2091–2138, 1996.

[Leo01] Y. Leonov. A lower bound for the growth of a 3-generator 2-group. *Sbornik: Mathematics*, 192, 12 2001.

[Löh17] C. Löh. *Geometric group theory.* Springer, 2017.

[LS01] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory.* Classics in Mathematics. Springer Berlin Heidelberg, 2001.

[Mil68] J. Milnor. Problem 5603. *Amer. Math. Monthly*, 75(6):685–686, 1968.

[MP01] R. Muchnik and I. Pak. On growth of Grigorchuk groups. *International Journal of Algebra and Computation*, 11(01):1–17, 2001.

[NA68] P. S. Novikov and S. I. Adian. Infinite periodic groups. i, ii, iii. *Mathematics of the USSR-Izvestiya*, 2:665, 1968.

[Nek05] V. Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2005.

[Nek18] V. Nekrashevych. Palindromic subshifts and simple periodic groups of intermediate growth. *Annals of Mathematics*, to appear, 2018.

[Zuk06] A. Zuk. Groupes engendrés par des automates. Seminaire Bourbaki 971, 2006.