What is the Grigorchuk group?

Jake Huryn

Abstract

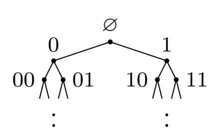
The Grigorchuk group, first constructed in 1980 by Grigorchuk, will be defined in this talk, and some important properties of this group will be explored. In particular, we study it as a negative example to a variant of the Burnside problem posed in 1902, an example of a nonlinear group, and the first discovered example of a group of intermediate growth.

1 The Grigorchuk group Γ

Grigorchuk originally defined his group, which we will denote by Γ, as a set of measure-preserving transformations of the unit interval. We will give a simpler definition in terms of binary trees. First, we must define the object on which Γ will act.

1.1 The infinite binary tree

We will denote the *infinite binary tree* by T. The vertex set of T is all finite words in the alphabet $\{0, 1\}$, and two words have an edge between them if and only if deleting the rightmost letter of one of them yields the other:



This will in fact be a rooted tree, with the root at the empty sequence, so that any automorphism of T must fix the empty sequence.

Here are some exercises about $\mathrm{Aut}(T)$, the group of automorphisms of T. In this handout, exercises are marked with either * or ** based on difficulty. Most are taken from exercises or statements made in the referenced books.

Exercise 1. Show that the group $\mathrm{Aut}(T)$ is uncountable and has a subgroup isomorphic to $\mathrm{Aut}(T) \times \mathrm{Aut}(T)$.*

Exercise 2. Impose a topology on $\mathrm{Aut}(T)$ to make it into a topological group homeomorphic to the Cantor set.**

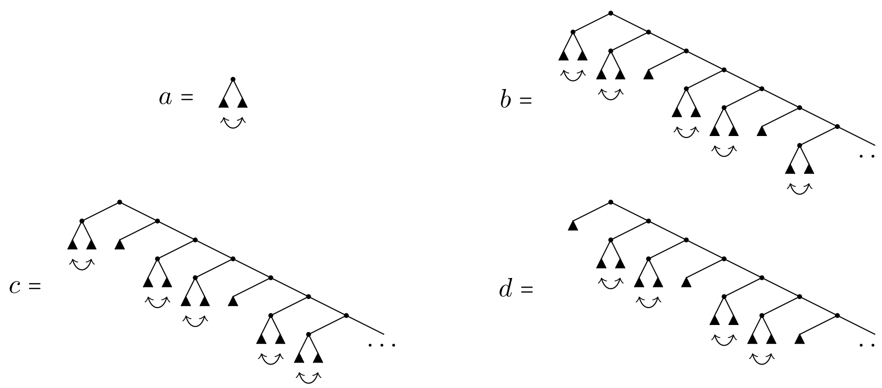
Exercise 3. Find automorphisms of T of infinite order (in fact, there are non-Abelian free subgroups of $\mathrm{Aut}(T)$).**

1.2 The generators

We will now define the *Grigorchuk group* Γ as a subgroup of $\mathrm{Aut}(T)$ generated by four automorphisms a, b, c, and d of T. First, if $x \in \{0,1\}$ let $\overline{x}$ denote the opposite symbol (replacing 0 with 1 and vice versa). Describing the automorphism a is easy:

$$a(x_1 x_2 \cdots x_n) = \overline{x}_1 x_2 \cdots x_n$$

for any $x_1, \dots, x_n \in \{0,1\}$. The other two are not as simple. Let's see a picture that should make the definitions clear:



(1)

The filled triangles represent sub-binary trees whose internal structures are unchanged by the automorphism. Where in the picture two triangles are drawn being swapped, you should imagine them "sliding" across the page onto each other's spots, rather than being reflected onto each other.

The picture should make it obvious that all four generators of Γ have order two, that is, $a^2 = b^2 = c^2 = d^2 = 1$ is the identity automorphism of T. We also see that

$$bc = cb = d, \quad bd = db = c, \quad \text{and} \quad cd = dc = b. \tag{2}$$

Thus any $g \in \Gamma$ can be expressed as a product

$$a^{\varepsilon_1} u_1 a u_2 \cdots a u_n a^{\varepsilon_2}, \tag{3}$$

where $\varepsilon_1, \varepsilon_2 \in \{0,1\}$ and $u_1, \dots, u_n \in \{b, c, d\}$. However, such an expression isn't necessarily unique; you can check that $dadad = ada$. (If you like, this means that Γ is a proper quotient of the free product $\mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.)

We are going to use (1) to intuitively justify many of the following statements. However, we can also give recursive definitions for b, c, and d:

$$\begin{aligned}
b(0x_2 \cdots x_n) &= 0\overline{x}_2 \cdots x_n, \quad & b(1x_2 \cdots x_n) &= 1c(x_2 \cdots x_n), \\
c(0x_2 \cdots x_n) &= 0\overline{x}_2 \cdots x_n, \quad & c(1x_2 \cdots x_n) &= 1d(x_2 \cdots x_n), \\
d(0x_2 \cdots x_n) &= 0x_2 \cdots x_n, \quad & d(1x_2 \cdots x_n) &= 1b(x_2 \cdots x_n).
\end{aligned}$$

Exercise 4. Confirm that the recursive definitions of b, c, and d indeed give well-defined automorphisms of T which agree with (1).*

Exercise 5. Show that the subgroups $\langle a, d\rangle$, $\langle a, c\rangle$, and $\langle a, b\rangle$ of Γ are dihedral of order 8, 16, and 32, respectively.**

2 The general Burnside problem

In 1902, Burnside asked the following question, which later came to be known as the *general Burnside problem*:

Question. If G is a finitely generated group, all of whose elements have finite order, is G necessarily finite?

Although the answer is "yes" given some additional assumptions, the answer is "no" in general and it turns out that the group Γ provides a counterexample. (The Grigorchuk group was not the first such group discovered; Golod and Shafarevich provided an example in 1964.) By definition, Γ is finitely generated, so let's start by showing that it is infinite.

2.1 Γ is infinite

Theorem 6. *The group Γ is infinite.*

Proof. Let Γ_1 denote the subgroup of Γ which satisfies $g(x) = x$ for all $g \in \Gamma_1$ and $x \in \{0, 1\}$. That is, Γ_1 are the elements of Γ which fix both the first and second rows of T (i.e., they fix the sequences 0 and 1). It is easy to see that a word in $\{a, b, c, d\}$ represents an element of Γ_1 if and only if it has an even number of occurrences of a, and so Γ_1 is generated by the elements b, c, d, aba, aca, and ada by (3).

Now define a homomorphism $\varphi_1 : \Gamma_1 \to \Gamma$ by

$$\begin{aligned} \varphi_1(b) &= c, & \varphi_1(c) &= d, & \varphi_1(d) &= b \\ \varphi_1(aba) &= a, & \varphi_1(aca) &= a, & \varphi_1(ada) &= 1. \end{aligned} \tag{4}$$

This map is defined by restricting each element of Γ_1 to the branch of T starting at the sequence 1, and then applying the automorphism of this branch to the whole tree (check this with (1)!). This description makes it intuitively obvious that φ_1 is a homomorphism, and since the image of φ_1 contains $\{a, b, c, d\}$, this map is surjective. But Γ_1 is a proper subgroup of Γ, so Γ is infinite. □

2.2 Γ is a 2-group

It remains to show that every element of Γ has finite order. In fact, a stronger statement is true: Γ is a 2-*group*, meaning that the order of each element is a power of 2. This is the main result of the talk.

Theorem 7. *For any $g \in \Gamma$ there exists $n \in \mathbb{N}$ such that $g^{2^n} = 1$.*

Proof. For each $g \in \Gamma$ we define its *length* $\ell(g)$ to be the length of shortest word in the generating set $\{a, b, c, d\}$ which is equal to g. We are going to induct on the length of g; recall that we know the claim is true if $\ell(g) \leqslant 1$. So suppose we are given $g \in \Gamma$ with $\ell := \ell(g) \geqslant 2$, and use (3) to write $g = a^{\varepsilon_1} u_1 a u_2 \cdots a u_n a^{\varepsilon_2}$ for some $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$ and $u_1, \ldots, u_n \in \{b, c, d\}$. Let us also suppose that this is a shortest such expression.

Suppose g has odd length. Then it must be the case that either $\varepsilon_1 = \varepsilon_2 = 0$ or $\varepsilon_1 = \varepsilon_2 = 1$. In the latter case, g is conjugate by a to an element of Γ of shorter length. In the former case, (2) tell us that g is again conjugate, by either u_1 or u_n, to an element of shorter length. Either way, since conjugation preserves order, the inductive hypothesis applies and proves the claim for g.

Now suppose ℓ is even. By using (3) again and conjugating if necessary, we can assume that g has the form

$$g = a u_1 a u_2 \cdots a u_n,$$

where $u_1, \ldots, u_n \in \{b, c, d\}$ and $n = \ell/2$.

Assume first ℓ is a multiple of 4. Then n is even, so we know that $g \in \Gamma_1$, as defined in the proof of Theorem 6. In this case, it is easy to see that the order of g is the least common multiple of $\varphi_1(g)$ and $\varphi_0(g)$, where $\varphi_0 \colon \Gamma_1 \to \Gamma$ is defined analogously to φ_1 except we look at the automorphism on the branch of T starting at the sequence 0. Now by (4), $\varphi_1(g)$ must have length less than ℓ; it is not hard to produce the definition for φ_0 analogous to (4) to show that the same holds for $\varphi_0(g)$. Thus the inductive hypothesis tells us that the order of g is a power of 2.

Finally, for the case where ℓ is even but n is not, see Exercise 8.

Exercise 8. Finish the final case of Theorem 7 in the following way: First, $g^2 \in \Gamma_1$. Now $\varphi_0(g^2)$ and $\varphi_1(g^2)$ have length at most ℓ. If our expression for g contains d, then in fact both will have length at most $\ell - 1$. If the expression of g has c but not d, then both $\varphi_0(g^2)$ and $\varphi_1(g^2)$ have expressions of length at most ℓ containing d, so now look at $\varphi_0(\varphi_0(g^2)^2)$, $\varphi_0(\varphi_1(g^2)^2)$, $\varphi_1(\varphi_0(g^2)^2)$, and $\varphi_1(\varphi_1(g^2)^2)$. The last case is similar—or, invoke Exercise 5.* □

Exercise 9. Pick up the author's slack and make the proofs above formal and explicit.*

2.3 Some consequences and related facts

Thus Γ indeed solves the general Burnside problem. This has some fun consequences. Most familiar examples of finitely generated groups are *linear groups*, groups which are isomorphic to a group of matrices. For example, any finite group is linear, and countable free groups are linear. In general, finitely generated nonlinear groups tend to have exotic properties.

However, one of the "additional assumptions" under which the Burnside's question has a positive answer is if G is a subgroup of $\mathrm{GL}(n, F)$ for some field F and $n \in \mathbb{N}$, as shown by Schur in 1911 if F has characteristic zero, and otherwise by Kaplansky in 1972. So, we get the following as a corollary to Theorems 6 and 7 and the result of Kaplansky:

Corollary 10. *For any field F and $n \in \mathbb{N}$, if $\varphi\colon \Gamma \to \mathrm{GL}(n, F)$ is a homomorphism, then φ has finite image. In particular, Γ is not a linear group.*

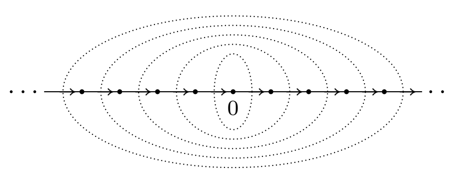
Another variant of Burnside's problem asks if G is guaranteed to be finite if there exists $n \in \mathbb{N}$ such that $g^n = 1$ for all $g \in G$. Although if n is small the answer is "yes" (try $n = 2$), it is unknown for even $n = 5$ and we know that for large enough n the answer is "no". Unfortunately, Γ does not provide any answers to this question, since for all $n \in \mathbb{N}$ there exists $g \in \Gamma$ satisfying $g^{2^n} \neq 1$. However, Γ has a different and still very interesting property: *any finite 2-group is isomorphic to a subgroup of* Γ.

Exercise 11. Try defining new groups similarly to how we defined Γ. What interesting properties does your group have? How about groups defined using the infinite n-ary tree, for $n \geqslant 3$?**

3 Γ as a group of intermediate growth

In this section we define the concept of the growth rate of a group, the fundamental notion in geometric group theory, and briefly describe its relation to the Grigorchuk group. The main claim of this section will not be proven, since the proof would take too long, and the reader is instead referred to the references where far more in-depth expositions can be found.

Suppose G is a group with finite generating set $X \subseteq G$. The *(closed) ball of radius n* of G is the set $B_{G,X}(n)$ of all elements of G which can be expressed as a product of at most n elements of X and X^{-1} (the inverses of elements of X). For example, $B_{G,X}(1) = X \cup X^{-1} \cup \{1\}$. Then the *growth function* of G with respect to the generating set X is the function $\beta_{G,X}\colon \mathbb{N} \to \mathbb{N}$ defined by $\beta_{G,X}(n) := |B_{G,X}(n)|$. For example, it is clear that the growth function of $\mathbb{Z}$ with respect to the generating set $\{1\}$ is given by $\beta_{\mathbb{Z},\{1\}}(n) = 2n + 1$:



Here, balls of successively larger radii are represented by the dotted ellipses, the smallest having radius zero.

It is easy to find examples of growth functions which are polynomials of any integer degree and which are exponential. Additionally, every growth function of an infinite group must be monotonically increasing and cannot grow faster than exponentially.

Exercise 12. Prove the claims made in the previous paragraph.*

However, the growth function is dependent on the choice of generating set. You may wish to check that, for example, $\beta_{\mathbb{Z},\{2,3\}}(n) = 6n + 5$. Even though a group can have multiple growth functions, they cannot be "too" different. In particular, every group falls into one of the following *growth types*:

- ▷ A group G is of *polynomial growth* if every growth function for G is asymptotically polynomial (in other words, can be bounded above and below by two polynomials).
- ▷ A group G is of *exponential growth* if every growth function for G is asymptotically exponential.
- ▷ A group G is of *intermediate growth* if every growth function for G grows faster than any polynomial but slower than any exponential function.

It is easy to find groups of polynomial growth of order k for every $k \in \mathbb{N}$ (take $\mathbb{Z}^n$), and every non-Abelian free group of finite rank is of exponential growth. In 1968, Milnor asked the natural question of whether intermediate groups exist at all. Grigorchuk, in 1984, showed that his group Γ indeed is of intermediate growth. In fact, it has been shown by Bartholdi, improving Grigorchuk's original bounds, that every growth function for Γ grows like e^{n^α} for some α satisfying, approximately, $0.5157 \leqslant \alpha \leqslant 0.7674$. Grigorchuk went further, constructing an uncountably infinite family of groups indexed by certain infinite $\{0,1\}$-sequences, all of which are of intermediate growth.

References

[1] R. Grigorchuk and I. Pak. "Groups of Intermediate Growth: an Introduction for Beginners". In: *arXiv Mathematics e-prints* (2006). eprint: `math/0607384`.

[2] Rostislav Grigorchuk. "Degrees of Growth of Finitely Generated Groups, and the Theory of Invariant Means". In: *Mathematics of the USSR-Izvestiya* 25 (1984), pp. 259–300.

[3] Pierre de la Harpe. *Topics in Geometric Group Theory*. University of Chicago Press, 2000.

[4] Clara Löh. *Geometric Group Theory. An Introduction*. Springer, 2017.