MASTER'S DEGREE THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

Title: The Grigorchuk group and groups of intermediate growth

Author: Aitor Pérez Pérez

Advisor: José Burillo Puig

Department: Departament de Matemàtica Aplicada IV

Academic year: 2014-2015

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Abstract

In this work we make an introduction of growth in groups, giving the definition, some properties and examples. We present the Grigorchuk group $\mathbb{G}$ as a subgroup of automorphisms of the infinite binary tree, and prove that it has intermediate growth, becoming a counterexample both for Milnor's conjecture [8] and for the Burnside problem on periodic groups. Finally, we propose some generalizations to this group and analyze their similarities and differences with the group $\mathbb{G}$ itself, exploring the order of some elements and making some conjectures about their growth.

Mathematical Subject Classification: 20F65, 20F50, 20F69, 20E08.

Keywords: groups of intermediate growth, Grigorchuk group, automorphisms of the infinite binary tree.

Contents

Introduction

Growth in groups has been a studied topic since the 1960s, motivated by the fact that the volume growth of the universal covering of a Riemannian manifold is equal to the growth of its fundamental group. This was presented by Milnor [8], who also stated that soluble groups had either polynomial or exponential growth.

Since at that time no groups of intermediate growth were known, this fact motivated Milnor to state the conjecture that not only soluble groups had polynomial or exponential growth but all groups. This conjecture remained open some years, until 1980, year in which R. I. Grigorchuk [3] found a group of intermediate growth, not polynomial nor exponential. This group was an adequately chosen subgroup of the group of automorphisms of the infinite binary tree, with several good properties which allowed to prove both the superpolynomial and the subexponential growth. Moreover, Grigorchuk also contributed to the Burnside problem, since the same group served as a counterexample. The Burnside problem stated the question of whether every periodic group must be finite. A periodic group is a group in which every element has finite order. Indeed, every element of the Grigorchuk group has finite order (it is a 2-group), but it is not difficult to see that it is infinite.

In parallel, Gromov [4] arrived to a characterization of groups of polynomial growth as the virtually nilpotent groups. A group is virtually nilpotent if it contains a nilpotent subgroup of finite index, and a group is nilpotent if it has a finite lower central series $G = G_1 \rhd \cdots \rhd G_n = 1$, where $G_i = [G_{i-1}, G]$.

This classification and Grigorchuk's work already unveiled a lot about

growth in groups. From this point, several authors have studied this topic and have made important contributions: P. de la Harpe [1], R. I. Grigorchuk and I. Pak [2], A. Mann [7] or Lysenok [6]. Gupta and Sidki [5] proposed some generalizations of the Grigorchuk group as other counterexamples for the Burnside problem on periodic groups, which also served as candidates for other groups of intermediate growth. However, this still remains as an open problem.

This document is structured in the following way: In the first chapter, we aim to give an introduction about growth in order to make this work as self-contained as possible. The second chapter presents the Grigorchuk group, starting with the automorphisms of the infinite binary tree in search of its generators. The proof of its intermediate growth is detailed in the third chapter, separating the superpolynomial and the subexponential growth, which is more involved and needs the definition of the rewriting rules. Finally, in the fourth chapter we try to generalize the construction of the Grigorchuk group as a family of groups by considering other sets as generators, indexing them by a natural number $n \geq 2$, which yield some surprising facts and allow some conjectures, as for instance that such groups have intermediate growth for odd n and that they have an element of infinite order if n is even, which could imply their exponential growth.

1 Growth

1.1 Basic definitions

Definition 1.1. Let G be a finitely generated group, and let $S = \{x_1, \ldots, x_d\}$ be a set of generators. Let $x \in G$. The *length* of x with respect to this set of generators, denoted $\ell_S(x)$ or simply $\ell(x)$, is the minimum length of words in $x_1, \ldots, x_d, x_1^{-1}, \ldots, x_d^{-1}$ representing the element x. Since the length of the empty word is zero, so is $\ell(1)$, the length of the trivial element.

Definition 1.2. For $n \geq 0$, we denote $\gamma(n) = |\{x \in G \mid \ell(x) \leq n\}|$ the number of elements of length at most n. As a function of n, $\gamma_{G,S}(n)$, or simply $\gamma(n)$, is the *growth function* of G with respect to the generating set S.

Remark 1.3. This function can be regarded as the cardinality of balls centered in the trivial element and with radius n. Note that the definition of the growth function strongly depends on the generating set used to define the length. The only fact we assume is that no one of the generators equals another one or the inverse of another one, but we are not assuming, for example, that the set of generators does not contain a proper subset which also generates the same group.

Remark 1.4. G is finite if and only if $\gamma(n)$ is eventually constant.

Proposition 1.5. *Growth functions are* subadditive*:*

$$\gamma(n+m) \leq \gamma(n)\gamma(m)$$

Proof. We can split words of length up to $n+m$ into a word of length up to n concatenated with a word of length up to m. There are $\gamma(n)\gamma(m)$ possibilities for this decomposition, but not all of them will represent different elements. Hence, $\gamma(n+m) \leq \gamma(n)\gamma(m)$. □

Example 1.6. The growth function of $G = \mathbb{Z}$ with respect to the generating set $S = \{1\}$ is $\gamma(n) = 1 + 2n$, for $n \geq 0$.

Proposition 1.7. *The growth function of $G = F_d = \langle x_1, \ldots, x_d \rangle$, the free group on d generators, with respect to the generating set $\{x_1, \ldots, x_d\}$ is*

$$\gamma(n) = \frac{d(2d-1)^n - 1}{d-1}.$$

Proof. In $F_d = \langle x_1, \ldots, x_d \rangle$, each reduced word of length n is obtained by multiplying a reduced word of length $n-1$, for instance $y_1 y_2 \ldots y_{n-1}$, with $y_i = x_{j_i}^{\pm 1}$, by a generator different from y_{n-1}^{-1}. Then, we have the recurrence $\gamma(n) - \gamma(n-1) = (\gamma(n-1) - \gamma(n-2)) \cdot (2d-1)$, since for the last generator we have only $2d-1$ possibilities. This holds for $n \geq 2$, because for $n = 1$ we can choose any of the $2d$ generators and inverses, so $\gamma(1) = 1 + 2d$, which agrees with the expression. All together, we have that

$$\gamma(n) = 2d\gamma(n-1) - (2d-1)\gamma(n-2).$$

Substituting in this equation the expression for γ we stated, for $n-1$ and $n-2$, as an inductive hypothesis, we get to the same expression. □

Corollary 1.8. *If G is not free, then some words are identified and lower the number of elements for some length. Hence, for every finitely generated group G on d generators, $\gamma(n) \leq \frac{d(2d-1)^n - 1}{d-1}$.*

1.2 Equivalence of growth functions

Recall that the definition of length and growth function as we stated it strongly depended on a generating set. Since groups may have several generating sets, one might want to compare two growth functions for the same group using different generating sets. Something we may want to expect is that such functions are equal, but as we will see, they are not. However, we can define an equivalence relation for functions in a way that two different growth functions of the same group belong to the same class.

Definition 1.9. Let $f, g : \mathbb{R} \longrightarrow \mathbb{R}$. We say that $f \preccurlyeq g$ if there exists a real number $A \geq 1$ such that $f(x) \leq Ag(Ax)$, for every x. We call f and g *equivalent* if $f \preccurlyeq g$ and $g \preccurlyeq f$, and we denote it $f \sim g$. One can easily check that this is an equivalence relation.

Proposition 1.10. *Let G be a finitely generated group, and let X_1 and X_2 be two sets of generators for G. Let γ_1 and γ_2 be their associated growth functions. Then, γ_1 and γ_2 are equivalent.*

Proof. Express each element of X_1 as a word in the elements of X_2 and viceversa. Take A to be the maximum length of the resulting set of words. For every $x \in G$, it is clear that $\ell_{X_1}(x) \leq A\,\ell_{X_2}(x)$, which implies that $\gamma_2(n) \leq \gamma_1(An)$. By symmetry, we have that $\gamma_1(n) \leq \gamma_2(An)$. □

As we anticipated, this shows that although growth functions might differ in their expression, the growth rate is the same.

Example 1.11. To illustrate this fact, we may consider $\mathbb{Z}^2$ and three sets of generators: the usual one $X = \{(1,0),(0,1)\}$, $Y = \{(1,0),(1,1)\}$ and $Z =$

$\{(1,0),(0,1),(1,1),(1,-1)\}$. The following figure shows, for each generating set, some regions of elements up to a given length.

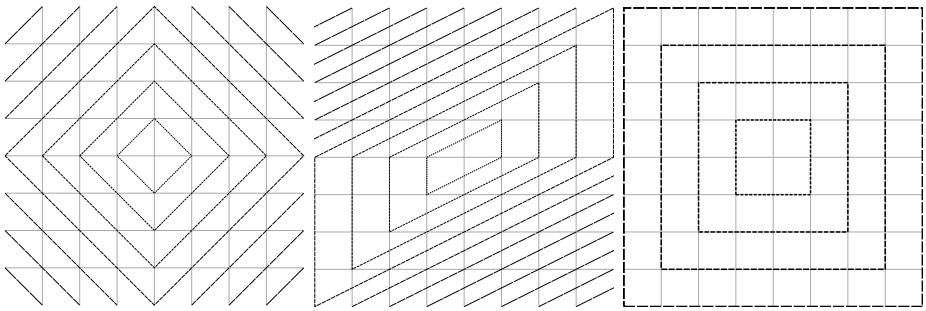

Figure 1: Regions of elements of the same length in $\mathbb{Z}^2$ with respect to generating sets X, Y and Z, respectively.

Notice that the length of an element depends on the generating set. Moreover, it is not difficult to check that the growth functions of $\mathbb{Z}^2$ associated to each generating set are the following:

$$\gamma_X(n) = (n+1)^2 + n^2 \qquad \gamma_Y(n) = (n+1)^2 + n^2 \qquad \gamma_Z(n) = (2n+1)^2.$$

Even though they are different generating sets, X and Y have the same growth function. Nevertheless, the growth function associated to Z is different. Despite this difference, all the polynomials are quadratic, and this is the invariant on which we have to focus, since it is preserved for every generating set of $\mathbb{Z}^2$.

1.3 Finite index subgroups

Before proceeding, we will prove a couple of results regarding finite-index subgroups which will be used later.

Proposition 1.12. *A finite-index subgroup of a finitely generated group is finitely generated.*

Proof. Let $G = \langle x_1, \ldots, x_d \rangle$, and H a subgroup with index s. Let $\{1 = a_1, \ldots, a_s\}$ be a transversal for H in G. For any $x \in G$, we can write it as a product of the generators and their inverses $x = y_1 \ldots y_n$. If we call a_{i_1} the representative of Hy_1, we have $x = (y_1 a_{i_1}^{-1}) a_{i_1} y_2 \ldots y_n$. Again, if a_{i_2} is the representative of $Ha_{i_1}y_2$, then $x = (y_1 a_{i_1}^{-1})(a_{i_1} y_2 a_{i_2}^{-1}) a_{i_2} y_3 \ldots y_n$.

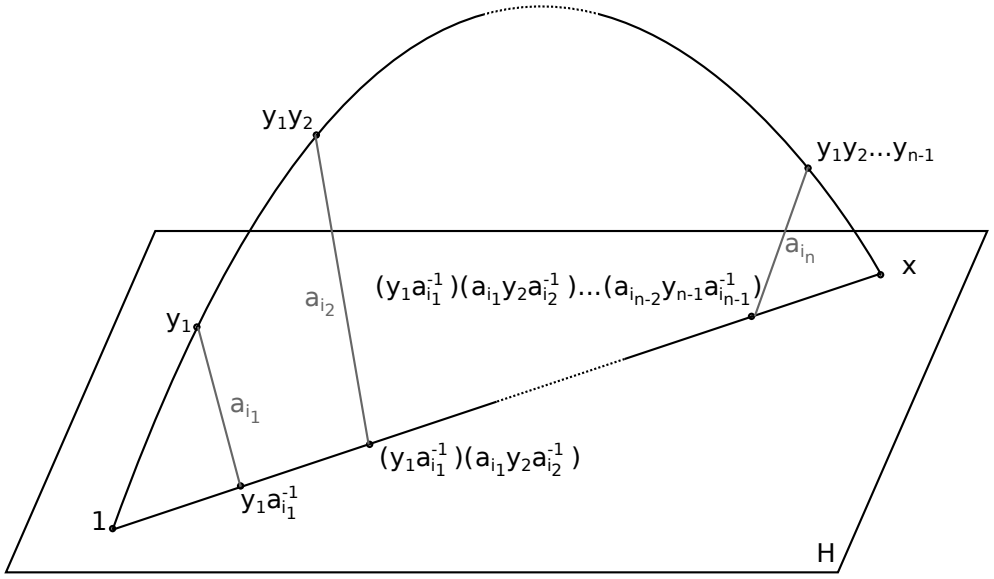

Figure 2: In order to represent an element $x \in H$, we can find generators also in H of the form $a_j y_k a_l^{-1}$.

Repeating and writing $a_{i_0} = a_{i_n} = 1$, we obtain

$$x = (a_{i_0} y_1 a_{i_1}^{-1})(a_{i_1} y_2 a_{i_2}^{-1}) \dots (a_{i_{n-1}} y_n a_{i_n}^{-1}) a_{i_n}.$$

By construction, each of the factors belongs to H, and, if $x \in H$, then a_{i_n} has to be 1, and x is a product of elements of H of the form $a_j y_k a_l^{-1}$, as in 1.3, which are finitely many. □

Proposition 1.13. *Let G be a finitely generated group and $s \in \mathbb{N}$. Then, G contains a finite number of subgroups of index s.*

Proof. Let G be generated by $x_1, \dots, x_d$, and let H be a subgroup of index s. Consider r cosets ($r < s$) $Ha_1, \dots, Ha_r$ and call their union K, which is not all of G, so K cannot be closed under multiplication on the right by the generators and their inverses. This means that there exists some i and some generator x_j for which either $Ha_i x_j$ or $Ha_i x_j^{-1}$ is a coset not in K. Inductively, it follows that every coset has a representative of length at most $s-1$, and then the products $a_i x_j a_k^{-1}$, which generate H, have length at most $2s-1$. Since there is a finite amount of such elements, there are only a finite number of ways of choosing the generators for H. □

1.4 Growth rates

Now we would like to classify groups according to their growth. For this purpose, we will define the following invariants:

Definition 1.14. Let G be a finitely generated group. Then, we define

$$\omega(G) = \lim_{n \longrightarrow \infty} \gamma(n)^{1/n}.$$

Lemma 1.15 (Fekete's lemma)**.** *Let $\{a_n\}_n$ be a sequence such that $a_{n+m} \leq a_n + a_m$ for every n, m. Then,*

$$\lim_{n\to\infty} \frac{a_n}{n} = \inf_n \frac{a_n}{n}.$$

In particular, the limit exists.

Proof. On one hand, it is obvious that $\lim_{n\to\infty} \inf_n \frac{a_n}{n} \geq \inf_n \frac{a_n}{n}$. To see the other inequality, let us write $n = km + r$, as in the euclidean division, where $n, k, m, r \in \mathbb{N}$. Now we have

$$\frac{a_n}{n} = \frac{a_{km+r}}{km+r} \leq \frac{ka_m + a_r}{km+r} = \frac{a_m + a_r/k}{m + r/k}.$$

If we fix m but consider the limit when $k \to \infty$ (and so $n \to \infty$), r remains bounded and we have

$$\lim_{n\to\infty} \frac{a_n}{n} \leq \frac{a_m}{m}.$$

Finally, we can choose an m minimizing $\frac{a_m}{m}$ to see the result. □

Remark 1.16. Since $\gamma(n+m) \leq \gamma(n)\gamma(m)$, Fekete's Lemma can be applied to the sequence defined by $a_n = \log \gamma(n)$, which satisfies $\log \gamma(n+m) \leq$

$\log(\gamma(n)\gamma(m)) = \log\gamma(n) + \log\gamma(m)$, to show that the limit $\lim_{n\to\infty} \frac{\log\gamma(n)}{n} = \lim_{n\to\infty} \log\gamma(n)^{1/n}$ exists, and hence also $\omega(G)$. Besides, $\omega(G) \geq 1$, and, since the free group serves as an upper bound, $\omega(G) \leq 2d-1$, if G has d generators.

Remark 1.17. While the exact value for $\omega(G)$ depends on the chosen set of generators X, because $\gamma(n)$ may be different, the fact that $\omega(G) = 1$ or not does not. This can be seen taking two generating sets and their growth functions and using the equivalence conditions on the limits for $\omega(G)$.

There are groups satisfying $\omega(G) > 1$ for every generating set but for which there exist a sequence of generating sets $\{X_n\}_n$ such that $\omega_{X_1}(G) > \cdots > \omega_{X_n}(G) > \cdots$, in a way that $\sup_i \omega_{X_i}(G) = 1$. However, this supreme is never attained, so it does not contradict what we stated before.

Definition 1.18. Let G be a finitely generated group, and let $\gamma(n)$ be a growth function.

- G has *exponential growth* if $\omega(G) > 1$, and has *subexponential growth* if $\omega(G) = 1$. The number $\omega(G)$ is called the *exponential growth rate* of G (or of (G, X), when the set of generators is not clear from the context).

- G has *polynomial growth* if there exist c, t such that $\gamma(n) \leq cn^t$ for every n. Depending on the value of t, we say that G has *linear growth* ($t = 1$), *quadratic growth* ($t = 2$), etc. Obviously, groups with polynomial growth have subexponential growth. If G has polynomial growth, we define its *degree* in a natural way as $\deg(G) = \inf\{t \mid \exists c \quad s(G) \leq cn^t\}$.

- G has *intermediate growth* if it has neither exponential nor polynomial growth.

Proposition 1.19. *Let G be a group, $H \leq G$ and $N \triangleleft G$, all of them finitely generated.*

(a) The type of growth of G does not depend on the chosen set of generators X.

(b) If G has subexponential growth, so have H and G/N. If G has polynomial growth, $\deg(H), \deg(G/N) \leq \deg(G)$.

(c) If the index of H is finite, then G and H have equivalent growth functions. In particular, they have the same type of growth. If it is polynomial, they have the same degree.

(d) If N is finite, then G and G/N have equivalent growth functions. In particular, they have the same type of growth. If it is polynomial, they have the same degree.

(e) If G has polynomial growth and H has infinite index, then $\deg(H) \leq \deg(G) - 1$.

(f) If G has polynomial growth and N is infinite, then $\deg(G/N) \leq \deg(G) - 1$.

Proof. Let $G = \langle x_1, \ldots, x_d \rangle$ and $H = \langle y_1, \ldots, y_e \rangle$. If we put $k = \max \ell(y_i)$, then $\gamma_H(n) \leq \gamma_G(kn)$. Let $G/N = \langle Nx_1, \ldots Nx_d \rangle$, so $\gamma_H(n) \leq \gamma_G(n)$ trivially. This shows (b), and (a) is a particular case when $G = H$.

If H has finite index t, take a transversal of H $\{1 = a_1, \ldots, a_t\}$, and consider $r = \max \ell(a_i)$. Now let $g \in G$ be an element of length at most n. We write $g = ha$, with $h \in H$ and a in the transversal. In particular, write

$h = y_1 \dots y_l$, relabeling the y_i or maybe taking their inverses. Since $h = ga^{-1}$, $l = \ell_H(h) \leq n + r$. We can write $g = (y_1 a_{i_1}^{-1})(a_{i_1} y_2 a_{i_2}^{-1}) \dots (a_{i_{l-1}} y_l a_{i_l}^{-1})$, and then, if we consider the generators $a_i y_j a_m^{-1}$, $\ell(g) \leq l$. Hence, $\gamma_G(n) \leq r\gamma_H(l) \leq r\gamma_H(n + r) \leq r\gamma_H((r + 1)n)$. In particular, if the growth rate is polynomial, they have the same degree. This shows (c).

For (d), consider again the generators $Nx_1, \dots Nx_d$ of N. Every element $g \in G$ of length at most n maps to one of length at most n in the quotient G/N. Since exactly $|N|$ elements of G map in each element of G/N, we have $\gamma_{G/N}(n) \leq \gamma_G(n) \leq |N|\gamma_{G/N}(n)$. This implies that, if the growth is polynomial, the degree is the same.

If H has infinite degree, let $Ha_1, \dots, Ha_n$ be n different cosets of H. We can assume that $\ell(a_i) \leq i$, using the same construction as in Proposition 1.13. Now take $h_1, \dots, h_k \in H$ of length at most n. All elements $h_i a_j$ are different, otherwise the two a's would be in the same coset, so $ns_H(n) \leq s_G(2n)$. If the growth is polynomial, we have $\deg(H) \leq \deg(G) - 1$, which proves (e).

Finally, if N is infinite, we choose a set of generators for G containing a subset of generators of N. Then, there are more elements in G of length $2n$ than those of the form xa, with $x \in N$ and a a representative of any n cosets. This means that $\gamma_G(2n) \geq n\gamma_{G/N}(n)$, and so if the growth is polynomial, $\deg(G/H) \leq \deg(G) - 1$. □

2 Grigorchuk's first group: $\mathbb{G}$

2.1 Automorphisms of the tree

Definition 2.1. Let T be an infinite rooted binary tree. Given a node $v \in T$, we will denote its left and right children as v_0 and v_1, respectively.

In general, we can define recursively the n-children of v to be the $(n-1)$-children of v_0 and v_1, being v_0 and v_1 its 1-children.

The level of v is the distance of v to the root.

Notice that, since T is infinite, if we denote as T_v the subtree rooted at v, T is isomorphic to T_v.

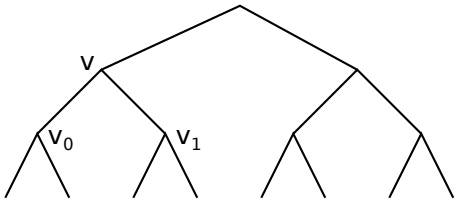

Figure 3: Rooted infinite binary tree T.

Definition 2.2. $\mathrm{Aut}(T)$ is the group of automorphisms of T. Precisely,

$$\mathrm{Aut}(T) = \{\tau : T \longrightarrow T \mid \{\tau(v_0), \tau(v_1)\} = \{\tau(v)_0, \tau(v)_1\}, \quad \forall v \in T\}.$$

This condition means that an automorphism of T maps edges to edges. This implies, for instance, that the root is always mapped to itself and more generally that each vertex is mapped to a vertex in the same level.

Now we are interested in defining some particular elements of $\mathrm{Aut}(T)$, which will be used later as generators of the Grigorchuk's group.

Definition 2.3. Let $a \in \mathrm{Aut}(G)$ be the automorphism of T that exchanges the two subtrees $T_0 = T_{r_0}$ and $T_1 = T_{r_1}$ rooted at the two children of the root vertex. Formally, if r is the root of T, a maps r to itself, r_0 to r_1, r_1 to r_0, and the subtrees below r_0 and r_1 are exchanged. More generally, a maps a vertex $r_{0\varepsilon_1 \ldots \varepsilon_n}$ to $r_{1\varepsilon_1 \ldots \varepsilon_n}$ and viceversa.

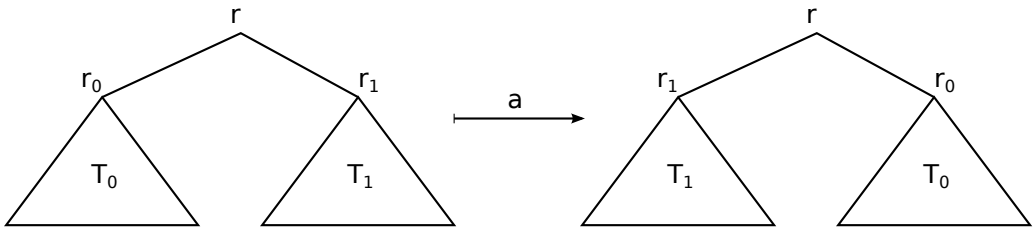

Figure 4: $a \in \mathrm{Aut}(T)$ exchanges the subtrees T_0 and T_1.

Notice that a is an involution: $a^2 = id$.

Moreover, we can extend this definition to the rest of vertices. For any vertex v, a_v is the automorphism fixing every $v' \notin T_v$ and defined as a in T_v via the isomorphism $T \cong T_v$. In this setting, $a = a_r$.

To define the rest of generators, let us introduce the following map, which will help to better understand the structure of $\mathrm{Aut}(T)$.

Let $i_0 : T \longrightarrow T_0$ and $i_1 : T \longrightarrow T_1$ be the isomorphisms between T_0, T_1 and T. Now we define the map φ as follows:

$$\begin{array}{rccc} \varphi: & \mathrm{Aut}(T) \times \mathrm{Aut}(T) & \longrightarrow & \mathrm{Aut}(T) \\ & (\tau_0, \tau_1) & \longmapsto & i_0(\tau_0) \cdot i_1(\tau_1) \end{array}$$

If we define $\mathrm{Aut}(T_\varepsilon)$ to be the subgroup of $\mathrm{Aut}(T)$ fixing every vertex outside T_ε, then $i_\varepsilon(\tau_\varepsilon) \in Aut(T_\varepsilon)$, so the order of the factors in this definition is irrelevant, because they commute.

Nevertheless, this map φ is not surjective. For instance, a is not in the image. Indeed, automorphisms mapping r_0 to r_1 and viceversa do not belong to $\operatorname{Im}\varphi$. In order to extend this map to an isomorphism, we have to consider the following definition.

Definition 2.4. The *wreath product* of a group G with $\mathbb{Z}_2$ is $G \wr \mathbb{Z}_2 = G \times G \rtimes \mathbb{Z}_2$, where the semidirect product exchanges the order of both copies of G. In particular, if $g_1, g_2 \in G$, and $\mathbb{Z}_2 = \{1, t\}$,

$$t(g_1, g_2)t = (g_2, g_1).$$

We will use this definition with the group $\operatorname{Aut}(T)$. If we consider $\mathbb{Z}_2 = \{1, t\}$ in the wreath product, we can define the following extension for φ:

$$\begin{array}{rccc} \varphi: & \operatorname{Aut}(T) \times \operatorname{Aut}(T) \rtimes \mathbb{Z}_2 & \longrightarrow & \operatorname{Aut}(T) \\ & (\tau_0, \tau_1) & \longmapsto & i_0(\tau_0) \cdot i_1(\tau_1) \\ & t & \longmapsto & a \end{array}$$

For $1 \in \mathbb{Z}_2$, φ is exactly the same map as before. However, for $t \in \mathbb{Z}_2$, we get the automorphism exchanging the two vertices r_0 and r_1, and behaving as τ_1 in T_0 and as τ_0 in T_1.

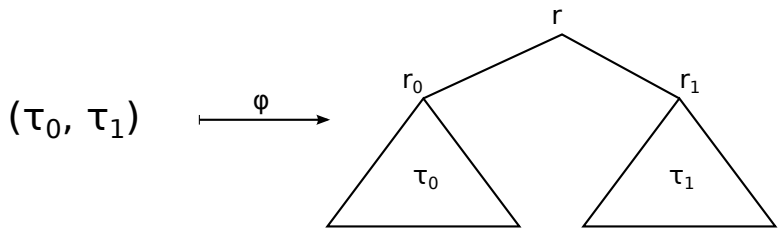

Figure 5: If t is not involved, $\varphi(\tau_0, \tau_1)$ is the automorphism constructed as τ_0 in the first subtree and τ_1 in the second.

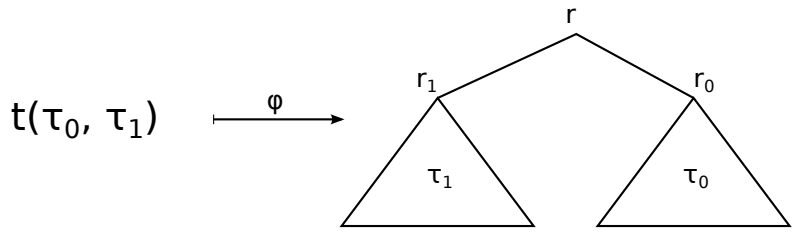

Figure 6: If t is present, we have to apply a after the previous construction and switch the subtrees.

Extending φ to $\mathrm{Aut}(T) \wr \mathbb{Z}_2$ converts it to an isomorphism between $\mathrm{Aut}(T) \wr \mathbb{Z}_2$ and $\mathrm{Aut}(T)$, because every automorphism can be decomposed into how does it map the left subtree, the right subtree and whether it exchanges the two children of the root.

From now on, we will refer to this isomorphism as φ and to its inverse as $\psi : \mathrm{Aut}(T) \longrightarrow \mathrm{Aut}(T) \times \mathrm{Aut}(T) \rtimes \mathbb{Z}_2$, which maps an automorphism to its left and right children, and to 1 or t if it exchanges r_0 and r_1, respectively.

2.2 Generators of $\mathbb{G}$

As we have mentioned, one of the generators of $\mathbb{G}$ is a. Now we are in a good situation to define the remaining generators.

Definition 2.5. Let b, c and d be the elements of $\mathrm{Aut}(T)$ complementarily defined as $b = \varphi(a, c)$, $c = \varphi(a, d)$ and $d = \varphi(id, b)$. Although this definition may not be very intuitive, it uniquely defines these three elements. Pictorially, these elements are the following:

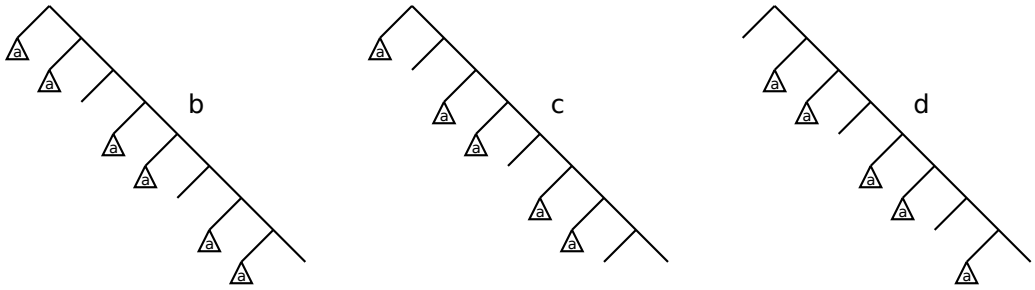

Figure 7: b, c and d are defined applying a to each left child, but skipping one every three.

Definition 2.6. The Grigorchuk group is $\mathbb{G} = \langle a, b, c, d \rangle \subset \mathrm{Aut}(T)$.

2.3 Basic properties of $\mathbb{G}$

With the generators defined, we want to present some of the properties of the group $\mathbb{G}$, as for example the order of some special elements, the definition of one important subgroup and a normal form for elements of $\mathbb{G}$.

Remark 2.7. The first we can notice about the generators of $\mathbb{G}$ is that not only a is an involution, but every one of them is. Hence,

$$a^2 = 1 \qquad b^2 = 1 \qquad c^2 = 1 \qquad d^2 = 1.$$

Another relation we can easily see through the pictures is the following:

$$bcd = 1.$$

This means that we can express any of the generators b, c and d in terms of the other two: $b = dc$, $c = bd$ and $d = cb$. This proves that, actually, we do not need to have the four generators define $\mathbb{G}$, since $\mathbb{G} = \langle a, b, c\rangle = \langle a, b, d\rangle = \langle a, c, d\rangle$. However, in order to keep everything symmetric, we prefer to consider all four of them as a generating set for $\mathbb{G}$.

Finally, other relations one may want to check are that b, c and d commute pairwise:

$$bc = cb \qquad bd = db \qquad cd = dc$$

and that the orders of the elements ab, ac and ad are the following:

$$(ab)^{16} = (ac)^8 = (ad)^4 = 1.$$

They imply that the subgroups $\langle a, b\rangle$, $\langle a, c\rangle$ and $\langle a, d\rangle$ of $\mathbb{G}$ are finite.

Remark 2.8. Every element of $\mathbb{G}$ can be written as a word $w = (a) * a * \cdots * a * (a)$, where $* \in \{b, c, d\}$ and the first and the last a may or may not appear. Since the generators have order 2, their inverses are themselves, and if we consider an arbitrary word in a, b, c, d representing an element, we can collapse any two consonants into the third one. Iterating this process, we eventually modify the word to this form, without altering the element it represents.

Definition 2.9. There is a very important subgroup of $\mathbb{G}$. The *fundamental subgroup of* $\mathbb{G}$, denoted $\mathbb{H}$, is the subgroup of automorphisms leaving fixed the first layer of the tree:

$$\mathbb{H} = \{\tau \in \mathbb{G} \mid \tau(v) = v \quad \forall v \text{ such that } |v| = 1\}.$$

As a first check, we may notice that $a \notin \mathbb{H}$, while $b, c, d \in \mathbb{H}$.

Proposition 2.10.

1. $[\mathbb{G} : \mathbb{H}] = 2$.
2. $\mathbb{H} \lhd \mathbb{G}$.
3. $\mathbb{H} = \langle b, c, d, b^a, c^a, d^a \rangle$.

Proof. Let $g \in \mathbb{G}$ and let $w = (a) * a * \cdots * a * (a)$ be a reduced word representing g. If we focus on the two vertices on the first layer of T, they are fixed by b, c, d but exchanged by a. Hence, $g \in \mathbb{H}$ if and only if w has an even number of occurrences of a ($|w|_a$ even). This shows that $[\mathbb{G} : \mathbb{H}] = 2$, and, since subgroups of index 2 are always normal, we also have the second statement. Finally, since $|w|_a$ is even, we can arrange w either as

$*(a*a)\cdots*(a*a) = **^a\cdots**^a$ or $(a*a)*\ldots(a*a)* = *^a*\cdots*^a*$, so we see that indeed $\mathbb{H}$ is generated by $\{b, c, d\}$ and their conjugates by a. $\square$

Remark 2.11. If we recall the isomorphism we defined for the automorphisms of the tree $\psi : \mathrm{Aut}(T) \longrightarrow \mathrm{Aut}(T) \times \mathrm{Aut}(T) \rtimes \mathbb{Z}_2$, we may want to consider its restriction to $\mathbb{G}$. Since $\psi(a) = t(1,1)$, $\psi(b) = (a, c)$, $\psi(c) = (a, d)$ and $\psi(d) = (1, b)$, we see that $\psi(\mathbb{G}) = \mathbb{G} \times \mathbb{G} \rtimes \mathbb{Z}_2$, so both restrictions of ψ and φ are again inverse isomorphisms. We will denote $\psi(\mathbb{H})$ as $\tilde{\mathbb{H}}$.

Theorem 2.12. $\mathbb{G}$ *is infinite.*

Proof. First notice that $\tilde{\mathbb{H}} = \psi(\mathbb{H}) \subset \mathbb{G} \times \mathbb{G}$. Indeed, we have

$$b \longmapsto (a, c) \qquad c \longmapsto (a, d) \qquad d \longmapsto (1, b)$$

$$b^a \longmapsto (c, a) \qquad c^a \longmapsto (d, a) \qquad d^a \longmapsto (b, 1)$$

Moreover, $\tilde{\mathbb{H}}$ projects surjectively onto each component, since every generator belongs to the image.

If $\mathbb{G}$ was finite, then we would have $|\mathbb{G}| = 2|\mathbb{H}| > |\mathbb{H}| \geq |\mathbb{G}|$, which is a contradiction. $\square$

Remark 2.13. In order to be consistent with the definition of growth, we should point out that $\mathbb{G}$ is finitely generated. This is trivial because of the way we defined it, but let us say some words about the presentation of $\mathbb{G}$.

Aside to the obvious relations, such as $a^2 = b^2 = c^2 = d^2 = bcd = 1$, we can find others as for instance $(ad)^4$, $(ac)^8$ or $(acab)^8$.

The word problem for $\mathbb{G}$ is solvable, and although the proof involves the rewriting rules and the bound on the length that we will explain in the next section, the algorithm, which can be found in [1], can be simplified as

1. If $w \notin \mathbb{H}$, then $w \neq 1$.

2. Else, decompose w as the action on the left and right children. Recurse with both and conclude that $w = 1$ if and only if both children are also 1.

This decomposes the words representing 1 into different subsets K_n in the following way: $w = 1$ belongs to K_n if this algorithm needs to go down not more than n levels to decide that $w = 1$.

Now consider the group $F = \mathbb{Z}_2 * \mathbb{V}$, the free product of (committing an abuse of notation using the same names) $\mathbb{Z}_2 = \{1, a\}$ and $\mathbb{V} = \{1, b, c, d\}$, and the morphism defined by

$$\begin{array}{ccc} F & \longrightarrow & \mathbb{G} \\ a & \longmapsto & a \\ b & \longmapsto & b \\ c & \longmapsto & c \\ d & \longmapsto & d. \end{array}$$

Obviously, this is an epimorphism, and if we consider its kernel, we can transfer the decomposition of the K_n to F, thus stratificating the kernel.

Indeed, one can check that all K_n (now as subgroups of F) are proper subgroups of F, that inclusions are strict, and that all of them are normal, so we have

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_n \lhd \cdots \lhd \bigcup_{n \geq 0} K_n$$

and the union is exactly the kernel of the morphism. A detailed proof can be found in [1].

This fact implies that $\mathbb{G}$ does not admit a finite presentation, because each relation lies in one of these K_n, and if they were finitely many, then the inclusion chain would stabilize, which is in contradiction with the stated above. The problem of finding a finitely presented group of intermediate growth remains still an open problem.

Finally, Lysenok found a presentation for the group $\mathbb{G}$ in [6], with the four generators, the trivial relations and a non-trivial recursive way of defining the rest of relations.

3 Intermediate growth of $\mathbb{G}$

3.1 Technical lemmas

Lemma 3.1 (Lower bound lemma)**.** *Let $f : \mathbb{N} \longrightarrow \mathbb{R}_+$ be a monotone increasing map, such that $\lim_{n\to\infty} f(n) = \infty$ and $f(n) \geq n$ for every $n \in \mathbb{N}$. If $f \succcurlyeq f^m$ for some $m > 1$, then $f \succcurlyeq e^{n^\nu}$, for some $\nu > 0$.*

Proof. We can extend f to $\mathbb{R}_+$ by setting $f(x) = \lfloor x \rfloor$. The map $g(n) = \ln f(n)$ is also monotone increasing and $\lim_{n\to\infty} g(n) = \lim_{n\to\infty} \ln f(n) = \infty$. Since $f \succcurlyeq f^m$, $f(n) \geq K f(\alpha n)^m$ for some $K, \alpha \geq 0$, which means that

$$g(n) = \ln f(n) \geq \ln K f(\alpha n)^m = \ln K + m \ln f(\alpha n) = C + m g(\alpha n).$$

We can check that $0 < \alpha < 1$. Indeed, if $\alpha \geq 1$, then

$$-C \geq m g(\alpha n) - g(n) \geq m g(n) - g(n) = (m-1) g(n) \longrightarrow \infty,$$

which is a contradiction.

Iterating the inequality above, we get

$$g(n) \geq C + m g(\alpha n) \geq C + m(C + m g(\alpha^2 n)) \geq$$

$$\geq \cdots \geq m^k g(\alpha^k n) + C(1 + m + \cdots + m^{k-1}).$$

Now we distinguish two cases depending on the value of C. If $C \geq 0$, then we define $k = \lfloor \frac{\ln n - 1}{\ln 1/\alpha} \rfloor$. In this case, we have $k \leq \frac{\ln n - 1}{\ln 1/\alpha}$ and, since $\alpha < 1$,

$$\alpha^k n \geq \alpha^{\frac{\ln n - 1}{\ln 1/\alpha}} n = (\alpha^{\frac{1}{\ln 1/\alpha}})^{\ln n - 1} n = (\alpha^{\frac{\log_\alpha e}{\log_\alpha 1/\alpha}})^{\ln n - 1} n =$$

$$= (\alpha^{-\log_\alpha e})^{\ln n - 1} n = e^{-\ln n + 1} n = \frac{1}{n} e n = e.$$

Hence, provided that ln and f are monotone increasing and $f(e) \geq e$,

$$g(\alpha^k n) = \ln f(\alpha^k n) \geq \ln f(e) \geq \ln e = 1.$$

Finally, recovering the iterated inequality, for a large enough n we have

$$g(n) \geq m^k g(\alpha^k n) + C(1 + m + \cdots + m^{k-1}) \geq m^k \ln f(\alpha^k n) \geq m^k \geq$$

$$\geq m^{\frac{\ln n - 1}{\ln 1/\alpha} - 1} = m^{\frac{\ln n}{\ln 1/\alpha} - \frac{1}{\ln 1/\alpha} - 1} = m^{-\frac{1}{\ln 1/\alpha} - 1} m^{\frac{\ln n}{\ln 1/\alpha}} = m^{-\frac{1}{\ln 1/\alpha} - 1} n^{\frac{\ln m}{\ln 1/\alpha}} = An^{\nu},$$

for $A, \nu > 0$. Taking exponentials in both sides of the inequality, $f(n) \geq e^{An^{\nu}}$.

On the other hand, if $C = -C' < 0$, then we define $k = \lfloor \frac{\ln n - C' - 1}{\ln 1/\alpha} \rfloor$ and similarly as before we have

$$\alpha^k n \geq \alpha^{\frac{\ln n - C' - 1}{\ln 1/\alpha}} n = (\alpha^{\frac{1}{\ln 1/\alpha}})^{\ln n - C' - 1} n = (\alpha^{\frac{\log_\alpha e}{\log_\alpha 1/\alpha}})^{\ln n - C' - 1} n =$$

$$= e^{-\ln n + C' + 1} n = \frac{1}{n} e^{1 + C'} n = e^{1 + C'}.$$

Using the summation formula $1 + m + \cdots + m^{k-1} = \frac{1 - m^k}{1 - m}$ we get

$$1 + m + \cdots + m^{k-1} \leq m^k \Leftrightarrow \frac{1 - m^k}{1 - m} \leq m^k \Leftrightarrow \frac{1}{m^k} - 1 \leq m - 1$$

which holds for every $m \geq 2$. Therefore,

$$g(n) \geq m^k g(\alpha^k n) - C'(1 + m + \cdots + m^{k-1}) \geq m^k (g(\alpha^k n) - C') =$$

$$= m^k (\ln f(\alpha^k n) - C') \geq m^k (\ln f(e^{1 + C'}) - C') \geq m^k (\ln(e^{1 + C'}) - C') =$$

$$= m^k (1 + C' - C') = m^k \geq m^{\frac{\ln n - C' - 1}{\ln 1/\alpha} - 1} = m^{\frac{-C' - 1}{\ln 1/\alpha} - 1} m^{\frac{\ln n}{\ln 1/\alpha}} =$$

$$= m^{\frac{-C' - 1}{\ln 1/\alpha} - 1} n^{\frac{\ln m}{\ln 1/\alpha}} = An^{\nu},$$

for $A, \nu > 0$. Again taking exponentials, we obtain $f(n) \geq e^{An^{\nu}}$. □

Lemma 3.2 (Upper bound lemma)**.** *Let $f : \mathbb{N} \longrightarrow \mathbb{R}_+$ be a monotone increasing map, such that $\lim_{n\to\infty} f(n) = \infty$. Let $f^{*k}(n) = \sum_{(n_1,\ldots,n_k)} f(n_1)\ldots f(n_k)$, where the summation runs for every $(n_1,\ldots,n_k) \in \mathbb{N}^k$ such that $n_1 + \cdots + n_k \leq n$. If $f(n) \leq Cf^{*k}(\alpha n)$ for some $k > 1$, $C > 0$ and $0 < \alpha < 1$, then $f \preccurlyeq e^{n^\nu}$, for some $\nu < 1$.*

Proof. We proceed by induction on n. By hypothesis we have

$$f(n) \leq Cf^{*k}(\alpha n) = C \sum_{(n_1,\ldots,n_k)} f(n_1)\ldots f(n_k),$$

for $(n_1,\ldots,n_k)$ such that $n_1 + \cdots + n_k \leq \alpha n$. Notice that this summation involves not more than $(\alpha n)^k$ terms. We define $g(n) = \ln f(n)$. Since $\alpha < 1$, we can assume that $f(n_i) \preccurlyeq e^{n_i^\nu}$, or equivalently, that $g(n_i) = \ln f(n_i) \leq An_i^\nu$.

Now we have

$$\ln\left(f(n_1)\ldots f(n_k)\right) = \ln f(n_1) + \cdots + \ln f(n_k) = g(n_1) + \cdots + g(n_k) \leq$$

$$\leq A(n_1^\nu + \cdots + n_k^\nu) \leq Ak\left(\frac{\alpha n}{k}\right)^\nu = An^\nu\left(k\frac{\alpha^\nu}{k^\nu}\right) \leq An^\nu(1-\varepsilon),$$

for $\varepsilon > 0$ and ν as close to 1 as needed, but both depending only on k and α, which are fixed. In addition, we have used that $n_1^\nu + \cdots + n_k^\nu \leq k\left(\frac{\alpha n}{k}\right)^\nu$ (which is a consequence of the function x^ν being concave) and that $k\frac{\alpha^\nu}{k^\nu} < 1$.

Therefore,

$$f(n) \leq C \sum_{(n_1,\ldots,n_k)} f(n_1)\ldots f(n_k) < C \sum_{(n_1,\ldots,n_k)} e^{An^\nu(1-\varepsilon)} = C(\alpha n)^k e^{An^\nu(1-\varepsilon)}.$$

Hence,

$$g(n) = \ln f(n) < \ln C + \ln(\alpha n)^k + An^\nu(1-\varepsilon) =$$

$$= (\ln C + k \ln \alpha + k \ln n) + An^{\nu}(1 - \varepsilon) \leq An^{\nu},$$

for an adequate choice of A, satisfying both this condition and the base of the induction. $\square$

3.2 Superpolynomial growth of $\mathbb{G}$

Definition 3.3. Two groups G_1 and G_2 are *commensurable* ($G_1 \approx G_2$) if they contain isomorphic subgroups of finite index (i.e. $\exists H_1 \subseteq G_1, H_2 \subseteq G_2$ such that $H_1 \cong H_2$ and $[G_1 : H_1], [G_2 : H_2] < \infty$).

Remark 3.4. Recall that finite-index subgroups have the same growth as the group itself. This means that $\gamma_G \sim \gamma_H$. If $G_1 \approx G_2$, then we have that $\gamma_{G_1} \sim \gamma_{H_1} \sim \gamma_{H_2} \sim \gamma_{G_2}$, and so commensurable groups have equivalent growth functions.

To prove the superpolynomial growth of $\mathbb{G}$, we will see that $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$.

Definition 3.5. Let $\mathbb{B}$ be the normal subgroup of $\mathbb{G}$ generated by b:

$$\mathbb{B} = \langle g^{-1}bg \mid g \in \mathbb{G} \rangle$$

Proposition 3.6. $[\mathbb{G} : \mathbb{B}] \leq 8$.

Proof. Notice that $a^2 = d^2 = (ad)^4 = 1$. The first two imply that reduced words in a and d are $(a)dad \dots ad(a)$, and the third implies that since $adad = dada$, in fact there are 8 such words. Indeed, $\langle a, d \rangle \cong D_4$, the dihedral group of 8 elements. But $\mathbb{G} = \langle a, b, d \rangle$, and since $b \in \mathbb{B}$, $\mathbb{G}/\mathbb{B}$ is a quotient of $\langle a, d \rangle$. In particular, $[\mathbb{G} : \mathbb{B}] \leq 8$. □

Proposition 3.7. $\mathbb{B} \times \mathbb{B} \subseteq \tilde{\mathbb{H}} \subseteq \mathbb{G} \times \mathbb{G}$.

Proof. $\tilde{\mathbb{H}} = \psi(\mathbb{H})$, so, since $d, d^a \in \mathbb{H}$, $\langle \psi(d), \psi(d^a) \rangle = \langle (1, b), (b, 1) \rangle \subseteq \tilde{\mathbb{H}}$. Let $h \in \mathbb{H}$ such that $\psi(h) = (h_0, h_1)$.

$$\psi(d^h) = \psi(h^{-1}dh) = \psi(h)^{-1}\psi(d)\psi(h) = (h_0^{-1}, h_1^{-1})(1, b)(h_0, h_1) = (1, b^{h_1}).$$

Now since both projections $pr_1 : \tilde{\mathbb{H}} \longrightarrow \mathbb{G}$ and $pr_2 : \tilde{\mathbb{H}} \longrightarrow \mathbb{G}$ are epimorphisms, we can choose h_1 to be any element of $\mathbb{G}$. This means that $\tilde{\mathbb{H}}$ contains all elements of the form $(1, b^g)$, $\forall g \in \mathbb{G}$, and these elements generate $\langle (1, b^g) \mid g \in \mathbb{G} \rangle = 1 \times \mathbb{B} \subseteq \tilde{\mathbb{H}}$.

Similarly, writing d^a instead of d we get $\mathbb{B} \times 1 \subseteq \tilde{\mathbb{H}}$, and these two subgroups generate another subgroup $\langle (b^{g_1}, 1), (1, b^{g_2}) \mid g_1, g_2 \in \mathbb{G} \rangle = \langle (b^{g_1}, b^{g_2}) \mid g_1, g_2 \in \mathbb{G} \rangle \cong \mathbb{B} \times \mathbb{B} \subseteq \tilde{\mathbb{H}}$. □

Proposition 3.8. $[\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}] \leq 64$.

Proof. Using the previous proposition, we have that $[\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}] \leq [\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}]$. Now, if $\varphi : \mathbb{G} \longrightarrow \mathbb{G}/\mathbb{B}$ is the natural quotient epimorphism, we can consider the homomorphism $(\varphi, \varphi) : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}/\mathbb{B} \times \mathbb{G}/\mathbb{B}$, which is also an epimorphism, and its kernel is $\mathbb{B} \times \mathbb{B}$. This defines an isomorphism $(\mathbb{G} \times \mathbb{G})/(\mathbb{B} \times \mathbb{B}) \cong \mathbb{G}/\mathbb{B} \times \mathbb{G}/\mathbb{B}$, and so $[\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}] = [\mathbb{G} : \mathbb{B}]^2 \leq 8^2 = 64$. This proves the proposition. □

Proposition 3.9. $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$.

Proof. We consider $\mathbb{H} \subseteq \mathbb{G}$ and $\tilde{\mathbb{H}} \subseteq \mathbb{G} \times \mathbb{G}$. Both are normal subgroups of finite index, since the former has index 2 and the latter has index ≤ 64, as we have just checked. Moreover, $\mathbb{H} \cong \tilde{\mathbb{H}}$, via the isomorphism ψ. □

Theorem 3.10. $\mathbb{G}$ *has superpolynomial growth. In particular, there exists some* $\nu > 0$ *such that* $\gamma_{\mathbb{G}} \succcurlyeq e^{n^\nu}$.

Proof. Now that we have that $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$, we can simply use the lower bound lemma to prove the result. □

3.3 Rewriting rules

It will be useful to have an explicit way of writing the image by ψ of any element of $\mathbb{G}$. The rewriting rules we will introduce now will fulfill this purpose.

Definition 3.11. We define the *rewriting rules* as the following rules acting on words representing elements of $\mathbb{G}$ by substituting each letter by its corresponding letter or the empty word 1:

$$\Phi_0 : \begin{cases} a \to 1, & & & \\ b \to a, & c \to a, & d \to 1, & \text{if } \pi(*) \text{ odd}, \\ b \to c, & c \to d, & d \to b, & \text{if } \pi(*) \text{ even}. \end{cases}$$

$$\Phi_1 : \begin{cases} a \to 1, & & & \\ b \to a, & c \to a, & d \to 1, & \text{if } \pi(*) \text{ even}, \\ b \to c, & c \to d, & d \to b, & \text{if } \pi(*) \text{ odd}. \end{cases}$$

We denote by $\pi(*)$ the number of a preceding $*$ in the word. Thus, for instance, if we take $w = abacadad$, then $\Phi_0(w) = adb$ and $\Phi_1(w) = cab$.

Notice that these words may not be reduced, but they still represent elements of $\mathbb{G}$. In this example, $\Phi_0(w)$ is not reduced but represents the same element as ac and $\Phi_1(w)$ is already a reduced word.

Proposition 3.12. *Let $g \in \mathbb{G}$, and let $\psi(g) = s(g_0, g_1) \in \mathbb{G} \times \mathbb{G} \rtimes \mathbb{Z}_2$, with $s \in \{0, t\} = \mathbb{Z}_2$. Let $w = (a) * a * \cdots * a * (a)$ be a reduced word representing g, as in Remark 2.8, and let g'_0 and g'_1 be the elements of $\mathbb{G}$ represented, respectively, by $\Phi_0(w)$ and $\Phi_1(w)$. Then, $g_0 = g'_0$ and $g_1 = g'_1$.*

Proof. We proceed by induction on the length of g. The base case is trivial as shown in Theorem 2.12, and for the general case we only have to decompose

w into products of $*$ and $a * a = *^a$. Then, (g_0, g_1) equals the product of the images by ψ of such syllables, which by induction hypothesis are represented by the rewriting rules. □

Remark 3.13. This decomposition can be used to prove that $\ell(g_0)+\ell(g_1) \leq \ell(g) + 1$, which is not enough to see the subexponential growth but still is useful.

3.4 Subexponential growth of $\mathbb{G}$

Definition 3.14. The n-th level stabilizer of $\mathbb{G}$ is

$$\mathbb{H}^{(n)} = \mathrm{St}_{\mathbb{G}}(n) = \{\tau \in \mathbb{G} \mid \tau(v) = v \quad \forall v \in T : |v| \leq n\},$$

the subgroup of elements in $\mathbb{G}$ leaving fixed the first n levels of the tree.

Proposition 3.15. $[\mathbb{G} : \mathbb{H}^{(n)}] \leq 2^{2^n - 1}$.

Proof. Let $v \in T$. Let $\varepsilon_v : \mathrm{Aut}(T) \longrightarrow \{0, 1\}$ be a map defined as

$$\varepsilon_v(\tau) = \begin{cases} 0 & \text{if } \tau(v_0) = \tau(v)_0,\ \tau(v_1) = \tau(v)_1 \\ 1 & \text{if } \tau(v_0) = \tau(v)_1,\ \tau(v_1) = \tau(v)_0. \end{cases}$$

In other words, at each vertex $v \in T$, τ maps its children v_0, v_1 to the children of $\tau(v)$. So, for each vertex, τ has two possibilities: either τ maps the left child to the left child and the right child to the right child, and so $\varepsilon_v(\tau) = 0$, or it exchanges them, and so $\varepsilon_v(\tau) = 1$. Notice that an automorphism $\tau \in \mathrm{Aut}(T)$ is uniquely determined by $\varepsilon_v(\tau)$, $\forall v \in T$.

Now let us consider the following subgroup of $\mathrm{Aut}(T)$:

$$A_m = \{\tau \in \mathrm{Aut}(T) \mid \varepsilon_v(\tau) = 0 \quad \forall v \in T : |v| \geq m\}.$$

Elements in A_m may only exchange vertices in the first m levels. For instance, $A_1 = \{1, a\}$ and A_2 has 8 elements, since we can only choose the value for $\varepsilon_v(\tau)$ in three vertices, the root and its children. More generally, since elements in A_m have freedom in the first m levels of the tree, which means $2^m - 1$ vertices, and for each vertex we may choose $\varepsilon_v(\tau) = 0, 1$, A_m has $2^{2^m - 1}$ elements.

Finally, consider the quotient $\mathrm{Aut}(T)/\mathbb{H}^{(n)}$. Every element in $\mathrm{Aut}(T)$ can be decomposed as the product of an element in A_n and an element in $\mathbb{H}^{(n)}$. In the quotient, this decomposition means that the number of equivalence classes is $|A_n|$. Now, $[\mathbb{G} : \mathbb{H}^{(n)}] \leq [\mathrm{Aut}(T) : \mathbb{H}^{(n)}] = |A_n| = 2^{2^n-1}$. □

At this point, we are interested in finding some upper bound condition on the length of elements in $\mathbb{G}$ in order to check its subexponential growth. If we denote $\psi_3 = \psi\big|_{\mathbb{H}^{(3)}}$, we have a map

$$\begin{array}{rccc} \chi: & \mathbb{H}^{(3)} & \longrightarrow & \mathbb{G}^8 \\ & h & \longmapsto & (g_{000}, g_{001}, \ldots, g_{111}) \end{array}$$

where g_{ijk} denote 3-children of h, which all belong to $\mathbb{G}$. A straightforward application of the rewriting rules yields that $\ell(g_{000}) + \ell(g_{001}) + \cdots + \ell(g_{111}) \leq \ell(h) + 7$, but unfortunately, this condition is not enough to assure the subexponential growth. To this purpose we introduce the following lemma.

Lemma 3.16. *Let $h \in \mathbb{H}^{(3)}$ and $g_{000}, g_{001}, \ldots, g_{111}$ as above. Then, $\ell(g_{000}) + \ell(g_{001}) + \cdots + \ell(g_{111}) \leq \frac{5}{6}\,\ell(h) + 8$.*

Proof. Let $w = (a)*a*\cdots*a*(a)$ be a reduced decomposition of h. Applying the rewriting rules, we get two words w_0, w_1, representing elements g_0, g_1. If we do it again with these two words, we get four words $w_{00}, w_{01}, w_{10}, w_{11}$, representing the elements $g_{00}, g_{01}, g_{10}, g_{11}$. Finally, another iteration gives eight words $w_{000}, w_{001}, \ldots, w_{111}$, and again we call the elements they represent $g_{000}, g_{001}, \ldots, g_{111}$. Notice that the resulting words may not be reduced, but in any case we have $\ell(g_i) \leq |w_i|$, $\ell(g_{ij}) \leq |w_{ij}|$ and $\ell(g_{ijk}) \leq |w_{ijk}|$.

Moreover, the rewriting rules provide the following inequalities:

$$\ell(g_0) + \ell(g_1) \leq \ell(h) + 1$$

$$\ell(g_{00}) + \cdots + \ell(g_{11}) \leq \ell(g_0) + \ell(g_1) + 2$$

$$\ell(g_{000}) + \cdots + \ell(g_{111}) \leq \ell(g_{00}) + \cdots + \ell(g_{11}) + 4.$$

Now, to simplify notation, let us define the words $w' = w_0 w_1$, $w'' = w_{00} \dots w_{11}$, $w''' = w_{000} \dots w_{111}$ by concatenation.

By the construction of the rewriting rules, every a in w gets cancelled both in w_0 and w_1, and every d in w gets cancelled either in w_0 or in w_1, and not in both. So $|w'| \leq |w| + 1 - |w|_d$. This inequality cannot be iterated because w_0 and w_1 may not be reduced, but similarly, every c in w produces a d in w', which is cancelled in w'', and every b in w produces a c in w', which produces a d in w'', which is cancelled in w'''. Hence we have the following inequalities:

$$|w'| \leq |w| + 1 - |w|_d$$

$$|w''| \leq |w| + 3 - |w|_c$$

$$|w'''| \leq |w| + 7 - |w|_b.$$

Since $|w|_b + |w|_c + |w|_d \geq \frac{|w|-1}{2}$, at least one letter satisfies $|w|_* > \frac{|w|}{6} - 1$. Recovering all the inequalities above, we have

$$\ell(g_{000}) + \cdots + \ell(g_{111}) \leq \min\{|w'| + 2 + 4, |w''| + 4, |w'''|\} \leq$$

$$\leq \min\{|w| + 1 - |w|_d + 2 + 4, |w| + 3 - |w|_c + 4, |w| + 7 - |w|_b\} =$$

$$= \min\{|w| + 7 - |w|_d, |w| + 7 - |w|_c, |w| + 7 - |w|_b\} =$$

$$= |w| + 7 - \max\{|w|_b, |w|_c, |w|_d\} \leq |w| + 7 - (\frac{|w|}{6} - 1) = \frac{5}{6}|w| + 8 = \frac{5}{6}\,\ell(h) + 8.$$

□

Proposition 3.17. $\mathbb{G}$ *has subexponential growth. In particular, there exists some* $\nu < 1$ *such that* $\gamma_{\mathbb{G}}(n) \preccurlyeq e^{n^\nu}$.

Proof. Let $g \in \mathbb{G}$. It can be written as $g = uh$, with $h \in \mathbb{H}^{(3)}$ and u a coset representative of $\mathbb{G}/\mathbb{H}^{(3)}$. Since $[\mathbb{G} : \mathbb{H}^{(3)}] \leq 128$, there are at most 127 such representatives u, and moreover we can choose them to satisfy $\ell(u) \leq 127$. This is so because we start with the neutral element 1, which is a representative for $\mathbb{H}^{(3)}$, and multiply it by a, b, c or d. This gives, at least, one representative for a coset different from $\mathbb{H}^{(3)}$, and it has length 1. Iterating this construction, at each step i we have a number of cosets for which we have a representative with length not greater than i, and multiplying all these representatives by all the generators yield necessarily at least one representative of a coset for which we did not have one yet. Hence, we can assume $\ell(u) \leq 127$.

Writing $h = u^{-1}g$ gives $\ell(h) \leq \ell(u^{-1}) + \ell(g) \leq \ell(g) + 127$, but we can decompose h as the product of its 3-children, which commute since $h \in \mathbb{H}^{(3)}$. This gives $h = g_{000}g_{001}\dots g_{111}$. In this situation, Lemma 3.16 states that

$$\ell(g_{000})+\ell(g_{001})+\dots+\ell(g_{111}) \leq \frac{5}{6}\,\ell(h)+8 \leq \frac{5}{6}(\ell(g)+127)+8 < \frac{5}{6}\,\ell(g)+114.$$

Now we want to count how many elements g of length $\leq n$ can be constructed. Since $g = uh$, $\gamma(n) \leq 128k$, where k is the number of different h we can construct. Notice that $h = g_{000}g_{001}\dots g_{111}$, so the number of different such h equals the number of different such g_{ijk}. In this decomposition, we had the restriction $\ell(g_{000}) + \dots + \ell(g_{111}) \leq \frac{5}{6}\,\ell(g) + 114 = \frac{5}{6}n + 114$.

Hence,

$$\gamma(n) \leq 128 \sum_{(n_1,\dots,n_8)} \gamma(n_1)\dots\gamma(n_8), \qquad \text{with} \sum_i n_i \leq \frac{5}{6}n + 114.$$

To eliminate the constant term, let us define $m = 137 + n$, so that $\frac{5}{6}n + 114 < \frac{5}{6}m$, and rewrite

$$\gamma(m) = \gamma(137 + n) \leq 4^{137}\gamma(n) \leq 4^{137}128 \sum_{(n_1,\ldots,n_8)} \gamma(n_1)\ldots\gamma(n_8) =$$

$$= 2^{281}\gamma^{*8}\left(\frac{5}{6}n + 114\right) \leq 2^{281}\gamma^{*8}\left(\frac{5}{6}m\right).$$

With this inequality, the hypothesis for Lemma 3.2 are satisfied and so $\mathbb{G}$ has subexponential growth. □

4 Similar constructions

Back to 1980, Grigorchuk was the first one to find a group of intermediate growth. $\mathbb{G}$ was a group explicitly constructed to solve this problem. In this section, we wonder what happens if we construct groups in the way Grigorchuk did but slightly modifying the definition.

4.1 The group $\mathbb{G}_2$

Something that attracts the attention in the definition of $\mathbb{G}$ is the way in which the elements b, c and d are constructed. Recall that, to generate $\mathbb{G}$, they are defined as $b = \varphi(a, c)$, $c = \varphi(a, d)$ and $d = \varphi(1, b)$. Graphically, they are as follows:

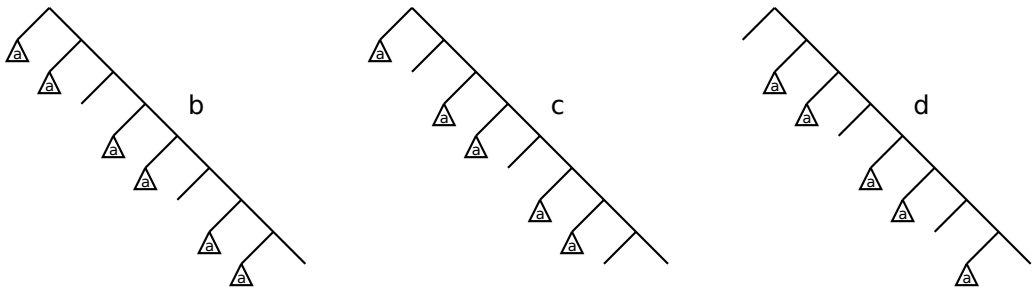

Figure 8: In the definition of $\mathbb{G}$, the construction of b, c and d skips left branches modulo 3.

Here, there is no obvious reason for which we should state this definition modulo 3. Thus, in this section we will introduce a new group, $\mathbb{G}_2$, with the same definition as $\mathbb{G}$ but modulo 2, and we will try to figure out what similarities and differences does it have compared to $\mathbb{G}$.

Definition 4.1. We retrieve the setting as in the definition of $\mathbb{G}$. Let T be the rooted infinite binary tree, and consider $\mathrm{Aut}(T)$ its group of automorphisms. Let $a \in \mathrm{Aut}(T)$ be the automorphism exchanging both subtrees of T, and let also φ and ψ be the inverse isomorphisms between $\mathrm{Aut}(T)$ and $\mathrm{Aut}(T) \times \mathrm{Aut}(T) \rtimes \mathbb{Z}_2$. Now we forget the definition of b, c, d as it was and define $b = \varphi(a, c)$ and $c = \varphi(1, b)$. Pictorially, they are as in the figure:

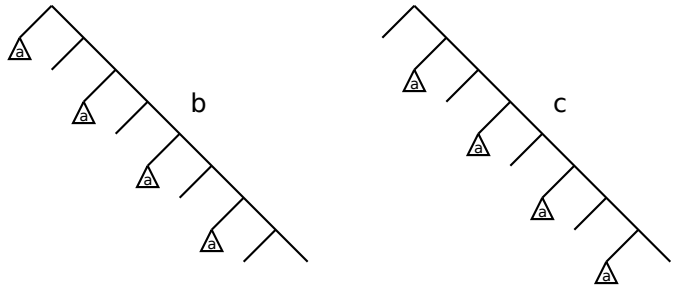

Figure 9: b and c are now defined skipping a branch in each two.

Definition 4.2. We use these elements to define $\mathbb{G}_2 = \langle a, b, c \rangle \subset \mathrm{Aut}(T)$.

Remark 4.3. The first similarity we already find between $\mathbb{G}_2$ and $\mathbb{G}$ is that all their generators are involutions:

$$a^2 = 1 \qquad b^2 = 1 \qquad c^2 = 1.$$

Moreover, b and c still commute:

$$bc = cb$$

However, we quickly notice also the first difference, which will become the key when comparing both groups. In $\mathbb{G}$, the product of all b, c and d was

the neutral element. Nevertheless, in $\mathbb{G}_2$, we have

$$bc = r \neq 1$$

where r is the element whose left branches all apply a, without skipping any level:

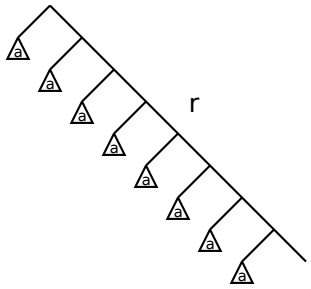

Figure 10: b and c produce a new element r which was not in $\mathbb{G}$.

This fact is very important and will have some consequences which will give us some information about the group $\mathbb{G}_2$ itself.

Remark 4.4. First of all, notice that this relation now does not allow us to generate the group $\mathbb{G}_2$ with fewer generators. Indeed, the relations

$$(ab)^8 = (ac)^4 = 1$$

show that both $\langle a, b\rangle$ and $\langle a, c\rangle$ are dihedral quotients, and we will see that $\mathbb{G}_2$ is infinite, so the three generators are needed.

Remark 4.5. The facts that all generators are involutions and that b and c commute show that every element of $\mathbb{G}_2$ can be written as $(a)*a*\cdots*a*(a)$, where $* \in \{b, c, r = bc\}$. Notice that this differs with what happened for $\mathbb{G}$, where an additional product was not needed.

Definition 4.6. We can also define the *fundamental subgroup* $\mathbb{H}_2$ of $\mathbb{G}_2$, as

$$\mathbb{H}_2 = \{\tau \in \mathbb{G}_2 \mid \tau(v) = v \quad \forall v \text{ such that } |v| = 1\}$$

Again we notice that $a \notin \mathbb{H}_2$, while b and c do.

Proposition 4.7.

1. $[\mathbb{G}_2 : \mathbb{H}_2] = 2$.

2. $\mathbb{H}_2 \lhd \mathbb{G}_2$.

3. $\mathbb{H}_2 = \langle b, c, b^a, c^a \rangle$.

Proof. The same argument as for $\mathbb{G}$ is still valid. a exchanges vertices in the first level, while b and c do not. □

Theorem 4.8. $\mathbb{G}_2$ *is infinite.*

Proof. Again, notice that $\tilde{\mathbb{H}}_2 = \psi(\mathbb{H}_2) \subset \mathbb{G}_2 \times \mathbb{G}_2$. Indeed, we have

$$b \longmapsto (a, c) \qquad c \longmapsto (1, b)$$

$$b^a \longmapsto (c, a) \qquad c^a \longmapsto (b, 1)$$

Moreover, $\tilde{\mathbb{H}}_2$ also projects surjectively onto each component, since every generator belongs to the image.

If $\mathbb{G}_2$ was finite, then we would have $|\mathbb{G}_2| = 2|\mathbb{H}_2| > |\mathbb{H}_2| \geq |\mathbb{G}_2|$, which is again a contradiction. □

So far, everything we have seen for $\mathbb{G}_2$ is quite similar to what we saw for $\mathbb{G}$, although we already found some differences. Now we will prove that both of them are essentially different, by finding an element in $\mathbb{G}_2$ of infinite order. This fact is strongly opposed to what we knew from $\mathbb{G}$, and implies that both groups are not isomorphic.

Lemma 4.9. *The element $ar = abc \in \mathbb{G}_2$ has infinite order.*

Proof. Since automorphisms of T preserve the level of the vertices, we can think an automorphism as an infinite sequence of permutations on 2^n vertices, each corresponding to the permutation induced at each level. An automorphism is the identity if and only if this sequence is the identity sequence.

We claim that, for the element ar, the order of the permutation at level n is 2^n. Proceeding by induction on n, we can easily see that the root is always fixed and that the two vertices in the first layer are exchanged by a, but fixed by b and c, since they belong to $\mathbb{H}_2$.

Now, if we consider the level n and assume the claim true for the previous levels, we have that the permutation at level $n-1$ is a 2^{n-1} cycle. Since tree automorphisms preserve the parent-child relation, each vertex on the nth layer must be mapped by any automorphism of the tree to a child of the image of its parent. This means that if v is a vertex in the $n-1$ level and $ar(v) = w$, then either $ar(v_0) = w_0$ and $ar(v_1) = w_1$, or $ar(v_0) = w_1$ and $ar(v_1) = w_0$. But now we observe that in the level n, ar maps a left children to a left children always except only for vertices $r_{01\ldots100}$ and $r_{01\ldots101}$, whose images are $r_{11\ldots101}$ and $r_{11\ldots100}$, respectively. Now the permutation involving any vertex must run through 2^{n-1} vertices before returning to its parent, but then the parity of the children (left/right) will have changed whenever it arrived to vertices of parent $r_{01\ldots10}$, hence having to repeat the whole process until arriving to the same vertex again. Therefore, the order of the permutation is 2^n. □

Corollary 4.10. $\mathbb{G}_2 \ncong \mathbb{G}$. *This is due to the fact that $\mathbb{G}_2$ has an element of infinite order and $\mathbb{G}$ has not.*

4.2 Generalizations

So far we have shown that $\mathbb{G}_2$ and $\mathbb{G}$ have some differences. Essentially, these differences come from the element resulting of the product of all generators different from a: In $\mathbb{G}$, $bcd = 1$ but for $\mathbb{G}_2$ $bc = r$, a new element which is composed by an a rooted at each left branch. This new element is not in $\mathbb{G}$, and ar has infinite order.

If we consider the same construction modulo 4, and define b, c, d and e in a similar way, then we get again the element r as $bcde$, and so ar is also in $\mathbb{G}_4$. For $\mathbb{G}_5$, however, we get again $bcdef = 1$.

This seems enough to conclude some conjectures, but before, let us define the groups formally.

Definition 4.11. We define $\mathbb{G}_n$ as $\langle a, a_1, \ldots, a_n \rangle$, where a_i is defined as $\varphi(a, a_{i+1})$ except for $a_n = \varphi(1, a_1)$.

Remark 4.12. Under this setting, Grigorchuk's group $\mathbb{G}$ is $\mathbb{G}_3$, and $\mathbb{G}_2$ preserves its definition.

Remark 4.13. If we consider the product $a_1 \ldots a_n$, we can write the following equality:

$$\psi(a_1 \ldots a_n) = \psi(a_1) \ldots \psi(a_n) = \psi(\varphi(a, a_2)) \ldots \psi(\varphi(a, a_n))\psi(\varphi(1, a_1)) =$$

$$= (a, a_2) \ldots (a, a_n)(1, a_1) = (a^{n-1}, a_2 \ldots a_n a_1) = (a^{n-1}, a_1 \ldots a_n),$$

where in the last step we have used that the a_i commute pairwise.

This is $(1, a_1 \ldots a_n)$ for odd n, which implies that $a_1 \ldots a_n$ is the identity at each left branch and so $a_1 \ldots a_n = 1$. For even n, however, this is $(a, a_1 \ldots a_n)$,

which shows that the product equals the element r we defined above, applying a to every left branch without exception.

It seems that the first left branch with an identity determines the order of the element, both in the Grigorchuk group ($(ab)^{16} = (ac)^8 = (ad)^4 = 1$) and in $\mathbb{G}_2$ ($(ab)^8 = (ac)^4 = 1$). Hence, the element ar has infinite order, and it belongs to $\mathbb{G}_n$ only for even n.

Regarding the growth, it seems plausible that for every n we have groups of superpolynomial growth, which might be proved in the same way that for $\mathbb{G}$, but adapting the proof. The subexponentiality, however, seems a reasonable hypothesis for odd n, but for even n we can find a subgroup $\langle a_1 \dots a_{n-1}, aa_n \rangle$ in $\mathbb{G}_n$ satisfying $(a_1 \dots a_{n-1})^2 = 1$, $(aa_n)^4 = 1$ but with the product $aa_1 \dots a_n$ with infinite order. If one can prove that this subgroup has no other relations, then it could be isomorphic to the free product $\mathbb{Z}_2 * \mathbb{Z}_4$, which has exponential growth, and so would have $\mathbb{G}_n$ with even n.

Indeed, we cannot expect the same proof of the subexponential growth of $\mathbb{G}$ to be easily generalized to $\mathbb{G}_n$ for even n. Recall the rewriting rules we defined, and now consider them for $\mathbb{G}_2$, for instance: If we have a reduced word $w = (a) * a * \cdots * a * (a)$, with $* \in \{b, c, r\}$, then they would be:

$$\Phi_0 : \begin{cases} a \to 1, & & & \\ b \to a, & c \to 1, & r \to a, & \text{if } \pi(*) \text{ odd}, \\ b \to c, & c \to b, & r \to r, & \text{if } \pi(*) \text{ even}. \end{cases}$$

$$\Phi_1 : \begin{cases} a \to 1, & & & \\ b \to a, & c \to 1, & r \to a, & \text{if } \pi(*) \text{ even}, \\ b \to c, & c \to b, & r \to r, & \text{if } \pi(*) \text{ odd}. \end{cases}$$

We observe that each r yields another r either by Φ_0 o by Φ_1. This implies that words of the type $w = (a)rar \dots rar(a)$ yield again two more words of the same type and half the length, and so the length of both words concatenated is constant, so the bound cannot be improved.

References

[1] Pierre de la Harpe. *Topics in geometric group theory*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2000.

[2] Rostislav Grigorchuk and Igor Pak. Groups of intermediate growth: an introduction. *Enseign. Math. (2)*, 54(3-4):251–272, 2008.

[3] R. I. Grigorčuk. On Burnside's problem on periodic groups. *Funktsional. Anal. i Prilozhen.*, 14(1):53–54, 1980.

[4] Mikhael Gromov. Groups of polynomial growth and expanding maps. *Inst. Hautes Études Sci. Publ. Math.*, (53):53–73, 1981.

[5] Narain Gupta and Saïd Sidki. On the Burnside problem for periodic groups. *Math. Z.*, 182(3):385–388, 1983.

[6] I. G. Lysënok. A set of defining relations for the Grigorchuk group. *Mat. Zametki*, 38(4):503–516, 634, 1985.

[7] Avinoam Mann. *How groups grow*, volume 395 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2012.

[8] John Milnor. Growth of finitely generated solvable groups. *J. Differential Geometry*, 2:447–449, 1968.