Groups of Intermediate Growth:
an Introduction for Beginners

Rostislav Grigorchuk
Department of Mathematics
Texas A&M University
College Station, TX 77843
grigorch@math.tamu.edu

Igor Pak
Department of Mathematics
MIT, Room 2-390
Cambridge, MA 02139
pak@math.mit.edu

January 3, 2004

Introduction

The study of growth of groups has a long and remarkable history spanning over much of the twentieth century, and goes back to Alphors, Hilbert, Poincare, etc. In 1968 it became apparent that all known classes of groups have either polynomial or exponential growth, and John Milnor formally asked whether groups of intermediate growth exist. The first such examples were introduced by the first author two decades ago [4] (see also [3, 5]), and since then there has been an explosion in the number of works on the subject. While new techniques and application have been developed, much of the literature remains rather specialized, accessible only to specialists in the area. This paper is an attempt to present the material in an introductory manner, to the reader familiar with only basic algebraic concepts.

We concentrate on study of *the first construction*, a finitely generated group $\mathbb{G}$ introduced by the first author to resolve Milnor's question, and which became a prototype for further developments. Our Main Theorem shows that $\mathbb{G}$ has *intermediate growth*, i.e. superpolynomial and subexponential.

Our proof is neither the shortest nor gives the best possible bounds. Instead, we attempt to simplify the presentation as much as possible by breaking the proof into a number of propositions of independent interest, supporting lemmas, and exercises. Along the way we prove two 'bonus' theorems: we show that $\mathbb{G}$ is *periodic* (every element has a finite order) and give a nearly linear time algorithm for the word problem in $\mathbb{G}$. We hope that the beginner readers now have an easy time entering the field and absorbing what is usually viewed as unfriendly material.

Let us warn the reader that this paper neither gives a survey nor presents a new proof of the Main Theorem. We refer to extensive survey articles [1, 2, 6] and a recent book [7] for further results and references. Our proofs roughly follow [5, 9], but the presentation and details are mostly new.

The paper is structured is as follows. We start with some background information on the growth of groups (Section 1) and technical results for bounding the growth function (Section 2). These technical results have elementary analytic nature; their proofs are moved to the Appendix (Section 13). In Section 3 we study the group $\mathrm{Aut}(\mathbf{T})$ of automorphisms of an infinite binary (rooted) tree. The 'first construction' group $\mathbb{G}$ is introduced in Section 4, while the remaining sections 5–11 prove the intermediate growth of $\mathbb{G}$ and two 'bonus' theorems. We conclude with final remarks and few open problems (Section 12).

Notation. Throughout the paper we use only *left* group multiplication. For example, a product $\tau_1 \cdot \tau_2$ of automorphisms $\tau_1, \tau_2 \in \mathrm{Aut}(\mathbf{T})$ is given by $[\tau_1 \cdot \tau_2](v) = \tau_2(\tau_1(v))$. We use notation $g^h = h^{-1}gh$ for conjugate elements, and $\mathtt{1}$ for the identity element. Finally, let $\mathbb{N} = \{0, 1, 2, \ldots\}$.

1. Growth of groups

Let $S = \{s_1, \ldots, s_k\}$ be a generating set of a group $G = \langle S \rangle$. For every group element $g \in G$, denote by $\ell(g) = \ell_S(g)$ the length of the shortest decomposition $g = s_{i_1}^{\pm 1} \cdots s_{i_\ell}^{\pm 1}$. Let $\gamma_G^S(n)$ be the number of elements $g \in G$ such that $\ell(g) \le n$. Function $\gamma = \gamma_G^S$ is called the *growth function* of the group G with respect to the generating set S. Clearly, $\gamma(n) \le \sum_{i=0}^{n} (2k)^n \le (2k+1)^n$.

Exercise 1.1. *Let G be an infinite group. Prove that the growth function γ is* monotone increasing: $\gamma(n+1) > \gamma(n)$*, for all $n \ge 1$.*

Exercise 1.2. *Check that the growth function γ is* submultiplicative:
$\gamma(m+n) \le \gamma(m)\,\gamma(n)$*, for all $m, n \ge 1$.*

Consider two functions $\gamma, \gamma' : \mathbb{N} \to \mathbb{N}$. Define $\gamma \preccurlyeq \gamma'$ if $\gamma(n) \le C\,\gamma'(\alpha n)$, for all $n > 0$ and some $C, \alpha > 0$. We say that γ and γ' are *equivalent*, write $\gamma \sim \gamma'$, if $\gamma \preccurlyeq \gamma'$ and $\gamma' \preccurlyeq \gamma$.

Exercise 1.3. *Let S and S' be two generating sets of G. Prove that the corresponding growth functions γ_G^S and $\gamma_G^{S'}$ are equivalent.*

A function $f : \mathbb{N} \to \mathbb{R}$ is called *polynomial* if $f(n) \sim n^\alpha$, for some $\alpha > 0$. A function f is called *superpolynomial* if there exists a limit $\frac{\ln \gamma(n)}{\ln n} \to \infty$ as $n \to \infty$. For example, n^π is polynomial, n^n is superpolynomial, while $\exp\bigl(n^{\sin n}\bigr)$ is neither.

Similarly, a function f is called *exponential* if $f(n) \sim e^n$. A function f is called *subexponential* if there exists a limit $\frac{\ln \gamma(n)}{n} \to 0$ as $n \to \infty$. For example, $\exp\bigl(n/2 - |\sin n|\sqrt{n}\,\log^2 n\bigr)$ is exponential, $e^{n/\log n}$ and n^π are subexponential, while $\exp\bigl(n^{\sin n}\bigr)$ and n^n are neither.

Finally, a functions f is said to have *intermediate growth* if f is both subexponential and superpolynomial. For example, $n^{\log\log n}$, $e^{\sqrt{n}}$, and $e^{n/\log n}$ all have intermediate growth, while functions $e^{\sqrt{\log n}}$ and $n! \sim \left(\frac{n}{e}\right)^n \sim e^{n\log n}$ do not.

Exercise 1.3 implies that we can speak of groups with *polynomial, exponential* and *intermediate growth.* By a slight abuse of notation, we denote by γ_G the growth function with respect to *any* particular set of generators. Using the equivalence of functions, we can speak of groups G and H as having *equivalent growth*: $\gamma_G \sim \gamma_H$.

Exercise 1.4. *Let G be an infinite group with polynomial growth. Prove that the direct product $G^m = G \times G \times \ldots \times G$ also has polynomial growth, but $\gamma_G \nsim \gamma_{G^m}$ for all $m \geq 2$. Similarly, if G has exponential growth then so does G^m, but $\gamma_G \sim \gamma_{G^m}$.*

Exercise 1.5. *Let H be a subgroup of G of finite index. Prove that their growth functions are equivalent: $\gamma_H \sim \gamma_G$.*

Exercise 1.6. *Let S be a generating set of a group G, and let $\gamma = \gamma_G^S(n)$ be its growth function. Show that the the limit*

$$\lim_{n\to\infty} \frac{\ln \gamma(n)}{n}$$

always exist. This limits is called the growth rate *of G. Deduce from here that every group G has either exponential or subexponential growth.*

2. Tools for proving the growth

The following two technical results are key is our analysis of growth of groups. Their proofs are based on straightforward analytic arguments and have no group theoretic content. For convenience of the reader we move the proof into Appendix (Section 13).

Lemma 2.1 (Lower Bound Lemma)**.** *Let $f : \mathbb{N} \to \mathbb{R}_+$ be a monotone increasing function, such that $f(n) \to \infty$ as $n \to \infty$. Suppose $f \succcurlyeq f^m$ for some $m > 1$. Then $f(n) \succcurlyeq \exp(n^\alpha)$ for some $\alpha > 0$.*

For the upper bound, we need to introduce a notation. Let $f : \mathbb{N} \to \mathbb{R}_+$ be a monotone increasing function, and let:

$$f^{\star k}(n) := \sum_{(n_1,\ldots,n_k)} f(n_1)\cdots f(n_k),$$

where the summation is over all k-tuples $(n_1, \ldots, n_k) \in \mathbb{N}^k$ such that $n_1 + \ldots + n_k \leq n$.

Lemma 2.2 (Upper Bound Lemma)**.** *Let $f(n)$ be a nonnegative monotone increasing function, such that $f(n) \to \infty$ as $n \to \infty$. Suppose $f(n) \leq C\, f^{\star k}(\alpha n)$ for some $k \geq 2$, $C > 0$, and $0 < \alpha < 1$. Then $f(n) \preccurlyeq \exp(n^\beta)$ for some $\beta < 1$.*

Let us note that $f^{\star k}(n) \leq f^k(n)$, but the Upper Bound Lemma does not hold if we substitute function $f^{\star k}$ with a power f^k.

3. Group automorphisms of a tree

Consider an infinite binary tree $\mathbf{T}$ as shown in Figure 1. Denote by V the set of vertices v in $\mathbf{T}$, which are in a natural bijection with finite **0**-**1** words $v = (x_0, x_1, \ldots) \in \{\mathbf{0}, \mathbf{1}\}^*$. Note that the root of $\mathbf{T}$, denotes $\mathbf{r}$, corresponds to an empty word $\varnothing$. Let E be the set of (oriented) edges in $\mathbf{T}$, which are oriented away from the root. By definition, $(v, w) \in E$ if $w = v\mathbf{0}$ or $w = v\mathbf{1}$. Denote by $|v|$ the distance from the root $\mathbf{r}$ to vertex v; we call it the *level* of v. Finally, denote by $\mathbf{T}_v$ a subtree of $\mathbf{T}$ rooted in $v \in V$. Clearly, $\mathbf{T}_v$ is isomorphic to $\mathbf{T}$.

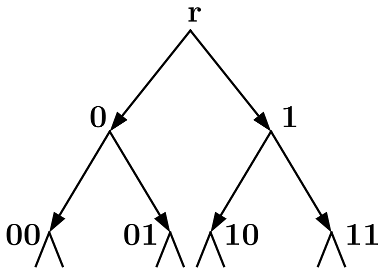

Figure 1. Infinite binary tree $\mathbf{T}$.

The main subject of this section is the group $\mathrm{Aut}(\mathbf{T})$ of automorphisms of $\mathbf{T}$, i.e. bijections $\tau : V \to V$ which map edges into edges. Note that the root $\mathbf{r}$ is always a fixed point of τ, i.e. $\tau(\mathbf{r}) = \mathbf{r}$. Furthermore, all automorphisms $\tau \in \mathrm{Aut}(\mathbf{T})$ preserve the level of vertices: $|\tau(v)| = |v|$, for all $v \in V$. Denote by $\mathtt{I} \in \mathrm{Aut}(\mathbf{T})$ a trivial (identity) automorphism of $\mathbf{T}$.

An example of a nontrivial automorphism $a \in \mathrm{Aut}(\mathbf{T})$ is given in Figure 2. This is the most basic automorphism which will be used throughout the paper, and can be formally defined as follows. Denote by $\mathbf{T_0}$ and $\mathbf{T_1}$ the left and right subtrees (branches) of the tree $\mathbf{T}$, with roots at $\mathbf{0}$ and $\mathbf{1}$, respectively. Let a be an automorphism which maps $\mathbf{T_0}$ into $\mathbf{T_1}$ and preserves the natural order on vertices:

$$\tau : (\mathbf{0}, x_1, x_2, \ldots) \longleftrightarrow (\mathbf{1}, x_1, x_2, \ldots).$$

Clearly, automorphism a is an involution: $a^2 = \mathtt{I}$.

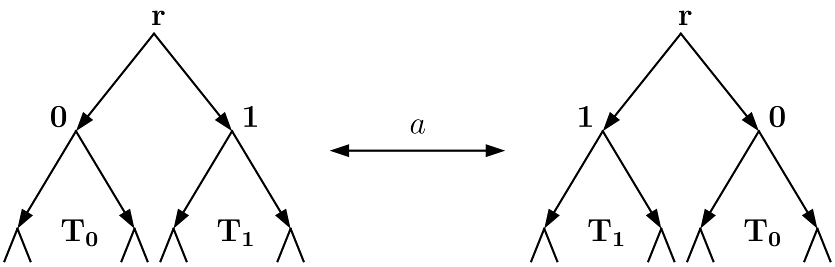

Figure 2. Automorphism $a \in \mathrm{Aut}(\mathbf{T})$.

Similarly, one can define an automorphism a_v which exchanges two branches $\mathbf{T}_{v\mathbf{0}}$ and $\mathbf{T}_{v\mathbf{1}}$ of a subtree $\mathbf{T}_v$ rooted in $v \in V$. These automorphisms will be used in the next section to define the subgroup $G \subset \mathrm{Aut}(\mathbf{T})$.

More generally, denote by $\mathrm{Aut}(\mathbf{T}_v)$ the subgroup of automorphisms in $\mathrm{Aut}(\mathbf{T})$ which preserve subtree T_v and are trivial on the outside of T_v. There is a natural graph isomorphism $\iota_v : \mathbf{T} \to \mathbf{T}_v$ which extends to a group isomorphism $\iota_v : \mathrm{Aut}(\mathbf{T}) \to \mathrm{Aut}(\mathbf{T}_v)$.

By definition, every automorphism $\tau \in \mathrm{Aut}(\mathbf{T})$ maps two edges leaving vertex v into two edges leaving vertex $\tau(v)$. Thus we can define a *sign* $\epsilon_v(\tau) \in \{0, 1\}$ as follows:

$$\epsilon_v(\tau) = \begin{cases} 0, & \text{if } \ \tau(v\mathbf{0}) = \tau(v)\mathbf{0}, \ \tau(v\mathbf{1}) = \tau(v)\mathbf{1}, \\ 1, & \text{if } \ \tau(v\mathbf{0}) = \tau(v)\mathbf{1}, \ \tau(v\mathbf{1}) = \tau(v)\mathbf{0}. \end{cases}$$

In other words, $\epsilon_v(\tau)$ is equal to 0 if the automorphism maps the left edge leaving vertex v into the left edge leaving $\tau(v)$, and is equal to 1 if the automorphism maps the left edge leaving v into the right edge leaving $\tau(v)$.

Observe that the collection of signs $\{\epsilon_v(\tau)\}$ can take all possible values, and uniquely determines the automorphism $\tau \in \mathrm{Aut}(\mathbf{T})$. As a corollary, the group $\mathrm{Aut}(\mathbf{T})$ is uncountable and cannot be finitely generated.

To further understand the structure of $\mathrm{Aut}(\mathbf{T})$, consider a map

$$\varphi : \ \mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T}) \ \to \ \mathrm{Aut}(\mathbf{T}),$$

defined as follows. If $\tau_0, \tau_1 \in \mathrm{Aut}(\mathbf{T})$, let $\tau = \varphi(\tau_0, \tau_1)$ be an automorphism defined by $\tau := \iota_{\mathbf{0}}(\tau_0) \cdot \iota_{\mathbf{1}}(\tau_1) \in \mathrm{Aut}(\mathbf{T})$. Here $\iota_{\mathbf{0}}(\tau_0) \in \mathrm{Aut}(\mathbf{T_0})$ and $\iota_{\mathbf{1}}(\tau_1) \in \mathrm{Aut}(\mathbf{T_1})$ are the automorphisms of subtrees $\mathbf{T_0}$ and $\mathbf{T}_1$, respectively, defined as above. Pictorially, automorphism τ is shown in Figure 3.

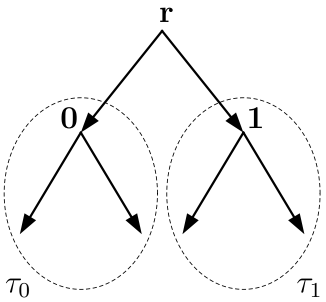

FIGURE 3. Automorphism $\tau = \varphi(\tau_0, \tau_1) \in \mathrm{Aut}(\mathbf{T})$.

For any group G, the *wreath product* $G \wr \mathbb{Z}_2$ is defined as a semidirect product $(G \times G) \rtimes \mathbb{Z}_2$, with $\mathbb{Z}_2$ acting by exchanging two copies of G.

Proposition 3.1. $\mathrm{Aut}(\mathbf{T}) \simeq \mathrm{Aut}(\mathbf{T}) \wr \mathbb{Z}_2$.

Proof. Let us extend the map φ to an isomorphism

$$\varphi : \ \big(\mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T})\big) \rtimes \mathbb{Z}_2 \ \longrightarrow \ \mathrm{Aut}(\mathbf{T})$$

as follows. When $\sigma = \mathtt{I}$, let $\varphi(\tau_0, \tau_1; \sigma) := \varphi(\tau_0, \tau_1)$, as before. When $\sigma \neq \mathtt{I}$, let $\varphi(\tau_0, \tau_1; \sigma) := \varphi(\tau_0, \tau_1) \cdot a$, where $a \in \operatorname{Aut}(\mathbf{T})$ is defined as above. Now check that multiplication of automorphisms $\varphi(\cdot)$ coincides with that of the semidirect product, and defines the group isomorphism. We leave this easy verification to the reader. □

We denote by $\psi = \varphi^{-1}$ the isomorphism $\psi : \operatorname{Aut}(\mathbf{T}) \to \operatorname{Aut}(\mathbf{T}) \wr \mathbb{Z}_2$ defined in the proof above. This notation will be used throughout the paper.

Exercise 3.2. *Let* $\mathrm{A}_m \subset \operatorname{Aut}(\mathbf{T})$ *be a subgroup of all automorphisms* $\tau \in \operatorname{Aut}(\mathbf{T})$ *such that* $\epsilon_v(\tau) = 0$ *for all* $|v| \geq m$. *For example,* $\mathrm{A}_1 = \{\mathtt{I}, a\}$. *Use the idea above to show that*

$$\mathrm{A}_m \simeq \mathbb{Z}_2 \wr \mathbb{Z}_2 \wr \cdots \wr \mathbb{Z}_2 \quad (m\ \textit{times}).$$

Conclude from here that the order of A_m *is* $|\,\mathrm{A}_m| = 2^{2^m - 1}$.

Exercise 3.3. *Consider a (unique) tree automorphism* $\tau \in \operatorname{Aut}(\mathbf{T})$ *with signs given by:* $\epsilon_v(\tau) = 1$ *if* $v = \mathbf{1}^k = \mathbf{1} \ldots \mathbf{1}$ *(k times), for* $k \geq 0$, *and* $\epsilon_v(\tau) = 0$ *otherwise. Check that* τ *has infinite order in* $\operatorname{Aut}(\mathbf{T})$.
Hint: Consider elements $\tau_m \in \mathrm{A}_m$ with signs as in the definition of above, and $k < m$. Show that the order $\operatorname{ord}(\tau_m) \to \infty$ as $m \to \infty$, and deduce the result from here.

4. The first construction

In this section we define a finitely generated group $\mathbb{G} \subset \operatorname{Aut}(\mathbf{T})$ which we call *the first construction*. Historically, this is the first example of a group with intermediate growth [4].

Let us first define group $\mathbb{G}$ implicitly, by specifying the necessary conditions on generators. Let $\mathbb{G} = \langle a, b, c, d \rangle \subset \operatorname{Aut}(\mathbf{T})$, where a is the automorphism defined as in Section 3, and automorphisms b, c, d satisfy the following conditions:

$$(\circ) \quad b = \varphi(a, c), \quad c = \varphi(a, d), \quad d = \varphi(\mathtt{I}, b).$$

Observe that the automorphisms b, c, and d are defined through each other. Since the generator d is acting as identity automorphism on the left subtree $\mathbf{T_0}$, and as b on the right subtree $\mathbf{T_1}$, one can recursively compute the action of all three automorphisms $b, c, d \in \operatorname{Aut}(\mathbf{T})$.

Here is a direct way to define automorphisms b, c, d :

$$(*) \quad \begin{aligned} b &:= (a_{\mathbf{0}} \cdot a_{\mathbf{1^30}} \cdot a_{\mathbf{1^60}} \cdot \ldots)\,(a_{\mathbf{10}} \cdot a_{\mathbf{1^40}} \cdot a_{\mathbf{1^70}} \cdot \ldots), \\ c &:= (a_{\mathbf{0}} \cdot a_{\mathbf{1^30}} \cdot a_{\mathbf{1^60}} \cdot \ldots)\,(a_{\mathbf{1^20}} \cdot a_{\mathbf{1^50}} \cdot a_{\mathbf{1^80}} \cdot \ldots), \\ d &:= (a_{\mathbf{10}} \cdot a_{\mathbf{1^40}} \cdot a_{\mathbf{1^70}} \cdot \ldots)(a_{\mathbf{1^20}} \cdot a_{\mathbf{1^50}} \cdot a_{\mathbf{1^80}} \cdot \ldots), \end{aligned}$$

where $\mathbf{1}^m$ is short for $\mathbf{1} \ldots \mathbf{1}$ (m times). Note that the automorphisms $a_{\mathbf{1^m0}}$ used in $(*)$ commute with each other, and thus elements $b, c, d \in \operatorname{Aut}(\mathbf{T})$ are well defined.

Theorem 4.1 (Main Theorem)**.** *Group* $\mathbb{G} = \langle a, b, c, d \rangle$ *has intermediate growth.*

The proof of Theorem 4.1 is quite involved and occupies much of the rest of the paper.

Exercise 4.2. *Check that elements* $b, c, d \in \mathrm{Aut}(\mathbf{T})$ *defined by* $(*)$ *satisfy conditions* $(\circ)$.

Exercise 4.3. *Check that elements* $b, c,$ *and* d *are involutions (have order 2), commute with each other, and satisfy* $b \cdot c \cdot d = \mathtt{1}$. *Conclude from here that* $\langle b, c, d\rangle \simeq \mathbb{Z}_2^2$ *and that the group* $\mathbb{G} = \langle a, b, c, d\rangle$ *is 3-generated.*

Exercise 4.4. *Check the following relations in* $\mathbb{G}$: $(ad)^4 = (ac)^8 = (ab)^{16} = \mathtt{1}$. *Deduce from here that 2-generator subgroups* $\langle a, b\rangle, \langle a, c\rangle, \langle a, d\rangle \subset \mathbb{G}$ *are finite.*

While these exercises have straightforward 'verification style' proofs, they will prove useful in the future. Thus we suggest the reader studies them before proceeding to read (hopefully) the rest of the paper.

5. Orders of elements

An element $g \in G$ is said to have a finite order $d = \mathrm{ord}(g)$ if $g^d = \mathtt{1}$ for some integer $d < \infty$. A group is called *periodic* if every element has a finite order. Below we prove that $\mathbb{G}$ is periodic. Interestingly, this was the original motivation for the study of $\mathbb{G}$. Although the result is somewhat tangential to the Main Theorem, the proof reveals some interesting information on the structure of $\mathbb{G}$.

Theorem 5.1. *Group* $\mathbb{G}$ *is periodic. Moreover, every element* $g \in \mathbb{G}$ *has order* $d = 2^m$ *for some integer* $m \geq 0$.

Before proving the theorem let us first justify the claim. Clearly, all finite groups are periodic, and we have yet to show that $\mathbb{G}$ is infinite; we do this in the next section. Now, recall that the full group of tree automorphisms contains an element of infinite order (Exercise 3.3), so not every finitely generated subgroup of $\mathrm{Aut}(\mathbf{T})$ is periodic. Note also that all generators in $\mathbb{G}$ are involutions (Exercise 4.3), and so are the products bc, bd and cd. Finally, the products ab, ac, and ad have orders which are powers of 2 (Exercise 4.4).

Proof. First, let us prove the following technical result. Define

$$\tau_v := \tau|_{\mathbf{T}_v} \in \mathrm{Aut}(\mathbf{T}_v) \subset \mathrm{Aut}(\mathbf{T}), \qquad \widehat{\tau}_v = \iota_v^{-1}(\tau_v) \in \mathrm{Aut}(\mathbf{T}).$$

Here the automorphism τ_v of the subtree $\mathbf{T}_v$ is obtained by keeping all signs ϵ_w for $w \in \mathbf{T}_v$ and setting $\epsilon_w = 0$ otherwise. Similarly, the automorphism $\widehat{\tau}_v$ of the subtree $\mathbf{T}$ is obtained from τ by the group isomorphism ι_v^{-1} induced by the graph isomorphism $\iota_v^{-1} : \mathbf{T}_v \to \mathbf{T}$.

We claim that for every $\tau \in \mathbb{G}$ there exists an integer $n = n(\tau)$ such that $\widehat{\tau}_v \in S = \{a, b, c, d\}$ for every vertex $v \in \mathbf{T}$ with $|v| \geq n$. We prove the claim by induction on the length $\ell(g)$ of elements $g \in \mathbb{G}$. The claim is trivial for the generators: $n(a) = n(b) = n(c) = n(d) = 0$ works in this case.

Suppose the claim holds for $g \in \mathbb{G}$. Then one can take $n(ga) = \max\{n(g), 1\}$ since $\widehat{ga}_v = \widehat{g}_v$ for all $v \neq \mathbf{r}$. Similarly, one can take $n(gb) = n(gc) = n(gd) = n(g) + 1$ since multiplication by an element $* \in \{b, c, d\}$ either changes no signs in $\mathbf{T}_v$, or only the 'top' sign ϵ_v, or it changes infinitely many signs as follows: $\widehat{g*} = \widehat{g} \cdot *'$ for some

$*' \in \{b, c, d\}$ which depends on element $*$ and the level $|v| \mod 3$. This completes the step of induction and proves the claim.

Now we can prove directly that every element $g \in \mathbb{G}$ has has power of 2 order. First, consider an element $h = g^N$ where $N = 2^{2^n - 1}$, and $n = n(g)$. By Exercise 3.2, $N = |\,\mathrm{A}_n|$, so the element h has signs $\epsilon_v = 0$ for all $|v| < n$. Therefore,

$$h \, = \, \prod_{|v|=n} \tau_v \, ,$$

and all elements $\tau_v \in \mathrm{Aut}(\mathbf{T}_v)$ commute with each other and lie in the generating set S. This implies that $g^{2N} = h^2 = \mathtt{I}$ and finishes the proof. □

Exercise 5.2. *Use the proof above to show that the order of every element* $\tau \in \mathrm{Aut}(\mathbf{T})$ *is either infinite or a power of 2.*

This exercise will not be used in the paper. Basically, it shows that the first part of Theorem 5.1 implies the second part.

6. Group $\mathbb{G}$ is infinite

We have yet to establish that $\mathbb{G}$ is infinite. Although one can prove this directly, the proof below introduces definitions and notation which will be helpful in the future.

Let $\mathrm{St}_{\mathbb{G}}(n)$ denote a subgroup of $\mathbb{G}$ stabilizing all vertices with level n. In other words, $\mathrm{St}_{\mathbb{G}}(n)$ consists of all automorphisms $\tau \in \mathbb{G}$ such that $\tau(v) = v$ for all vertices $v \in \mathbf{T}$ with $|v| = n$:

$$\mathrm{St}_{\mathbb{G}}(n) \, = \, \bigcap_{|v|=n} \mathrm{St}_{\mathbb{G}}(v).$$

The subgroup $\mathbb{H} := \mathrm{St}_{\mathbb{G}}(1)$ is called the *fundamental subgroup* of $\mathbb{G}$.

Lemma 6.1. *Let* $\mathbb{H} \subset \mathbb{G}$ *be the fundamental subgroup defined above. Then:*

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

Proof. From Exercise 4.3 we conclude that every reduced decomposition w can is a product $w = (a) * a * a * \ldots * a * (a)$, where each $*$ is either b, c, or d, while the first and last a may or may not appear. Denote by $|w|$ the length of the word w, and by $|w|_a$ the number of occurrences of a in w. Note that $w \in \mathbb{H}$ if and only if $|w|_a$ is even. This immediately implies the third part of the lemma. Since every subgroup of index 2 is normal this also implies the second part.

For the first part, suppose $|w|_a$ is even. Join subsequent occurrences of a to obtain w as a product of $*$ and $(a * a)$. Since $a^2 = \mathtt{I}$, we have $(a * a) = *^a$, which implies the result. □

This following exercise generalizes the second part of Lemma 6.1 and will be used in Section 10 to prove the upper bound on the growth function of $\mathbb{G}$.

Exercise 6.2. *Check that the stabilizer subgroup* $\mathbb{H}_n := \mathrm{St}_{\mathbb{G}}(n)$ *has finite index in* $\mathbb{G}$: $[\mathbb{G} : \mathbb{H}_n] \le |\,\mathrm{A}_n| = 2^{2^n - 1}$ (see Exercise 3.2).

Let $\psi = \varphi^{-1} : \mathrm{Aut}(\mathbf{T}) \to \big(\mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T})\big) \rtimes \mathbb{Z}_2$ be the isomorphism defined in Section 3. By definition, $\mathbb{H} \subset \mathbb{G} \subset \mathrm{Aut}(\mathbf{T})$.

Lemma 6.3. *The image $\psi(\mathbb{H})$ is a subgroup of $\mathbb{G} \times \mathbb{G}$, such that projection of $\psi(\mathbb{H})$ onto each component is surjective.*

Proof. By definition, $\mathbb{H}$ stabilizes $\mathbf{0}$ and $\mathbf{1}$, so $\psi(\mathbb{H}) \subset \mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T})$. From Exercise 4.2 we have

$$\psi : \begin{cases} b \to (a, c)\,, & b^a \to (c, a)\,, \\ c \to (a, d)\,, & c^a \to (d, a)\,, \\ d \to (\mathtt{1}, b)\,, & d^a \to (b, \mathtt{1})\,. \end{cases}$$

Now Lemma 6.1 implies that $\psi(\mathbb{H}) \subset \mathbb{G} \times \mathbb{G}$. On the other hand, the projection of $\psi(\mathbb{H})$ onto each component contains all four generators $a, b, c, d \in \mathbb{G}$, and is therefore surjective. □

Corollary 6.4. *Group $\mathbb{G}$ is infinite.*

Proof. From Lemma 6.1 and Lemma 6.3 above, we have $\mathbb{H}$ is a proper subgroup of $\mathbb{G}$ which is mapped surjectively onto $\mathbb{G}$. If $|\mathbb{G}| < \infty$, then $|\mathbb{G}| > |\mathbb{H}| \geq |\mathbb{G}|$, a contradiction. □

Here is a different application of Lemma 6.3. Let $G \subset \mathrm{Aut}(\mathbf{T})$ be a subgroup of the group automorphisms of the binary tree $\mathbf{T}$. Denote by $G_v = \mathrm{St}_G(v)|_{\mathbf{T}_v} \subset \mathrm{Aut}(\mathbf{T}_v)$ the subgroup of G of elements which fix vertex $v \in \mathbf{T}$ with the action restricted only to the subtree $\mathbf{T}_v$. We say that G has (strong) *self-similarity property* if $G_v \simeq G$ for all $v \in \mathbf{T}$.

Corollary 6.5. *Group $\mathbb{G}$ has self-similarity property.*

Proof. Use the induction on the level $|v|$. By definition, $\mathbb{G}_{\mathbf{r}} = \mathbb{G}$, and by Lemma 6.3 we have $\mathbb{G}_{\mathbf{0}}, \mathbb{G}_1 \simeq \mathbb{G}$. For general $v \in \mathbf{T}$ we similarly have $\mathbb{G}_{v\mathbf{0}}, \mathbb{G}_{v\mathbf{1}} \simeq \mathbb{G}_v$. This implies the result. □

7. Superpolynomial growth of $\mathbb{G}$

In this section we prove the first half of Theorem 4.1, by showing that the growth function γ of group $\mathbb{G}$ satisfies conditions of the Lower Bound Lemma.

Two groups G_1 and G_2 are called *commeasurable*, denotes $G_1 \approx G_2$, if they contain isomorphic subgroups of finite index:

$$H_1 \subset G_1,\ H_2 \subset G_2,\ \ H_1 \simeq H_2, \ \text{ and } \ [G_1 : H_1],\ [G_2 : H_2] < \infty.$$

For example, group $\mathbb{Z}$ is commeasurable with the infinite dihedral group $\mathrm{D}_\infty \simeq \mathbb{Z} \rtimes \mathbb{Z}_2$. Of course, all finite groups are commeasurable to each other. Another example is $\mathbb{H} \approx \mathbb{G}$, since $\mathbb{H}$ is a subgroup of finite index in $\mathbb{G}$. Note also that commeasurability is an equivalence relation.

Proposition 7.1. *Groups $\mathbb{G}$ and $\mathbb{G} \times \mathbb{G}$ are commeasurable: $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$.*

Proposition 7.1 describes an important phenomenon which can be formalized as follows. The group G is called *multilateral* if G is infinite and $G \approx G^m$ for some $m \geq 2$. As we show below, all such groups have superpolynomial growth.

To prove the proposition, consider the subgroups $\mathbb{H} \subset \mathbb{G}$ and $\widetilde{\mathbb{H}} := \psi(\mathbb{H}) \subset \mathbb{G} \times \mathbb{G}$. By Lemma 6.1 we have $[\mathbb{G} : \mathbb{H}] < \infty$. Since ψ is a group isomorphism, we also have $\widetilde{\mathbb{H}} \simeq \mathbb{H}$. If we show that $[\mathbb{G} \times \mathbb{G} : \widetilde{\mathbb{H}}] < \infty$, then $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$, as claimed in Proposition 7.1.

Denote by $\mathbb{B} = \langle b \rangle^G$ the normal closure of $b \in \mathbb{G}$, defined as $\mathbb{B} := \langle g^{-1}bg \mid g \in \mathbb{G} \rangle$.

Lemma 7.2. *Subgroup $\mathbb{B}$ has a finite index in $\mathbb{G}$. More precisely,* $[\mathbb{G} : \mathbb{B}] \leq 8$.

Proof. By Exercise 4.4, we have $a^2 = d^2 = (ad)^4 = \mathtt{1}$. It is easy to see now that the 2-generated subgroup $\langle a, d \rangle \subset \mathbb{G}$ is a dihedral group D_4 of order 8. By Exercise 4.3, we have $\mathbb{G} = \langle a, b, d \rangle$. Therefore, $\mathbb{G}/\mathbb{B}$ is a quotient of $\langle a, d \rangle$, and $[\mathbb{G} : \mathbb{B}] \leq |D_4| = 8$. □

Lemma 7.3. *Subgroup $\widetilde{\mathbb{H}} = \psi(\mathbb{H})$ contains $\mathbb{B} \times \mathbb{B} \subset \mathbb{G} \times \mathbb{G}$.*

Proof. By Lemma 6.1, we know that $\widetilde{\mathbb{H}} \supset \langle \psi(d), \psi(d^a) \rangle = \langle (1, b), (b, 1) \rangle$. Let $x \in \mathbb{H}$ and $\psi(x) = (x_0, x_1)$. We have:

$$\begin{aligned}\psi(d^x) \, &= \, \psi(x^{-1}dx) \, = \, \psi(x^{-1})\, \psi(d)\, \psi(x) \, = \, (x_0^{-1}, x_1^{-1})\, (\mathtt{1}, b)\, (x_0, x_1) \\ &= \, (\mathtt{1}, x_1^{-1}bx_1) \, = \, (\mathtt{1}, b^{x_1}).\end{aligned}$$

By Lemma 6.3, here we can take any element $x_1 \in \mathbb{G}$. Therefore, the image $\psi(\mathbb{H})$ contains all elements of the form $(\mathtt{1}, b^g)$, $g \in \mathbb{G}$. By definition, these elements generate a subgroup $1 \times \mathbb{B}$. In other words, $\widetilde{\mathbb{H}} = \psi(\mathbb{H}) \supset 1 \times \mathbb{B}$. Similarly, by conjugating the element d^a we obtain $\widetilde{\mathbb{H}} \supset \mathbb{B} \times 1$. Therefore, $\widetilde{\mathbb{H}} \supset \mathbb{B} \times \mathbb{B}$, as desired. □

Now Proposition 7.1 follows immediately once we note that $\mathbb{B} \times \mathbb{B} \subset \widetilde{\mathbb{H}} \subset \mathbb{G} \times \mathbb{G}$, and by Lemma 7.2 the index

$$[\mathbb{G} \times \mathbb{G} : \widetilde{\mathbb{H}}] \, \leq \, [\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}] \, = \, [\mathbb{G} : \mathbb{B}]^2 \, = \, 64.$$

Since $\mathbb{G}$ is infinite (Corollary 6.4) this implies that group $\mathbb{G}$ is multilateral. □

Lemma 7.4. *Every multilateral group G has superpolynomial growth. Moreover, the growth function $\gamma_G(n) \succcurlyeq \exp(n^\alpha)$ for some $\alpha > 0$.*

Proof. By definition, G is infinite, and $G \approx G^m$ for some $m > 1$. In other words, there exist $H \subset G$, $\widetilde{H} \subset G^m$ such that $H \simeq \widetilde{H}$ and $[G : H], [G^m : \widetilde{H}] < \infty$. From Exercise 1.5 we obtain $\gamma_G \sim \gamma_H \sim \gamma_{\widetilde{H}} \sim \gamma_{G^m}$. Thus $\gamma_G \succcurlyeq \gamma_{G^m}$, and the Lower Bound (Lemma 2.1) implies the result. □

Now Proposition 7.1 and Lemma 7.4 immediately imply the first part of Theorem 4.1:

Corollary 7.5. *Group $\mathbb{G}$ has superpolynomial growth. Moreover, the growth function $\gamma_{\mathbb{G}}(n) \succcurlyeq \exp(n^\alpha)$ for some $\alpha > 0$.*

8. Length of elements and rewriting rules

To prove the second half of Theorem 4.1 we derive sharp upper bounds on the growth function $\gamma = \gamma_{\mathbb{G}}^{S}$ of the group $\mathbb{G}$ with the generating set $S = \{a, b, c, d\}$. In this section we obtain some recursive bounds on the length $\ell(g) = \ell_{\mathbb{G}}^{S}(g)$ of elements $g \in \mathbb{G}$ in terms of S. Note that although $\mathbb{G}$ is 3-generated, having the fourth generator is convenient for technical reasons.

We begin with a simple classification of reduced decompositions of elements of $\mathbb{G}$ following the approach in the proof of Lemma 6.1. We define four *types* of reduced decompositions:

(i) if $g = a * a * a \cdots * a * a$,
(ii) if $g = a * a * a \cdots * a *$,
(iii) if $g = * a * a * \cdots a * a$,
(iv) if $g = * a * a * \cdots a * a *$.

Of course, element g can have many different reduced decompositions. On the other hand, the type of a decomposition is almost completely determined by g.

Lemma 8.1. *Every group element $g \in \mathbb{G}$ has all of its reduced decompositions of the same type* (i)*, or of type* (iv)*, or of type* (ii) *and* (iii)*.*

Proof. Recall that the number of a's in a reduced decomposition of $g \in \mathbb{G}$ is even if $g \in \mathbb{H}$, and is odd otherwise. Thus g cannot have decompositions of type (i) and (iv) at the same time. Noting that decompositions of type (i) and (iv) have odd length while those of type (ii) and (iii) have even length implies the result. □

It is easy to see that one cannot strengthen Lemma 8.1 since some elements can have decompositions of both type (ii) and (iii). For example, $adad = dada$ by Exercise 4.3, and both are reduced decompositions. From this point on we refer to elements $g \in \mathbb{G}$ as of *type* (i), (ii/iii), or (iv) depending on the type of their reduced decompositions.

For the next lemma recall the isomorphism $\psi = \varphi^{-1} : \mathrm{Aut}(\mathbf{T}) \to \mathrm{Aut}(\mathbf{T}) \wr S_2$, where $S_2 = \{\mathtt{1}, a\} \simeq \mathbb{Z}_2$.

Lemma 8.2. *Let $\ell(g)$ be the length of $g \in \mathbb{G}$ in generators $S = \{a, b, c, d\}$. Suppose $\psi(g) = (g_0, g_1; \sigma)$, where $g_0, g_1 \in \mathbb{G}$ and $\sigma \in S_2$. Then:*

$\ell(g_0), \ell(g_1) \le \frac{1}{2}(\ell(g) - 1)$ *if g has type* (i)*,*
$\ell(g_0), \ell(g_1) \le \frac{1}{2}\,\ell(g)$ *if g has type* (ii/iii)*,*
$\ell(g_0), \ell(g_1) \le \frac{1}{2}(\ell(g) + 1)$ *if g has type* (iv)*.*

Proof. Fix an element $g \in \mathbb{G}$, and let g_0, g_1, σ be as in the lemma. Recall that $\sigma = \mathtt{1}$ if $g \in \mathbb{H}$ and $\sigma = a$ otherwise (see the proof of Lemma 6.1). For every reduced decomposition $w = (a) * a * a \cdots * a * (a)$ of g we shall construct decompositions of elements g_0, g_1 with lengths as in the lemma. As before, we use $*$ to denote either of the generators b, c, d. Also, for every $*$ in a reduced decomposition denote by $\pi(*)$ the number of a's preceding $*$.

Consider the following *rewriting rules*:

$$\Phi_0 : \qquad \begin{cases} a \to \mathtt{I}, & \\ b \to a, \quad c \to a, \quad d \to \mathtt{I} & \text{if} \quad \pi(*) \quad \text{is odd}, \\ b \to c, \quad c \to d, \quad d \to b & \text{if} \quad \pi(*) \quad \text{is even}, \end{cases}$$

and

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

These rules act on words w in generators S, and substitute each occurrence of a letter with the corresponding letter or $\mathtt{I}$.

Let $\Phi_0(w)$, $\Phi_1(w)$ be the words obtained from the word $w = (a) * a \cdots a * (a)$ by the rewriting rules as above, and let $g_0', g_1' \in \mathbb{G}$ be group elements defined by these products. Check by induction on the length $\ell(g)$ that $\psi(g) = (g_0', g_1'; \sigma)$. Indeed, note that the rules give the first and second components in the formula for ψ in the proof of Lemma 6.3. Now, as in the proof of Lemma 6.1 subdivide the product w into elements (a) and $(* \, a *)$, and obtain the induction step. From here we have $g_0 = g_0'$, $g_1 = g_1'$, and by construction of rewriting rules the lengths of g_0, g_1 are as in the lemma. □

As we show below, the rewriting rules are very useful in the study of group $\mathbb{G}$, but also in a more general setting.

Corollary 8.3. *In conditions of Lemma 8.2 we have:* $\ell(g_0) + \ell(g_1) \le \ell(g) + 1$.

The above corollary is not tight and can be improved in certain cases. The following exercise give bounds in the other direction, limiting potential extensions of Corollary 8.3.

Exercise 8.4. *In conditions of Lemma 8.2 we have:* $\ell(g) \le 2\ell(g_0) + 2\ell(g_1) + 50$.

This result can be used to show that $\gamma_{\mathbb{G}} \succcurlyeq \exp(\sqrt{n})$. The proof is more involved that of other exercises; it will not be used in this paper.

9. Word problem

The classical *word problem* can be formulated as follows: given a word $w = s_{i_1} \cdots s_{i_n}$ in generators $s_j \in S$, decide whether this product is equal to $\mathtt{I}$ in $G = \langle S \rangle$. To set up the problem carefully one would have to describe presentation of the group and allowed operations [7]. We skip these technicalities in hope that the reader has an intuitive understanding of the problem.

Now, from the algorithmic point of view the problem is undecidable, i.e. there is no Turing machine which can resolve it in finite time for every group. On the other hand, for certain groups the problem can be solved very efficiently, in time polynomial in the length n of the product. For example, in the *free group* $F_k = \langle x_1^{\pm 1}, \ldots, x_k^{\pm 1} \rangle$ the problem can be solved in linear time: take a product w and repeatedly cancel every occurrence of $x_i x_i^{-1}$ and $x_i^{-1} x_i$, $1 \le i \le k$; the product $w = \mathtt{I}$ if and only if the resulting word is empty. Since every letter is cancelled at most once and new letters are not created, the algorithm takes $O(n)$ time.

The class of groups where word problem can be solved in linear time is called *word hyperbolic*; it has a simple description and many group theoretic applications. The following result shows that word problem can be resolved in $\mathbb{G}$ in nearly linear time[1].

Theorem 9.1. *Word problem in* $\mathbb{G}$ *can be solved in* $O(n \log n)$ *time.*

Proof. Consider the following algorithm. First, cancel products of b, c, d to write the word as $w = (a) * a * \cdots * a * (a)$. If the number $\pi(w)$ of a's is odd, then the product $w \neq_{\mathbb{G}} \mathtt{I}$. If the $\pi(w)$ is even, use the rewriting rules (proof of Lemma 8.2) to obtain words $w_0 = \Phi_0(w)$ and $w_1 = \Phi_1(w)$. Recall that the product $w =_{\mathbb{G}} \mathtt{I}$ if and only if $w_0, w_1 =_{\mathbb{G}} \mathtt{I}$. Now repeat the procedure for the words w_0, w_1 to obtain words $w_{00}, w_{01}, w_{10}, w_{11}$, etc. Check that $w =_{\mathbb{G}} \mathtt{I}$ if and only if eventually all the obtained words are trivial.

Observe that the length of each word w_i is at most $(n+1)/2$. Iterating this bound, we conclude that the number of 'rounds' in the algorithm of constructing smaller and smaller words is $O(\log n)$. Therefore, each letter is replaced at most $O(\log n)$ times and thus the algorithm finishes in $O(n \log n)$ time. □

Remark 9.2. For every reduced decomposition as above one can construct a binary tree of nontrivial words $w_{i_1 i_2 \ldots i_r}$. The distribution of *height* and *shape* (profile) of these trees is closely connected to the growth function $\gamma_{\mathbb{G}}$. Exploring this connection is of great interest, but lies outside the scope of this paper.

10. Subexponential growth of $\mathbb{G}$

In this section we prove the second half of Theorem 4.1, proving the upper bound on the growth function γ of group $\mathbb{G}$ with generators $S = \{a, b, c, d\}$. The proof relies on the technical Cancellation Lemma which will be stated here, but proved in the next section.

Let $\mathbb{H}_3 := \mathrm{St}_{\mathbb{G}}(3)$ be the stabilizer of vertices on the third level, and recall that the index $[\mathbb{G} : \mathbb{H}_3] \le 2^7 = 128$ (Exercise 6.2). There is a natural embedding

$$\psi_3 \, : \, \mathbb{H}_3 \longrightarrow \mathbb{G}_{\mathbf{000}} \times \mathbb{G}_{\mathbf{001}} \times \ldots \times \mathbb{G}_{\mathbf{111}}$$

(see Section 6), and by self-similarity each of the eight groups in the product is isomorphic: $\mathbb{G}_{\mathbf{ijk}} \simeq \mathbb{G}$, where $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \{\mathbf{0}, \mathbf{1}\}$. These isomorphisms are obtained by restrictions of natural maps: $\iota_v^{-1} : \mathrm{Aut}(\mathbf{T}_v) \to \mathrm{Aut}(\mathbf{T})$, where $v \in \mathbf{T}$. Now combine ψ_3 with the map $(\iota_{\mathbf{000}}^{-1}, \iota_{\mathbf{001}}^{-1}, \ldots, \iota_{\mathbf{111}}^{-1})$ we obtain a group homomorphism $\chi : \mathbb{H}_3 \to \mathbb{G}^8$ written as $\chi(h) = (g_{000}, g_{001}, \ldots, g_{111})$, where $h \in \mathbb{H}_3$ and $g_{ijk} \in \mathbb{G}$.

It follows easily from Corollary 8.3 that $\ell(g_{000}) + \ell(g_{001}) + \ldots + \ell(g_{111}) \le \ell(h) + 7$. The following result is an improvement over this bound:

[1] In computer science literature *nearly linear time* usually stands for $O(n \log^k n)$, for some fixed k.

Lemma 10.1 (Cancellation Lemma)**.** *Let $h \in \mathbb{H}_3$. In the notation above we have:*

$$\ell(g_{000}) + \ell(g_{001}) + \ldots + \ell(g_{111}) \,\le\, \frac{5}{6}\,\ell(h) + 8.$$

We postpone the proof of Cancellation Lemma till next section. Now we are ready to finish the proof of the Main Theorem.

Proposition 10.2. *Group $\mathbb{G}$ has subexponential growth. Moreover, $\gamma_{\mathbb{G}}(n) \preccurlyeq \exp(n^\nu)$ for some $\nu < 1$.*

Proof. All elements $g \in \mathbb{G}$ can be written as $g = u \cdot h$ where $h \in \mathbb{H}_3$ and u is a coset representative of $\mathbb{G}/\mathbb{H}_3$. Since $[\mathbb{G} : \mathbb{H}_3] \le 128$, there are at most 128 such elements u. Note that we can choose elements u which have length at most 127 in $S = \{a, b, c, d\}$, since all prefixes of a reduced decomposition can be made to lie in distinct cosets. The decomposition $h = u^{-1}g$ then gives $\ell(h) \le \ell(g) + 127$.

Now write $g = u g_{000} g_{001} \cdots g_{111}$. The Cancellation Lemma gives:

$$\sum_{ijk} \ell(g_{ijk}) \,\le\, \frac{5}{6}\,\ell(h) + 8 \,\le\, \frac{5}{6}\,\bigl(\ell(g) + 127\bigr) + 8 \,<\, \frac{5}{6}\,\ell(g) + 114.$$

Putting all this together we conclude:

$$\gamma(n) \,\le\, 128 \sum_{(n_1,\ldots,n_8)} \gamma(n_1) \cdots \gamma(n_8),$$

where the summation is over all integer 8-tuples with $n_1 + \ldots + n_8 \,\le\, \frac{5}{6}n + 114$. Let $m = n + 137$ so that $\frac{5}{6}n + 114 < \frac{5}{6}m$, and note that $\gamma(n + 137) \le \gamma(n) \cdot |S|^{137}$. We have:

$$\gamma(m) \,\le\, 4^{137}\,\gamma(n) \,\le\, (128 \cdot 4^{137})\,\gamma(m)^{\star 8}.$$

Applying the Upper Bound (Lemma 2.2) we obtain the result. □

Recall that subexponential growth of $\mathbb{G}$ is shown in Corollary 7.5. This completes the proof of Theorem 4.1. □

11. Proof of the Cancellation Lemma

Fix a reduced decomposition $(a) *_1 a *_2 a \cdots *_m (a)$ of $h \in \mathbb{H}_3$, and denote this decomposition by w. Apply rewriting rules Φ_0 and Φ_1 to w obtain words w_0 and w_1. Do not make any cancellations except remove all identities $\mathtt{I}$. Then apply these rules again to obtain w_{00}, w_{01}, w_{10} and w_{11}, and cancel the identities $\mathtt{I}$. Finally, repeat this once again to obtain words $w_{000}, w_{001}, \ldots, w_{111}$. Following the proof of Theorem 9.1, all these words give decompositions of elements g_0, g_1, then $g_{00}, \ldots, g_{11}$, and $g_{ijk} \in \mathbb{G}_{\mathbf{ijk}}$, respectively. Note that these decompositions are not necessarily reduced, so for the record:

$$(✠) \quad \ell(g_i) \le |w_i|, \quad \ell(g_{ij}) \le |w_{ij}|, \quad \ell(g_{ijk}) \le |w_{ijk}|, \quad \text{for all } \; i, j, k \in \{0, 1\},$$

where $|u|$ denotes the length of the word u. Also, by Corollary 8.3 we have:

$$\begin{aligned} \ell(g_0) + \ell(g_1) &\le \ell(h) + 1, \\ \ell(g_{00}) + \ldots + \ell(g_{11}) &\le \ell(g_0) + \ell(g_1) + 2, \\ \ell(g_{000}) + \ell(g_{001}) + \ldots + \ell(g_{111}) &\le \ell(g_{00}) + \ldots + \ell(g_{11}) + 4. \end{aligned} \tag{$\diamondsuit$}$$

To simplify the notation, consider the following concatenation of these words:

$$w' = w_0 \cdot w_1, \quad w'' = w_{00} \cdots w_{11}, \quad \text{and} \quad w''' = w_{000} \cdot w_{001} \cdots w_{111}.$$

By construction of the rewriting rules, since the only possible cancellation happens when $d \to \mathtt{I}$ we have: $|w'| \le |w| + 1 - |w|_d$, where $|w|_d$ is the number of letters d in w. Indeed, simply note that each letter d in w is cancelled by either Φ_0 or Φ_1. Unfortunately we cannot iterate this inequality as the words w_i are not reduced. Note on the other hand, that each letter c in w produces one letter d in w' and each of the latter is cancelled again by either Φ_0 or Φ_1. Finally, each letter b in w produces one letter c in w', which in turn produces letter d in w'', and each of the latter is cancelled again by either Φ_0 or Φ_1. Taking into account the types of decompositions we obtain:

$$\begin{aligned} |w'| \ &\le \ |w| + 1 - |w|_d \, , \\ |w''| \ &\le \ |w| + 3 - |w|_c \, , \\ |w'''| \ &\le \ |w| + 7 - |w|_b \, . \end{aligned} \tag{$\heartsuit$}$$

Since $|w|_b + |w|_c + |w|_d \ge (|w| - 1)/2$, at least one of the numbers $|w|_* > |w|/6 - 1$. Combining this with ($\heartsuit$), ($\diamondsuit$), and (✠) we conclude:

$$\begin{aligned} \ell(g_{000}) + \ell(g_{001}) + \ldots + \ell(g_{111}) \ &\le \ \max\bigl\{|w'| + 2 + 4, |w''| + 4, |w'''|\bigr\} \\ \le \ |w| + 7 - \max_{* \in \{b,c,d\}} |w|_* \ &\le \ |w| + 7 - (|w|/6 - 1) \ = \ \frac{5}{6}\,\ell(h) + 8, \end{aligned}$$

as desired. □

12. Further developments, conjectures and open problems

Much about groups of intermediate growth remains open. Below we include only the most interesting results and conjectures which are closely connected to the material presented in this paper. Everywhere below we refer to surveys [1, 2, 6] and a book [7] for details and further references.

Let us start by saying that the Upper and Lower Bound lemmas can be used to obtain effective bounds on the growth function of $\mathbb{G}$. Although considerably sharper bounds are known, the exact asymptotic behavior remain an open problem. Unfortunately, we do not even know whether it makes sense to say that $\gamma_{\mathbb{G}}$ has growth $\exp(n^\alpha)$ for some fixed $\alpha > 0$:

Conjecture 12.1. *Let $\gamma = \gamma_{\mathbb{G}}$ be the growth function of group $\mathbb{G}$. Prove that there exists a limit $\alpha = \lim_{n\to\infty} \log_n \log \gamma(n)$.*

The extend to which results for $\mathbb{G}$ generalize to other groups of intermediate growth remains unclear. Although there are now constructions of groups with subexponential growth function $\gamma(n) \sim e^{n(1-o(1))}$, there are no known examples of groups with superpolynomial growth function $\gamma(n) \sim \exp(n^{o(1)})$. The following result has been established for a large classes of groups, but not in general:

Conjecture 12.2. *Let G be a group of intermediate growth, and let $\gamma_G(n)$ be its growth function. Then $\gamma_S(n) \succcurlyeq \exp(n^\alpha)$ for some $\alpha > 0$.*

Moving away from the bounds on the growth, let us mention that group $\mathbb{G}$ is not finitely presented. Existence of finitely presented groups of intermediate growth is a major open problem in the field, and the answer is believed to be negative:

Conjecture 12.3. *There are no finitely presented groups of intermediate growth.*

Our final conjecture may seem technical and unmotivated as stated. If true it resolves positively Benjamini and Schramm's "$p_c < 1$" conjecture on percolation on Cayley graphs.

Conjecture 12.4. *Every group G of intermediate growth contains two infinite subgroups H_1 and H_2 which commute with each other: $[h_1, h_2] = \mathtt{I}$ for all $h_1 \in H_1$ and $h_2 \in H_2$.*

We refer to [8] for an overview of this conjecture and its relation to groups of intermediate growth.

Acknowledgements. We would like to thank [numerous nice people] for the interest in the subject and engaging discussions [over the years]. The second author was supported by the NSA and the NSF.

References

[1] L. Bartholdi, R. I. Grigorchuk, V. V. Nekrashevych, From fractal groups to fractal sets, in *Fractals in Graz* (P. Grabner, W. Woess, eds.), Birkhaüser, Basel, 2003, 25–118.

[2] L. Bartholdi, R. I. Grigorchuk, Z. Sunik, Branch groups, in *Handbook of Algebra, vol. 3* (ed. M. Hazewinkel), North-Holland, Amsterdam, 2003, 989–1112.

[3] R. I. Grigorchuk, On Burnside's problem on periodic groups, *Funct. Anal. Appl.* **14** (1980), 41–43.

[4] R. I. Grigorchuk, On the Milnor problem of group growth, *Soviet Math. Dokl.* **28** (1983), no. 1, 23–26.

[5] R. I. Grigorchuk, Degrees of growth of finitely generated groups and the theory of invariant means, *Math. USSR-Izv.* **25** (1985), 259–300.

[6] R. I. Grigorchuk, V. V. Nekrashevych, V. I. Sushchanskiĭ, Automata, dynamical systems, and groups, *Proc. Steklov Inst. Math.* **231** (2000), 128–203.

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

[8] R. Muchnik, I. Pak, Percolation on Grigorchuk groups, *Comm. Algebra* **29** (2001), 661–671.

[9] R. Muchnik, I. Pak, On growth of Grigorchuk groups, *Int. J. Algebra Comp.* **11** (2001), 1–17.

13. Appendix

Proof of the Lower Bound Lemma. To simplify the notation, let us extend definition of f to the whole line $f : \mathbb{R}_+ \to \mathbb{R}_+$ by setting $f(x) := f(\lfloor x \rfloor)$. Let $\pi(n) = \ln f(n)$. Clearly, $\pi(n)$ is monotone increasing, and $\pi(n) \to \infty$ as $n \to \infty$. By definition, condition $f \succcurlyeq f^m$ gives $f(n) \geq C\, f^m(\alpha n)$ for some $C, \alpha > 0$. Write this as

$$(\divideontimes) \qquad \pi(n) \, \geq \, c \, + \, m\, \pi(\alpha n)\,,$$

where $c = \log C$. Let us first show that $\alpha < 1$. Indeed, if $\alpha \geq 1$, we have:

$$(\divideontimes\divideontimes) \quad m\, \pi(\alpha n) \, - \, \pi(n) \, > \, m\, \pi(n) \, - \, \pi(n) \, = \, (m-1)\, \pi(n) \, \to \, \infty \ \text{ as } \ n \to \infty.$$

On the other hand, $(\divideontimes)$ implies that the l.h.s. of $(\divideontimes\divideontimes)$ is $\leq -c$, a contradiction.

Applying $(\divideontimes)$ repeatedly to itself gives us:

$$\begin{aligned} \pi(n) \, &\geq \, c + m\pi(\alpha n) \, \geq \, c + m(c + m\pi(\alpha n)) \, \geq \, \ldots \\ &\geq \, m^k \pi(\alpha^k n) + c(1 + m + \ldots + m^{k-1}). \end{aligned}$$

Suppose $c \geq 0$. Take $k = \lfloor (\log n - 1)/\log 1/\alpha \rfloor$. Then $\pi(\alpha^k n) \geq \log(\alpha^k n) \geq 1$ and $\pi(n) \, \geq \, m^k \, \geq An^\nu$, where $m^{1/\log \alpha} \geq A \geq m^{(1/\log \alpha)-1}$ and $\nu = (\log m)/(\log 1/\alpha) > 0$.

Suppose now $c < 0$ and recall that $m \geq 2$. Then $\pi(n) \geq m^k\big(\pi(\alpha^k n) + c\big)$. Take $k = \lfloor (\log n + c - 1)/\log 1/\alpha \rfloor$. Then $\pi(\alpha^k n) + c \geq \log(\alpha^k n) + c \geq 1$, and $\pi(n) \geq m^k \geq An^\nu$, where $m^{-(c-1)/\log \alpha} \geq A \geq m^{-1-(c-1)/\log \alpha}$ and ν as above.

Therefore, in both cases we have $f(n) = \exp \pi(n) \geq \exp(An^\nu)$ for some $A, \nu > 0$, as desired. □

Proof of the Upper Bound Lemma. We prove the result by induction on n. Suppose $\pi(n) := \log f(m) \leq An^\nu$. We have:

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

where the summation is over all $n_1 + \ldots + n_k \leq \alpha n$. Clearly, the number of terms of the summation is at most $(\alpha n)^k$. Also, for each product in the summation we have by induction:

$$\begin{aligned} \log\big(f(n_1)\cdots f(n_k)\big) \, &\leq \, \pi(n_1) + \ldots + \pi(n_k) \, \leq \, A(n_1^\nu + \ldots + n_k^\nu) \\ &\leq \, Ak(\alpha n/k)^\nu \, \leq \, An^\nu \cdot \left[k\left(\frac{\alpha}{k}\right)^\nu\right] \, = \, An^\nu \cdot (1-\varepsilon), \end{aligned}$$

where $\varepsilon = \varepsilon(k,\alpha) > 0$, and where $\nu < 1$ is large enough. Therefore,

$$(\diamond) \quad \begin{aligned} \pi(n) \, &= \, \log f(n) \, \leq \, \log C + \log(\alpha n)^k + An^\nu \cdot (1-\varepsilon) \\ &\leq \, (\log C + k\log\alpha + k\log n) + An^\nu \cdot (1-\varepsilon) \, \leq \, An^\nu \end{aligned}$$

for A large enough. Setting A large enough to satisfy $(\diamond)$ and the base of induction, we obtain the result. □