Groups of Intermediate Growth, an Introduction

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

Igor Pak
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
pak@math.umn.edu

April 4, 2008

Introduction

The study of growth of groups has a long and remarkable history spanning over much of the twentieth century, and goes back to Hilbert, Poincarè, Ahlfors, 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 [8] for further results and references. The proof ideas in the paper follow [5], the paper has the same structure as [9], but the presentation and details are mostly new.

The paper is structured as follows. We start with some background information on the growth of groups (Section 1) and technical results for bounding the growth function (sections 2 and 3). In Section 4 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 5, while the remaining sections 6–11 prove the intermediate growth of $\mathbb{G}$ and one 'bonus' theorem. We conclude with few final remarks (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 $\mathtt{I}$ 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 finite 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, $\gamma(n) \le \sum_{i=0}^{n} (2k)^i \le (2k+1)^n$.

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 $n \ge 0$.*

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 finite 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

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

For example, n^π is polynomial, while n^n and $n^{\log\log n}$ are superpolynomial.

Similarly, a function f is called *exponential* if $f(n) \sim e^n$. A function f is called *subexponential* if

$$\lim_{n\to\infty} \frac{\ln \gamma(n)}{n} = 0.$$

For example, $n^e e^n$ and $\exp\bigl(\frac{n}{2} - \sqrt{n}\,\log^2 n\bigr)$ are exponential, $e^{n/\log n}$ and n^π are subexponential, while n^n is neither.

Let us note also that there are functions which cannot be categorized. For example, $\exp\bigl(n^{\sin n}\bigr)$ fluctuates between 1 and e^n, so it is neither polynomial nor superpolynomial, neither exponential nor subexponential.

Finally, a function 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, and $\gamma_G \sim \gamma_{G^m}$.*

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 finite 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 exists. This limit is called the growth rate *of G. Deduce from here that every group G has either exponential or subexponential growth.*

2. The Lower Bound Lemma

In the next two section we present two technical results that are key in our analysis of the growth of finitely generated groups. Their proofs are based on elementary albeit delicate analytic arguments and have no group theoretic content.

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 $\alpha > 0$.*

Proof. To simplify the notation, let us extend definition of f to the whole line $f : \mathbb{R}_+ \to \mathbb{R}_+$ by setting $f(x) := f(\lfloor x \rfloor)$. Without loss of generality we can assume that $f(1) \geq 3$, since otherwise we can multiply all values of f by a large enough constant. Similarly, we can assume that $m \geq 2$ since $f \succcurlyeq f^m \succcurlyeq f^{m^2} \succcurlyeq f^{m^3} \succcurlyeq \ldots$ which gives $f \succcurlyeq f^2$.

Let $\pi(n) = \log f(n)$, where here and everywhere below log denotes the natural logarithm. Clearly, $\pi(n)$ is monotone increasing, $\pi(1) > 1$, and $\pi(n) \to \infty$ as $n \to \infty$. We need to show that $\pi(n) \geq A n^\nu$ for some $A, \nu > 0$.

By definition, condition $f \succcurlyeq f^m$ gives $f(n) \geq C\, f^m(\alpha n)$ for some $C, \alpha > 0$. Write this as

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

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

$$(\circledast\circledast) \quad m\,\pi(\alpha n) \,-\, \pi(n) \,\geq\, m\,\pi(n) \,-\, \pi(n) \,=\, (m-1)\,\pi(n) \,\to\, \infty \;\text{ as }\; n \to \infty,$$

since $m > 1$. On the other hand, $(\circledast)$ implies that the l.h.s. of $(\circledast\circledast)$ is $\leq -c$, a contradiction.

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

$$(\div) \qquad \begin{aligned} \pi(n) \,&\geq\, m\pi(\alpha n) + c \,\geq\, m(m\pi(\alpha n) + c) \,+\, c \,=\, m^2\pi(\alpha n) \,+\, c(1+m) \\ &\geq\, \ldots \,\geq\, m^k\pi(\alpha^k n) + c(1+m+\ldots+m^{k-1}). \end{aligned}$$

Suppose $c \geq 0$. Take $k = \lfloor \log_{\frac{1}{\alpha}} n \rfloor$. Then $\alpha^k \geq \frac{1}{n}$, $\pi(\alpha^k n) \geq \pi(1) > 1$, and from inequality $(\div)$ we have $\pi(n) \geq m^k$. On the other hand, $m^k = (\frac{1}{\alpha})^{\nu k} \geq An^\nu$, where $\nu = \log_{\frac{1}{\alpha}} m > 0$ and $A = m^{-(1+\log\frac{1}{\alpha})} > 0$. That proves the result in this special case.

Suppose now $c < 0$. Since $m \geq 2$ by assumption, we have $(1+m+m^2+\ldots+m^{k-1}) < m^k$, and the above equation can be written as $\pi(n) > m^k\big(\pi(\alpha^k n) + c\big)$. Take the smallest integer $s \geq 1$ such that $\pi(s) > 1-c$. Clearly, s is a constant independent of n. Take $k = \lfloor \log_{\frac{1}{\alpha}} \frac{n}{s} \rfloor$, so that $\alpha^k n \geq s$ and $\pi(\alpha^k n) + c \geq \pi(s) + c \geq 1$. From above, we conclude $\pi(n) \geq m^k\big(\pi(\alpha^k n)+c\big) \geq m^k$. On the other hand, $m^k = (\frac{1}{\alpha})^{\nu k} \geq (A/s^\nu)n^\nu$, where ν and A are as above. This completes the proof. $\square$

3. The Upper Bound Lemma

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 3.1 (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 $\beta < 1$.*

Note that the functions f^k and $f^{\star k}$ are strongly related:

$$f^k\left(\left\lfloor \frac{n}{k} \right\rfloor\right) \leq f^{\star k}(n) \leq n^k f^k(n)$$

However, to analyze the growth we need the lemma in this particular form.

Proof. We prove the result by induction on n. Suppose $\pi(n) := \log f(m) \leq An^\nu$. Note that we can always choose A large enough to satisfy the base of induction. We have:

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

where the summation is over all $n_1 + \ldots + n_k \le \alpha n$. Clearly, the number of terms of the summation is at most $(\alpha n)^k$. Using the inductive assumption or each product in the summation and the Cauchy-Schwartz inequality we obtain:

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

where $\varepsilon = 1 - \left[k\,\left(\frac{\alpha}{k}\right)^\nu\right] > 0$, for $\nu < 1$ large enough. From here and ($\bigstar$) we conclude:

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

for A large enough. In summary, recall that C, α and k are universal constants. Take $\nu < 1$ large enough to satisfy ($\Bumpeq$) with $\varepsilon > 0$. Now that ε is fixed, take A large enough to satisfy ($\diamond$). This completes the step of induction and finishes the proof. $\square$

4. Group of 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 $\mathbf{T}$, denoted $\mathbf{r}$, corresponds to the empty word $\varnothing$. Orient all edges in the tree $\mathbf{T}$ away from the root. We denote by E the set of all (oriented) edges in $\mathbf{T}$. 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 the vertex v; we call it the *level* of v. Finally, denote by $\mathbf{T}_v$ the subtree of $\mathbf{T}$ rooted in $v \in V$. Clearly, $\mathbf{T}_v$ is isomorphic to $\mathbf{T}$.

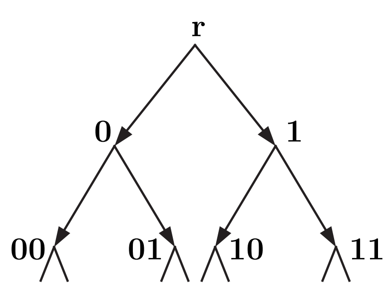

Figure 1. Infinite binary tree $\mathbf{T}$.

The main subject of this section is the group $\mathrm{Aut}(\mathbf{T})$ of automorphisms of $\mathbf{T}$, i.e. the group of bijections $\tau : V \to V$ which map edges into edges. Note that the root $\mathbf{r}$ is always a fixed point of τ. In other words, $\tau(\mathbf{r}) = \mathbf{r}$ for all $\tau \in \mathrm{Aut}(\mathbf{T})$. More generally, all automorphisms $\tau \in \mathrm{Aut}(\mathbf{T})$ preserve the level of vertices: $|\tau(v)| = |v|$, for all $v \in V$. Denote by $\mathtt{I} \in \mathrm{Aut}(\mathbf{T})$ the 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. Let a be an automorphism which maps $\mathbf{T_0}$ into $\mathbf{T_1}$ and preserves the natural order on vertices:

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

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

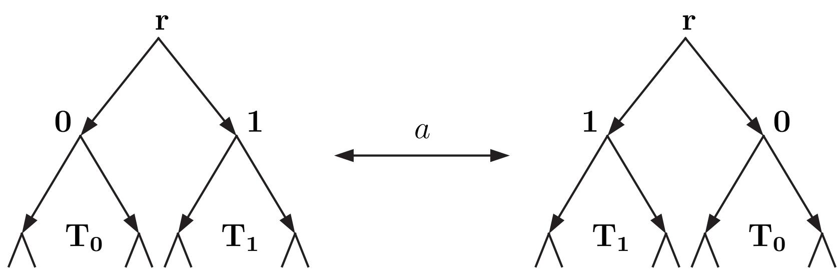

FIGURE 2. Automorphism $a \in \mathrm{Aut}(\mathbf{T})$.

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

More generally, denote by $\mathrm{Aut}(\mathbf{T}_v)$ the subgroup of automorphisms in $\mathrm{Aut}(\mathbf{T})$ which preserve the subtree $\mathbf{T}_v$ and are trivial on the outside of $\mathbf{T}_v$. There is a natural graph isomorphism $\iota_v : \mathbf{T} \to \mathbf{T}_v$ and a corresponding 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 the vertex v into two edges leaving the vertex $\tau(v)$. Thus we can define the *sign* $\epsilon_v(\tau) \in \{0, 1\}$ as follows:

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

In other words, $\epsilon_v(\tau)$ is equal to 0 if the automorphism maps the left edge leaving the 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 signs $\{\epsilon_v(\tau), v \in \mathbf{T}\}$ can take all possible 0–1 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 the 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, the automorphism τ is shown in Figure 3.

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

Proposition 4.1. $\mathrm{Aut}(\mathbf{T}) \simeq \mathrm{Aut}(\mathbf{T}) \wr \mathbb{Z}_2$.

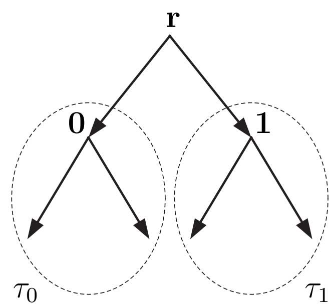

FIGURE 3. Automorphism $\tau = \varphi(\tau_0, \tau_1) \in \mathrm{Aut}(\mathbf{T})$.

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 $a \in \mathrm{Aut}(\mathbf{T})$ 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. $\square$

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

Exercise 4.2. *Let* $\mathrm{A}_m \subset \mathrm{Aut}(\mathbf{T})$ *be a subgroup of all automorphisms* $\tau \in \mathrm{Aut}(\mathbf{T})$ *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 4.3. *Consider the unique tree automorphism* $\tau \in \mathrm{Aut}(\mathbf{T})$ *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* $\mathrm{Aut}(\mathbf{T})$.
Hint: Consider elements $\tau_m \in \mathrm{A}_m$ with signs as in the definition of above, and $k < m$. Show that the order $\mathrm{ord}(\tau_m) \to \infty$ as $m \to \infty$, and deduce the result from here.

5. THE FIRST CONSTRUCTION

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

Let us first define the group $\mathbb{G}$ by defining recursively a set of generators. More precisely, set $\mathbb{G} = \langle a, b, c, d \rangle \subset \mathrm{Aut}(\mathbf{T})$, where a is the automorphism defined as in Section 4, and automorphisms b, c and d are defined recursively by the following equations:

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

Observe that the automorphisms b, c, and d are defined through each other. Since the generator d is acting as the 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 $b, c, d \in \mathrm{Aut}(\mathbf{T})$.

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

$$(*) \qquad \begin{aligned} b &:= (a_{\mathbf{0}} \cdot a_{\mathbf{1}^3\mathbf{0}} \cdot a_{\mathbf{1}^6\mathbf{0}} \cdot \ldots)\,(a_{\mathbf{10}} \cdot a_{\mathbf{1}^4\mathbf{0}} \cdot a_{\mathbf{1}^7\mathbf{0}} \cdot \ldots), \\ c &:= (a_{\mathbf{0}} \cdot a_{\mathbf{1}^3\mathbf{0}} \cdot a_{\mathbf{1}^6\mathbf{0}} \cdot \ldots)\,(a_{\mathbf{1}^2\mathbf{0}} \cdot a_{\mathbf{1}^5\mathbf{0}} \cdot a_{\mathbf{1}^8\mathbf{0}} \cdot \ldots), \\ d &:= (a_{\mathbf{10}} \cdot a_{\mathbf{1}^4\mathbf{0}} \cdot a_{\mathbf{1}^7\mathbf{0}} \cdot \ldots)(a_{\mathbf{1}^2\mathbf{0}} \cdot a_{\mathbf{1}^5\mathbf{0}} \cdot a_{\mathbf{1}^8\mathbf{0}} \cdot \ldots), \end{aligned}$$

where $\mathbf{1}^m$ is short for $\mathbf{1}\ldots\mathbf{1}$ (m times). Note that the automorphisms $a_{\mathbf{1}^m\mathbf{0}}$ used in $(*)$ commute with each other, and thus elements $b, c, d \in \mathrm{Aut}(\mathbf{T})$ are well defined.

Elements $b, c, d \in \mathrm{Aut}(\mathbf{T})$ are graphically shown in Figure 4. Here black triangles in vertices of trees represent the subtrees swaps.

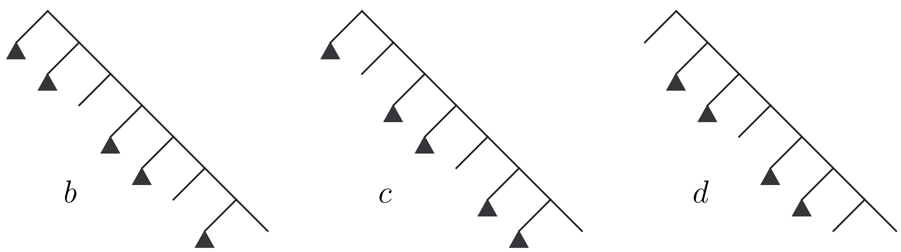

FIGURE 4. Elements b, c and $d \in \mathrm{Aut}(\mathbf{T})$.

Theorem 5.1 (Main Theorem)**.** *Group $\mathbb{G} = \langle a, b, c, d\rangle$ has intermediate growth.*

The proof of Theorem 5.1 is quite involved and occupies much of the rest of the paper.

Exercise 5.2. *Check that the elements $b, c, d \in \mathrm{Aut}(\mathbf{T})$ defined by $(*)$ satisfy conditions $(\circ)$.*

Exercise 5.3. *Check that elements $b, c,$ and d are involutions (have order 2), commute with each other, and satisfy $b \cdot c \cdot d = \mathtt{I}$. 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 5.4. *Check the following relations in $\mathbb{G}$: $(ad)^4 = (ac)^8 = (ab)^{16} = \mathtt{I}$. Deduce from this that the 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.

6. The 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 the 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 5.3 we conclude that every reduced decomposition w 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 4.2).

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 4. 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 5.2 we have

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

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. □

Proposition 6.4. *The 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 $|\mathbb{G}| > |\mathbb{H}| \ge |\mathbb{G}|$, 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 $v \in \mathbf{T}$.

Proposition 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 any $v \in \mathbf{T}$, we similarly have $\mathbb{G}_{v\mathbf{0}}, \mathbb{G}_{v\mathbf{1}} \simeq \mathbb{G}_v$. This implies the result. $\square$

Exercise 6.6. *Consider the following rewriting rules:*

$$\eta : \ a \to aba, \quad b \to d, \quad c \to b, \quad d \to c$$

Define a sequence of elements in $\mathbb{G}$: $x_1 = a$ and $x_{i+1} := \eta(x_i)$ for all $i \geq 1$. Prove directly that all these elements are distinct. Conclude from here that $\mathbb{G}$ is infinite.

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

In this section we prove the first half of Theorem 5.1, 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 *commensurable*, denoted $G_1 \approx G_2$, 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 commensurable with the infinite dihedral group $\mathrm{D}_\infty \simeq \mathbb{Z} \rtimes \mathbb{Z}_2$. Of course, all finite groups are commensurable 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 commensurable: $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$.*

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. *The subgroup $\mathbb{B}$ has finite index in $\mathbb{G}$. More precisely, $[\mathbb{G} : \mathbb{B}] \leq 8$.*

Proof. By Exercise 5.4, 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 5.3, we have $\mathbb{G} = \langle a, b, d \rangle$. Therefore, $\mathbb{G}/\mathbb{B}$ is a quotient of $\langle a, d \rangle$, and $[\mathbb{G} : \mathbb{B}] \leq |D_4| = 8$. $\square$

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:

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

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 $(\mathtt{I}, b^g)$, $g \in \mathbb{G}$. 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, using the element d^a in place of d, we obtain $\widetilde{\mathbb{H}} \supset \mathbb{B} \times 1$. Therefore, $\widetilde{\mathbb{H}} \supset \mathbb{B} \times \mathbb{B}$, as desired. $\square$

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

$$[\mathbb{G} \times \mathbb{G} : \widetilde{\mathbb{H}}] \, \leq \, [\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}] \, = \, [\mathbb{G} : \mathbb{B}]^2 \, \leq \, 8^2 \, = \, 64.$$

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

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. $\square$

Now Proposition 7.1 and Lemma 7.4 immediately imply the first part of Theorem 5.1:

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 5.1 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. $\square$

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 5.3, 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.

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

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 Lemma. We have $\sigma = \mathtt{I}$ 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*:

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

and

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

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 the 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 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.

Exercise 8.5. *Prove that every element $g \in \mathbb{G}$ has order 2^k, for some integer k.* Hint: *use induction to reduce the problem to elements g_0, g_1 (cf. Lemma 8.2).*

9. The 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 $\mathtt{1}$ in $G = \langle S \rangle$. To set up the problem carefully one would have to describe presentation of the group and allowed operations [8]. We skip these technicalities in the 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 $w = \mathtt{1}$ 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 $O(n)$ cancellations.

Exercise 9.1. *By the construction, at every iteration there is a search for the next cancellation, increasing the complexity of the algorithm to as much as $O(n^2)$. Modify the algorithm to show that word problem in F_k can in fact be solved in linear time.*

The class of groups where the word problem can be solved in linear number of cancellations is called *word hyperbolic*. This class has a simple description and many group theoretic applications [7]. The following result shows that word problem can be resolved in $\mathbb{G}$ in nearly linear time[1].

Theorem 9.2. *The word problem in $\mathbb{G}$ can be solved in $O(n \log n)$ time.*

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

Proof. Consider the following algorithm. First, cancel products of b, c, d to write the word as $w = (a) * a * \cdots * a * (a)$. If 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 $w_1 = \Phi_1(w)$ (which may no longer by reducible). 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 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. $\square$

Remark 9.3. 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 5.1 by establishing 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 and 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 $[\mathbb{G} : \mathbb{H}_3] \leq 2^7 = 128$ (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). By self-similarity, the eight groups in the product are 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 $(\iota_{\mathbf{000}}^{-1}, \iota_{\mathbf{001}}^{-1}, \ldots, \iota_{\mathbf{111}}^{-1})$ to obtain a group homomorphism $\chi : \mathbb{H}_3 \to \mathbb{G}^8$, which we write 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 $\ell(g_{000}) + \ell(g_{001}) + \ldots + \ell(g_{111}) \leq \ell(h) + 7$. The following result is an improvement over this bound:

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

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

We postpone the proof of Cancellation Lemma till next Section. Now we are ready to finish the proof of 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 $[\mathbb{G} : \mathbb{H}_3] \leq 128$, 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 $g = uh = ug_{000}g_{001}\cdots g_{111}$. 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 $n_1 + \ldots + n_8 \;\le\; \frac{5}{6}n + 114$. Set $m = n + 137$ so that $\frac{5}{6}n + 114 < \frac{5}{6}m$. Now note that

$$\gamma(m) \;=\; \gamma(n + 137) \;\le\; \gamma(n)\cdot|S|^{137} \;=\; 4^{137}\,\gamma(n).$$

Therefore, we have:

$$\gamma(m) \;\le\; 4^{137}\,\gamma(n) \;\le\; 4^{137}\cdot 128\cdot\gamma^{\star 8}\left(\frac{5}{6}\,n + 114\right) \;\le\; 2^{281}\,\gamma^{\star 8}\left(\frac{5}{6}\,m\right).$$

From here and the Upper Bound (Lemma 3.1) we obtain the result. $\square$

Recall that subexponential growth of $\mathbb{G}$ is shown in Corollary 7.5. This completes the proof of Theorem 5.1. $\square$

11. Proof of the Cancellation Lemma

Fix a reduced decomposition $(a) * a * a \cdots * (a)$ 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. At this moment remove all identities $\mathtt{I}$. Then apply these rules again to obtain w_{00}, w_{01}, w_{10} and w_{11}, and remove the identities $\mathtt{I}$. Finally, repeat this once again to obtain words $w_{000}, w_{001}, \ldots, w_{111}$. Following the proof of Theorem 9.2, 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:

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

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

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

To simplify the notation, consider the following cancatenations 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 those 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 one letter d in w'', and each of those is cancelled again by either Φ_0 or Φ_1. Taking into account the types of decompositions we obtain:

$$(\heartsuit) \qquad \begin{aligned} |w'| &\leq |w| + 1 - |w|_d\,, \\ |w''| &\leq |w| + 3 - |w|_c\,, \\ |w'''| &\leq |w| + 7 - |w|_b\,. \end{aligned}$$

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

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

as desired. $\square$

12. Further developments, conjectures and open problems

There is a number of open problems on groups of intermediate growth. Below we include only the most interesting results and conjectures which are closely connected to the material presented in this paper. We refer to surveys [1, 2, 6] and the monograph [8] for details and further references.

Let us start by saying that the Upper Bound 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 of $\gamma_{\mathbb{G}}$ remains 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 $\alpha = \lim_{n\to\infty} \log_n \log \gamma(n)$.*

In fact, the limit as in the conjecture is not known to exist and satisfy $0 < \alpha < 1$ for *any* finitely generated group. In fact, the extent to which results for $\mathbb{G}$ generalize to other groups of intermediate growth remains unclear as well. Although there are now constructions of groups with subexponential growth function $\gamma(n) \sim e^{n(1-o(1))}$, there is no known example of a group with superpolynomial growth function $\gamma(n) \sim \exp(n^{o(1)})$. The following result has been established for a large class 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 $\alpha > 0$.*

In conclusion, let us mention that the 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.

Acknowledgements. We would like to thank Tatiana Nagnibeda and Roman Muchnik for the interest in the subject and engaging discussions, and to Pierre de la Harpe for the helpful remarks on the manuscript. Both authors were partially supported by the NSF (RG was supported by DMS-0456185 and DMS-0600975, IP was supported by DMS-0402028).

References

[1] L. Bartholdi, R. I. Grigorchuk and 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 and Z. Sunik, Branch groups, in *Handbook of Algebra*, vol. 3, 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 and V. I. Sushchanskiĭ, Automata, dynamical systems, and groups, *Proc. Steklov Inst. Math.* **231** (2000), 128–203.

[7] M. Gromov, Hyperbolic groups, in *Essays in group theory*, Math. Sci. Res. Inst. Publ. **8**, Springer, New York, 1987, 75–263.

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

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