Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 54 (2008)
Heft: 3-4

Artikel: Groups of intermediate growth : an introduction
Autor: Grigorchuk, Rostislav / Pak, Igor
DOI: https://doi.org/10.5169/seals-109938

L'Enseignement Mathématique (2) 54 (2008), 251–272

GROUPS OF INTERMEDIATE GROWTH: AN INTRODUCTION

by Rostislav GRIGORCHUK and Igor PAK *)

ABSTRACT. We present an accessible introduction to basic results on groups of intermediate growth.

INTRODUCTION

The study of the growth of groups has a long and remarkable history spanning much of the twentieth century, and goes back to Hilbert, Poincaré, Ahlfors and others. 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 examples of such groups 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 applications 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 a reader familiar with only basic algebraic concepts.

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

Our proof is neither the shortest nor the one which gives the best possible bounds. Instead, we attempt to simplify the presentation as much as possible by separating the proof into a number of propositions of independent interest, supporting lemmas, and exercises. Along the way we prove two 'bonus'

*) Both authors were partially supported by the NSF. The first author was supported by DMS-0456185 and DMS-0600975; the second author was supported by DMS-0402028.

theorems: we show that $\mathbf{G}$ is *periodic* (every element has finite order) and give a nearly linear-time algorithm for the word problem in $\mathbf{G}$. We hope that novice readers will thus 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 to a recent book [8] for further results and references. The ideas of the proof 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 $\mathbf{G}$ is introduced in Section 5, while the remaining Sections 6–11 prove the intermediate growth of $\mathbf{G}$ and one 'bonus' theorem. We conclude with a 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 the notation $g^h = h^{-1}gh$ for conjugate elements, and $\mathtt{I}$ for the identity element. Finally, we set $\mathbf{N} = \{0, 1, 2, \ldots\}$.

1. THE 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 $\ell(g) \le n$. The 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 $\gamma, \gamma' : \mathbf{N} \to \mathbf{N}$. Set $\gamma \preccurlyeq \gamma'$ if $\gamma(n) \leq C\gamma'(\alpha n)$, for all $n > 0$ and some $C, \alpha > 0$. We say that γ and γ' are *equivalent*, and 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 $f : \mathbf{N} \to \mathbf{R}$ is said to be *polynomial* if $f(n) \sim n^\alpha$, for some $\alpha > 0$. A function f is said to be *superpolynomial* if

$$\lim_{n\to\infty} \frac{\log f(n)}{\log n} = \infty,$$

where here and in the sequel log denotes the natural logarithm. For example, n^π is polynomial, while n^n and $n^{\log\log n}$ are superpolynomial.

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

$$\lim_{n\to\infty} \frac{\log f(n)}{n} = 0.$$

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

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

Finally, a function is said to have *intermediate growth* if it is both superpolynomial and subexponential. For example, $n^{\log\log n}$, $e^{\sqrt{n}}$, and $e^{n/\log n}$ all have intermediate growth, while $e^{\sqrt{\log n}}$ 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 $G^m = G \times \ldots \times G$ also has polynomial growth, but that $\gamma_G \nsim \gamma_{G^m}$ 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 $\gamma = \gamma_G^S$ be its growth function. Show that the limit*

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

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

2. THE LOWER BOUND LEMMA

In the next two sections we present two technical results that are keys 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 $f\colon \mathbf{N} \to \mathbf{R}_+$ be a monotone increasing function, such that $f(n) \to \infty$ as $n \to \infty$. Suppose that $f \succcurlyeq f^m$ for some $m > 1$. Then $f(n) \succcurlyeq \exp(n^\alpha)$ for some $\alpha > 0$.*

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

Let $\pi(n) = \log f(n)$. Clearly, $\pi(n)$ is monotone increasing, $\pi(1) > 1$, and $\pi(n) \to \infty$ as $n \to \infty$. We need to show that $\pi(n) \geq An^\nu$ for some $A, \nu > 0$.

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

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

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

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

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

Iterating $(*)$ repeatedly 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 that $c \geq 0$. 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 the 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 that $c < 0$. Since $m \geq 2$ by assumption, we have $(1 + m + m^2 + \ldots + m^{k-1}) < m^k$, and the above inequality 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 the above, we get $\pi(n) \geq m^k\big(\pi(\alpha^k n) + c\big) \geq m^k$. 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. □

3. The Upper Bound Lemma

For the upper bound we need to introduce some notation. Let $f\colon \mathbf{N} \to \mathbf{R}_+$ 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 sum is over all k-tuples $(n_1, \ldots, n_k) \in \mathbf{N}^k$ such that $n_1 + \ldots + n_k \leq n$.

Lemma 3.1 (Upper Bound Lemma). *Let f be a nonnegative monotone increasing function, such that $f(n) \to \infty$ as $n \to \infty$. Suppose that $f(n) \leq Cf^{\star k}(\alpha n)$ 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 closely 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 proceed by induction on n. Suppose $\pi(n) := \log f(n) \leq An^{\nu}$. Note that we can always choose A large enough to satisfy the base of induction.

We have:

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

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

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

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

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

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

4. The 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 $v = (x_0, x_1, \ldots) \in \{\mathbf{0}, \mathbf{1}\}^*$.

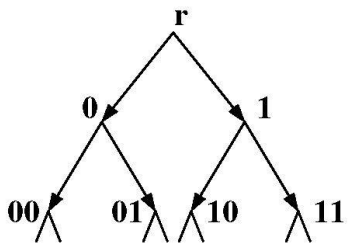

FIGURE 1
The infinite binary tree **T**

Note that the root of $\mathbf{T}$, denoted by $\mathbf{r}$, 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 $\mathbf{T}$.

The main subject of this section is the group $\mathrm{Aut}(\mathbf{T})$ of automorphisms of $\mathbf{T}$, i.e. the group of bijections $\tau\colon V \to V$ 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 the automorphism which maps $\mathbf{T_0}$ into $\mathbf{T_1}$ and preserves the natural order on vertices:

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

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

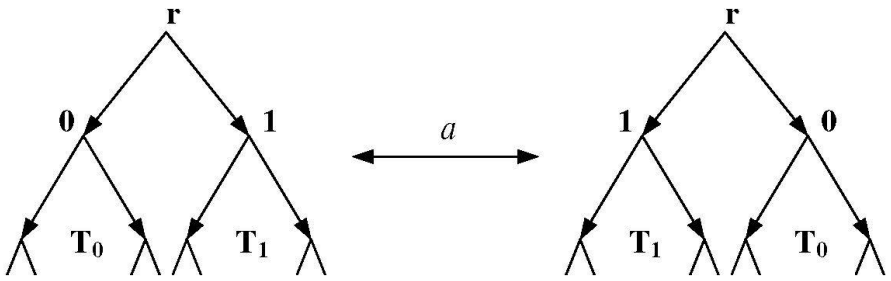

FIGURE 2
The automorphism $a \in \mathrm{Aut}(\mathbf{T})$

Similarly, one can define an automorphism a_v which exchanges the 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 $\iota_v\colon \mathbf{T} \to \mathbf{T}_v$ and a corresponding group isomorphism $\iota_v\colon \mathrm{Aut}(\mathbf{T}) \to \mathrm{Aut}(\mathbf{T}_v)$.

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:

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

In other words, $\epsilon_v(\tau)$ is equal to 0 if the automorphism maps the left edge leaving 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 determine 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 the map

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

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 the subtrees $\mathbf{T_0}$ and $\mathbf{T_1}$, respectively, defined as above. Pictorially, the automorphism τ is shown in Figure 3.

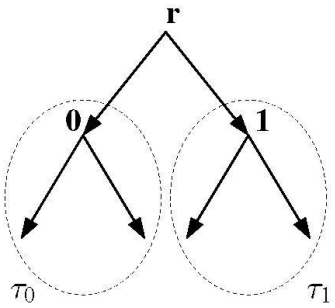

FIGURE 3
The automorphism $\tau = \varphi(\tau_0, \tau_1) \in \mathrm{Aut}(\mathbf{T})$

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

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

Proof. Let us extend the map φ to an isomorphism

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

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 the multiplication of automorphisms $\varphi(\cdot)$ coincides with that of the semidirect product, and defines a group isomorphism. We leave this easy verification to the reader. □

We denote by $\psi = \varphi^{-1}$ the isomorphism $\psi\colon \mathrm{Aut}(\mathbf{T}) \to \mathrm{Aut}(\mathbf{T}) \wr \mathbf{Z}_2$ 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 the 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 above idea to show that*

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

Conclude from this 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 prescribed as for* τ *above, but only for* $k < m$. *Show that the order* $\mathrm{ord}(\tau_m) \to \infty$ *as* $m \to \infty$, *and deduce the result from this.*)

5. THE FIRST CONSTRUCTION

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

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

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

Observe that the automorphisms b, c, and d are defined in a circular fashion via each other. Since the generator d acts 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 of defining the 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 an abbreviation 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 the elements $b, c, d \in \mathrm{Aut}(\mathbf{T})$ are well defined.

The elements $b, c, d \in \mathrm{Aut}(\mathbf{T})$ are shown graphically in Figure 4. Here the black triangles drawn at vertices correspond to places where the two subtrees rooted at each of these vertices are interchanged.

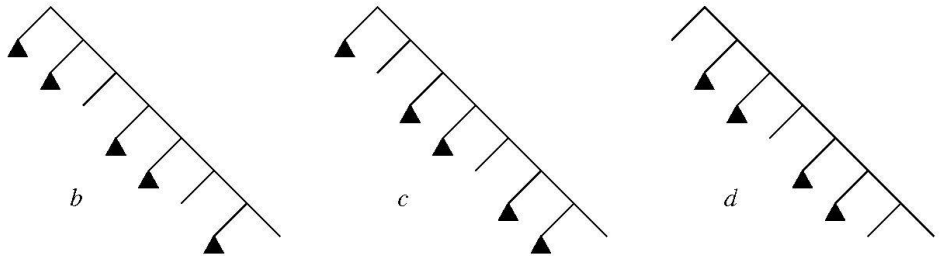

FIGURE 4
The elements b, c and $d \in \mathrm{Aut}(\mathbf{T})$

THEOREM 5.1 (Main Theorem). *The group* $\mathbf{G} = \langle a, b, c, d \rangle$ *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 the conditions* $(\circ)$.

EXERCISE 5.3. *Check that the 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 this that* $\langle b, c, d \rangle \simeq \mathbf{Z}_2^2$ *and that the group* $\mathbf{G} = \langle a, b, c, d \rangle$ *is* 3*-generated.*

EXERCISE 5.4. *Check the following relations in* $\mathbf{G}$: $(ad)^4 = (ac)^8 = (ab)^{16} = \mathtt{I}$. *Deduce from this that the* 2*-generator subgroups* $\langle a, b \rangle$, $\langle a, c \rangle$ *and* $\langle a, d \rangle$ *of* $\mathbf{G}$ *are finite.*

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

6. THE GROUP $\mathbf{G}$ IS INFINITE

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

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

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

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

LEMMA 6.1. *The fundamental subgroup* $\mathbf{H} \subset \mathbf{G}$ *satisfies:*

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

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 appear or not. Denote by $|w|$ the length of the word w, and by $|w|_a$ the number of occurrences of a in w. Note that $w \in \mathbf{H}$ 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 that $|w|_a$ 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. □

The 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 $\mathbf{G}$.

EXERCISE 6.2. *Check that the stabilizer subgroup* $\mathbf{H}_n := \mathrm{St}_{\mathbf{G}}(n)$ *has finite index in* $\mathbf{G}$: $[\mathbf{G} : \mathbf{H}_n] \leq |\mathrm{A}_n| = 2^{2^n - 1}$ (see Exercise 4.2).

Let $\psi = \varphi^{-1}\colon \mathrm{Aut}(\mathbf{T}) \to \big(\mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T})\big) \rtimes \mathbf{Z}_2$ be the isomorphism defined in Section 4. By definition, $\mathbf{H} \subset \mathbf{G} \subset \mathrm{Aut}(\mathbf{T})$.

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

Proof. By definition, $\mathbf{H}$ stabilizes $\mathbf{0}$ and $\mathbf{1}$, so $\psi(\mathbf{H}) \subset \mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T})$. From Exercise 5.2 we have

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

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

PROPOSITION 6.4. *The group $\mathbf{G}$ is infinite.*

Proof. From Lemmas 6.1 and 6.3, we have that $\mathbf{H}$ is a proper subgroup of $\mathbf{G}$ which is mapped surjectively onto $\mathbf{G}$. If $|\mathbf{G}| < \infty$ then $|\mathbf{G}| > |\mathbf{H}| \geq |\mathbf{G}|$, 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 the vertex $v \in \mathbf{T}$ with the action restricted only to the subtree $\mathbf{T}_v$. We say that G has the (strong) *self-similarity property* if $G_v \simeq G$ for all $v \in \mathbf{T}$.

PROPOSITION 6.5. *The group $\mathbf{G}$ has the self-similarity property.*

Proof. Use induction on the level $|v|$. By definition, $\mathbf{G_r} = \mathbf{G}$, and by Lemma 6.3 we have $\mathbf{G_0}, \mathbf{G_1} \simeq \mathbf{G}$. For any $v \in \mathbf{T}$, we similarly have $\mathbf{G}_{v\mathbf{0}}, \mathbf{G}_{v\mathbf{1}} \simeq \mathbf{G}_v$. This implies the result. □

EXERCISE 6.6. *Consider the following rewriting rules:*

$$\eta\colon a \to aba, \quad b \to d, \quad c \to b, \quad d \to c.$$

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

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

In this section we prove the first half of Theorem 5.1, by showing that the growth function γ of the group $\mathbf{G}$ satisfies the conditions of the Lower Bound Lemma.

Two groups G_1 and G_2 are called *commensurable* (which we denote by $G_1 \approx G_2$) 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, the group $\mathbf{Z}$ is commensurable with the infinite dihedral group $\mathrm{D}_\infty \simeq \mathbf{Z} \rtimes \mathbf{Z}_2$. Of course, all finite groups are commensurable to each other. Another example is $\mathbf{H} \approx \mathbf{G}$, since $\mathbf{H}$ is a subgroup of finite index in $\mathbf{G}$. Note also that commensurability is an equivalence relation.

Proposition 7.1. *The groups* $\mathbf{G}$ *and* $\mathbf{G} \times \mathbf{G}$ *are commensurable:* $\mathbf{G} \approx \mathbf{G} \times \mathbf{G}$.

Proposition 7.1 describes an important phenomenon which can be formalized as follows. A 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.

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

Denote by $\mathbf{B} = \langle b \rangle^{\mathbf{G}}$ the *normal closure of* $b \in \mathbf{G}$, defined as $\mathbf{B} := \langle g^{-1} b g \mid g \in \mathbf{G} \rangle$. Then the following lemma holds:

Lemma 7.2. *The subgroup* $\mathbf{B}$ *has finite index in* $\mathbf{G}$. *More precisely,* $[\mathbf{G} : \mathbf{B}] \leq 8$.

Proof. By Exercise 5.4, we have $a^2 = d^2 = (ad)^4 = \mathtt{I}$. It is now easy to see that the 2-generated subgroup $\langle a, d \rangle \subset \mathbf{G}$ is a dihedral group D_4 of order 8. By Exercise 5.3, we have $\mathbf{G} = \langle a, b, d \rangle$. Therefore, $\mathbf{G}/\mathbf{B}$ is a quotient of $\langle a, d \rangle$, and $[\mathbf{G} : \mathbf{B}] \leq |\mathrm{D}_4| = 8$. $\square$

LEMMA 7.3. *The subgroup* $\widetilde{\mathbf{H}} = \psi(\mathbf{H}) \subset \mathbf{G} \times \mathbf{G}$ *contains* $\mathbf{B} \times \mathbf{B}$.

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

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

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

Proposition 7.1 now follows immediately from Lemma 7.2:

$$[\mathbf{G} \times \mathbf{G} : \widetilde{\mathbf{H}}] \le [\mathbf{G} \times \mathbf{G} : \mathbf{B} \times \mathbf{B}] = [\mathbf{G} : \mathbf{B}]^2 \le 8^2 = 64.$$

Since $\mathbf{G}$ is infinite (Proposition 6.4) this implies that the group $\mathbf{G}$ 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 (Lemma 2.1) implies the result. □

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

COROLLARY 7.5. *The group* $\mathbf{G}$ *has superpolynomial growth. Moreover, the growth function* $\gamma_{\mathbf{G}}(n) \succcurlyeq \exp(n^\alpha)$ *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 $\gamma = \gamma_{\mathbf{G}}^S$ of the group $\mathbf{G}$ with generating set $S = \{a, b, c, d\}$. In this section we obtain some recursive bounds on the

length $\ell(g) = \ell_{\mathbf{G}}^{S}(g)$ of elements $g \in \mathbf{G}$ in terms of S. Note that, although $\mathbf{G}$ is 3-generated, having the fourth generator is convenient for technical reasons.

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

$$\begin{aligned} &\text{(i)} && \text{if } g = a*a*a\cdots*a*a, \\ &\text{(ii)} && \text{if } g = a*a*a\cdots*a*, \\ &\text{(iii)} && \text{if } g = *a*a*\cdots a*a, \\ &\text{(iv)} && \text{if } g = *a*a*\cdots a*a*. \end{aligned}$$

Of course, an 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 $g \in \mathbf{G}$ has all of its reduced decompositions of the same type* (i), or *of type* (iv), or *of types* (ii) *and* (iii).

Proof. Recall that the number of a's in a reduced decomposition of $g \in \mathbf{G}$ is even if $g \in \mathbf{H}$, and 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 5.4, and both are reduced decompositions. From now on we refer to elements $g \in \mathbf{G}$ as of *type* (i), (ii/iii), or (iv) depending on the type of their reduced decompositions.

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

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

$$\begin{aligned} &\ell(g_0), \ell(g_1) \le \tfrac{1}{2}(\ell(g) - 1) && \text{if } g \text{ has type (i)}, \\ &\ell(g_0), \ell(g_1) \le \tfrac{1}{2}\,\ell(g) && \text{if } g \text{ has type (ii/iii)}, \\ &\ell(g_0), \ell(g_1) \le \tfrac{1}{2}(\ell(g) + 1) && \text{if } g \text{ has type (iv)}. \end{aligned}$$

Proof. Fix an element $g \in \mathbf{G}$, and let g_0, g_1, σ be as in Lemma 8.2. We have $\sigma = \mathtt{I}$ if $g \in \mathbf{H}$, and $\sigma = a$ otherwise (see the proof of Lemma 6.1). For every reduced[1]) decomposition $w = (a)*a*a\cdots*a*(a)$ of g we shall construct decompositions of the elements g_0, g_1 with lengths as in the lemma. As before, we use $*$ to denote any one of the generators b, c, d. Also, for every $*$ in a reduced decomposition we denote by $\kappa(*)$ the number of a's preceding $*$.

Consider the following *rewriting rules*:

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

and

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

These rules act on words w in the 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 $g_0', g_1' \in \mathbf{G}$ 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 the rewriting rules the lengths of g_0, g_1 are as in Lemma 8.2. □

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

COROLLARY 8.3. *Under the conditions of Lemma* 8.2 *we have:*

$$\ell(g_0) + \ell(g_1) \le \ell(g) + 1\,.$$

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

[1]) Here by (a) we mean that this generator may or may not be present in the decomposition.

EXERCISE 8.4. *Under the conditions of Lemma* 8.2 *we have:*

$$\ell(g) \leq 2\ell(g_0) + 2\ell(g_1) + 50\,.$$

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

EXERCISE 8.5. *Prove that every element* $g \in \mathbf{G}$ *has order* 2^k, *for some integer* k. (Hint: *Use induction to reduce the problem to the 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 the 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 the 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 an algorithmic point of view the problem is undecidable, i.e. there is no Turing machine which can solve 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 $x_i^{-1} x_i$, $1 \leq i \leq k$; the product w is equal to $\mathtt{I}$ if and only if the resulting word is empty. Since every letter is cancelled at most once and no new letters are 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 the 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 a 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 the word problem can be solved in $\mathbf{G}$ in nearly linear time[2]).

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

THEOREM 9.2. *The word problem in* $\mathbf{G}$ *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 $w \neq_{\mathbf{G}} \mathtt{I}$. If $\pi(w)$ 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 be reduced). Recall that the product $w =_{\mathbf{G}} \mathtt{I}$ if and only if $w_0, w_1 =_{\mathbf{G}} \mathtt{I}$. Now repeat the procedure for the words w_0, w_1 to obtain words $w_{00}, w_{01}, w_{10}, w_{11}$, etc. It is easy to check that $w =_{\mathbf{G}} \mathtt{I}$ 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. □

REMARK 9.3. For every reduced decomposition as above one can construct a binary tree of 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 $\gamma_{\mathbf{G}}$. Exploring this connection is of great interest, but lies outside the scope of this paper.

10. SUBEXPONENTIAL GROWTH OF $\mathbf{G}$

In this section we prove the second half of Theorem 5.1 by establishing the upper bound on the growth function γ of the group $\mathbf{G}$ 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 $\mathbf{H}_3 := \mathrm{St}_{\mathbf{G}}(3)$ be the stabilizer of vertices on the third level, and recall that the index $[\mathbf{G} : \mathbf{H}_3] \leq 2^7 = 128$ (Exercise 6.2). There is a natural embedding

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

(see Section 6). By self-similarity, the eight groups in the product are isomorphic: $\mathbf{G}_{\mathbf{ijk}} \simeq \mathbf{G}$, where $\mathbf{i}, \mathbf{j}, \mathbf{k} \in \{\mathbf{0}, \mathbf{1}\}$. These isomorphisms are obtained by restrictions of natural maps: ι_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 χ: $\mathbf{H}_3 \to \mathbf{G}^8$, which we write as $\chi(h) = (g_{000}, g_{001}, \ldots, g_{111})$, where $h \in \mathbf{H}_3$ and $g_{ijk} \in \mathbf{G}$.

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 on this bound.

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

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

We postpone the proof of the Cancellation Lemma until the next section. We are now ready to complete the proof of the Main Theorem.

PROPOSITION 10.2. *The group $\mathbf{G}$ has subexponential growth. Moreover, $\gamma_{\mathbf{G}}(n) \preccurlyeq \exp(n^{\nu})$ for some $\nu < 1$.*

Proof. All elements $g \in \mathbf{G}$ can be written as $g = u \cdot h$, where $h \in \mathbf{H}_3$ and u is a coset representative of $\mathbf{G}/\mathbf{H}_3$. Since $[\mathbf{G} : \mathbf{H}_3] \leq 128$, 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 $\ell(h) \leq \ell(g) + 127$.

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

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

Putting all this together we conclude (using Exercise 10.3 below):

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

where the summation is over all integer 8-tuples with $n_1+\ldots+n_8 \leq \frac{5}{6}n+114$. Set $m = n + 137$, so that $\frac{5}{6}n + 114 < \frac{5}{6}m$. Now by Exercise 1.2 note that

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

Therefore we have:

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

From this and the Upper Bound Lemma (Lemma 3.1) we obtain the result. □

EXERCISE 10.3. *Let G be a group with length function ℓ and growth γ (relative to some finite generating set). Show that the size of the set $\Delta = \{(g_1,\ldots,g_k) \in G^k \mid \ell(g_1)+\cdots+\ell(g_k) \leq \lambda\}$ consisting of all k-tuples of 'total' length less than some constant λ satisfies: $|\Delta| \leq \sum_{(n_1,\ldots,n_k)\in\mathbf{N}^k} \gamma(n_1)\cdots\gamma(n_k)$, where the sum is over all k-tuples such that $n_1+\cdots+n_k \leq \lambda$.*

Recall that the superpolynomial growth of $\mathbf{G}$ has been 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 $h \in \mathbf{H}_3$, and denote it by w. By applying the rewriting rules Φ_0 and Φ_1 to w, we obtain words w_0 and w_1. Now 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 the elements g_0, g_1, then of $g_{00}, \ldots, g_{11}$, and of $g_{ijk} \in \mathbf{G_{ijk}}$, respectively. Note that these decompositions are not necessarily reduced, so for the record:

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

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

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

To simplify the notation, consider the following concatenations 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 that each of these 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 these is cancelled again by either Φ_0 or Φ_1. Taking into account the types of decompositions we obtain:

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

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

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

as desired. □

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 $\mathbf{G}$. Although considerably sharper bounds are known, the exact asymptotic behavior of $\gamma_{\mathbf{G}}$ remains an open problem. Unfortunately, we do not even know whether it makes sense to say that $\gamma_{\mathbf{G}}$ has growth $\exp(n^\alpha)$ for some fixed $\alpha > 0$:

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

In fact, the limit in the conjecture is not known to exist and satisfy $0 < \alpha < 1$ for *any* finitely generated group. Also, the extent to which results for $\mathbf{G}$ 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 conjecture 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 γ_G be its growth function. Then $\gamma_G(n) \succcurlyeq \exp(n^\alpha)$ for some $\alpha > 0$.*

In conclusion, let us mention that the group $\mathbf{G}$ is not finitely presented. The 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 their interest in the subject and engaging discussions, and Pierre de la Harpe for helpful remarks on the manuscript.

REFERENCES

[1] BARTHOLDI, L., R.I. GRIGORCHUK and V.V. NEKRASHEVYCH. From fractal groups to fractal sets. In: *Fractals in Graz* (P. Grabner, W. Woess, eds.), 25–118. Birkhaüser, Basel, 2003.

[2] BARTHOLDI, L., R.I. GRIGORCHUK and Z. SUNIK. Branch groups. In: *Handbook of Algebra*, vol. 3, 989–1112. North-Holland, Amsterdam, 2003.

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

[4] —— On the Milnor problem of group growth. *Soviet Math. Dokl. 28* (1983), 23–26.

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

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

[7] GROMOV, M. Hyperbolic groups. In: *Essays in Group Theory*, 75–263. Math. Sci. Res. Inst. Publ. *8*. Springer-Verlag, New York, 1987.

[8] DE LA HARPE, P. *Topics in Geometric Group Theory*. Chicago Lectures in Mathematics, University of Chicago Press, Chicago, 2000.

[9] MUCHNIK R. and I. PAK, On growth of Grigorchuk groups. *Internat. J. Algebra Comput. 11* (2001), 1–17.

(Reçu le 19 mars 2007)

Rostislav Grigorchuk

Department of Mathematics
Texas A&M University
College Station, TX 77843
USA
e-mail: grigorch@math.tamu.edu

Igor Pak

School of Mathematics
University of Minnesota
Minneapolis, MN 55455
USA
e-mail: (pak@math.umn.edu)