GROWTH RATE OF GROUPS

CONG HAN LIM

Abstract. The concept of growth rates in group theory has proven to be a potent tool for studying groups. For example, in 1981, Mikhail Gromov proved the set of finitely-generated virtually nilpotent groups are precisely the groups of polynomial growth. In this paper, we give an introduction to growth rate in group theory and provide many tools and examples to illustrate some of the methods used. We also construct the First Grigorchuk group and prove that it has intermediate growth.

Contents

Introduction 1
1. Word Length and Growth Rate 2
2. Exponential Growth 5
3. Polynomial Growth 8
The First Grigorchuk Group: A Group of Intermediate Growth 10
4. Rooted Binary Trees 10
5. Construction of the First Grigorchuk Group and Basic Properties 12
6. Superpolynomial Growth 14
7. Rewriting Rules 16
8. Subexponential Growth 17
9. Proof of Upper and Lower Bound Lemmas 19
Acknowledgments 21
References 21

Introduction

Consider a group G and a generating set $S = \{s_1, s_2, \ldots, s_k\}$. We define the *word length* $l_S(g)$ of an element $g \in G$ to be the length of the shortest decomposition $g = s_{i_1}^{\pm 1} \cdots s_{i_n}^{\pm 1}$. The *growth function* of G with respect to the generating set S, denoted by γ_G^S, associates to each integer $n \geq 0$ the number of elements $g \in G$ such that $l_S(g) \leq n$. The *growth rate of a group* G is the asymptotic behavior of γ_G^S.

It has been known since the 1960s that all finitely-generated groups have either polynomial, exponential or intermediate growth, but it was only in 1980 that Rostilav Grigorchuk constructed the first group proven to have intermediate growth. Also, while it has been known for many decades that all finitely-generated virtually nilpotent have polynomial growth, it was only in 1981 that the converse was proven by Mikhail Gromov. In this paper, we will introduce some of the concepts of growth and state some key results. We will also construct the First Grigorchuk group. The reader is assumed to be familiar with basic algebraic concepts.

The first half of this paper is designed to be more of an overview of some of the important concepts behind growth rates. The very first section focuses on introducing the concepts of growth, such as the properties of the word length (the shortest string of elements in the generating set needed to express an element) and the growth rate (the rate at which the number of elements increase with respect to an increase in the maximum word length allowed). We show that there are three classes of growth, namely *polynomial, exponential* and *intermediate* growth and lead up to the result that the growth rates of a finitely-generated group and any subgroup of finite index have to be equivalent.

The next two sections tackle some of the tools behind understanding polynomial and exponential growth. We provide an analogue of the "Ping-Pong Lemma" for free semi-groups and also show that the group of upper-triangular matrices with 1's along the diagonals and integers elsewhere has polynomial growth.

In contrast, the second half of this paper is focused on answering an important question in geometric group theory; in 1968, John Milnor asked if groups of intermediate growth exist and Rostilav Grigorchuk constructed the first such group in 1980. This part of the paper focuses on the construction of the First Grigorchuk group and introduces only essential tools and definitions to prove that it has intermediate growth. Along the way we prove that the First Grigorchuk group is infinite, multilateral, and also a 2-group. The last fact is of particular interest as it provides a negative answer to the General Burnside Problem, which asks if finitely-generated torsion groups are necessarily finite.

1. Word Length and Growth Rate

All groups in this paper are assumed to be finitely-generated unless explicitly stated otherwise.

Remark. There is a difference between the *word length* of an element g and the length of word w (denoted by $|w|$) representing g. The word w need not be the shortest decomposition of g, hence $|w| \geq l(g)$.

Exercise 1.1. Basic properties of word lengths and growth functions:

(1) For any group G with generating set S such that $|S| = k$, we have

$$\gamma_G^S(n) \leq \sum_{i=0}^{n} (2k)^i.$$

(2) For any infinite group G, the growth function is strictly increasing:

$$\gamma_G^S(n+1) > \gamma_G^S(n)$$

(3) Word length l_S is subadditive and growth rate γ is submultiplicative. i.e. for all $g_1, g_2 \in G$, we have

$$l_S(g_1 g_2) \leq l_S(g_1) + l_S(g_2)$$

and for $m, n \geq 1$:

$$\gamma_G^S(m+n) \leq \gamma_G^S(m)\gamma_G^S(n).$$

We now introduce terms and definitions that enable us to classify groups according to their growth rates.

Definition 1.2. Let f and g be functions from $\mathbb{N}$ to $\mathbb{R}^+$. We say f *dominates* g, denoted by $g \lesssim f$, if there exists constants $\alpha, C > 0$ such that

$$g(n) \leq C \cdot f(\alpha n)$$

for all $n \geq 1$. Furthermore, we say that f and g are *equivalent* (written as $f \sim g$) if $f \lesssim g$ and $g \lesssim f$.

One can check that this notion of equivalence of growth is an equivalence relation.

Proposition 1.3. *Given S and S', generating sets of G, their respective growth functions γ_G^S and $\gamma_G^{S'}$ are equivalent.*

Proof. Suppose $S = \{s_1, s_2, \dots s_k\}, S' = \{s_1', s_2', \dots, s_l'\}$. Since S is a generating set of G, we can express each element (and its inverse) in S' as words in $s_1, \dots s_k, s_1^{-1}, \dots, s_k^{-1}$. Let α denote the length of the longest such word. It follows that

$$l_{S'}(g) \leq n \Rightarrow l_S(g) \leq \alpha n,$$

so we have $\gamma_G^{S'}(n) \lesssim \gamma_G^S(\alpha n)$. By the same argument we have $\gamma_G^S(n) \lesssim \gamma_G^{S'}(\alpha n)$, proving our claim. □

Since Proposition 1.3 shows that considering different generating sets does not significantly alter the growth, for the rest of the paper, we will occasionally omit the superscript S from γ_G^S. We will also omit the subscript G if the choice of G is unambiguous.

Definition 1.4. A growth function $\gamma : \mathbb{N} \to \mathbb{R}^+$ is said to be *polynomial* if $\gamma(n) \lesssim n^\alpha$ for some $\alpha > 0$. Similarly, a growth function γ is *exponential* if $\gamma(n) \gtrsim e^n$.

If a growth function γ is neither polynomial or exponential, then we say that γ has *intermediate growth.*

Definition 1.5. A growth function $\gamma : \mathbb{N} \to \mathbb{R}^+$ is said to be *superpolynomial* if $\lim_{n\to\infty} \frac{\ln \gamma(n)}{\ln n} = \infty$. A growth function γ is *subexponential* if $\lim_{n\to\infty} \frac{\ln \gamma(n)}{n} = 0$.

Exercise 1.6. If a function is superpolynomial then it is not polynomial. Likewise, if a function is subexponential then it is not exponential.

Not all functions from $\mathbb{N}$ to $\mathbb{R}^+$ can be neatly categorized under the three main categories. For example, while n^e is polynomial, 2^n is exponential and $e^{\sqrt{n}}$ is of intermediate growth, we have $e^n \sin(\pi n)$ which fluctuates between being 0 and exponential and hence is neither.

However, we are able to neatly categorize finitely generated groups into three types depending on whether they have *polynomial, exponential or intermediate growth.* Proposition 1.3 shows us that all growth functions of a group G are equivalent, and Theorem 1.8 shows us that all growth functions have *exponential* or *subexponential growth.*

Lemma 1.7. *(Fekete Lemma). Let α_n be a subadditive sequence of non-negative numbers. Then sequence $\left(\frac{\alpha(n)}{n}\right)$ converges and*

$$\lim_{n\to\infty} \frac{\alpha(n)}{n} = \inf \frac{\alpha(n)}{n}.$$

Proof. For any positive integer a we can express each $n \in \mathbb{N}$ as $n = qa + r$ with $q \geq 0$ and $0 \leq r < a$. Note that

$$\frac{\alpha(n)}{n} = \frac{\alpha(qa+r)}{qa+r} \leq \frac{q\alpha(a)+\alpha(r)}{qa+r} \leq \frac{q\alpha(a)+\alpha(r)}{qa}.$$

Since $\lim_{n\to\infty} \frac{\alpha(r)}{qa} = 0$, it follows that $\limsup_{n\to\infty} \frac{\alpha(n)}{n} \leq \frac{\alpha(a)}{a}$. Also, we know that $\inf \frac{\alpha(a)}{a} \leq \frac{\alpha(n)}{n}$ for all $a \geq 1, n \in \mathbb{N}$. The lemma follows. □

Theorem 1.8. *Given a group G and a generating set S, the limit*

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

always exists.

Proof. Since γ is a submultiplicative function, for all $m, n \geq 1$ we have

$$\ln \gamma(m+n) \leq \ln(\gamma(m)\gamma(n)) = \ln \gamma(m) + \ln \gamma(n).$$

So $\ln \gamma$ is a subadditive function. We can then directly apply Lemma 1.7 to obain the result. □

We will state a few more properties about growth rates.

Exercise 1.9. If G is an infinite group with polynomial growth, then the direct product G^m also has polynomial growth, but $\gamma_G \nsim \gamma_{G^m}$ for any $m > 1$. If G has exponential growth, then the direct product G^m also has exponential growth, and $\gamma_G \sim \gamma_{G^m}$ for any $m \geq 1$.

Proposition 1.10. *Subgroups of finitely generated groups need not be finitely generated.*

In order to prove the above proposition, we will exhibit a class of groups with subgroups that are not finitely-generated.

Definition 1.11. The *Baumslag-Solitar groups* are groups of the form

$$B(m,n) = \langle s, t | st^m s^{-1} = t^n \rangle$$

for any integers m, n.

Note that the group $B(1,1)$ is precisely the free abelian group on 2 generators.

Proposition 1.12. *Let B be the Baumslag-Solitar groups $B = B(m,n)$ where $1 \leq m < n$ and m, n are coprime. Then, B has a subgroup that is infinitely-generated.*

Proof. We denote by $G_{n/m}$ the subgroup of $GL(2,\mathbb{R})$ generated by

$$\begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

One can show that this is a quotient of B.

We will now construct an infinitely-generated subgroup. Let A be the set of matrices of the form

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{Z}\left[\frac{1}{m}\right] \right\}.$$

A a subgroup of $GL(2,\mathbb{R})$ as $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix}$, where $a-b \in \mathbb{Z}\left[\frac{1}{m}\right]$.

We want to show that this is also a subgroup of $G_{n/m}$. Since m and n are coprime, by the Euclidean algorithm, for every $k > 1$ we can find $x_k, y_k \in \mathbb{Z}$ such that $x_k m^k + y_k n^k = 1$. This allows us to generate any matrix of the form $\begin{pmatrix} 1 & m^{-k} \\ 0 & 1 \end{pmatrix}$ in $G_{n/m}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{x_k}\begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix}^{n}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{y_k}\begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix}^{-n} = \begin{pmatrix} 1 & m^{-k} \\ 0 & 1 \end{pmatrix}$$

Hence, any element in A can be generated in $G_{n/m}$, thus $A \subset G_{n/m}$.

Finally, note that $A \cong \mathbb{Z}$. It suffices to show that $\mathbb{Z}\left[\frac{1}{m}\right]$ is not finitely generated as an additive group. Suppose $\mathbb{Z}\left[\frac{1}{m}\right]$ is finitely generated by $a_1, \ldots, a_l$. Select the greatest denominator m^k that appears in the generating set $\{a_i\}$. Then it is clear that $\frac{1}{m^{k+1}}$ cannot be written as a sum in $\{a_i\}$, which is a contradiction. □

Theorem 1.13. *Let H be a subgroup of G of finite index. Then, H is finitely generated and $\gamma_H \sim \gamma_G$.*

The last theorem can be solved directly by applying the *Fundamental Observation of Geometric Group Theory*. One can find an excellent treatment in [2] (Theorem IV.23).

Exercise 1.14. Let H be a quotient of a group G. Then $\gamma_H \lesssim \gamma_G$.

2. Exponential Growth

Notation 2.1. We denote by M_2 the *free semi-group* on two generators a, b. This is the semi-group generated by a, b such that every word in a, b corresponds to a unique element in M_2 and the product $(\cdot)$ is defined by $w_1 \cdot w_2 = w_1 w_2$, the concatenation of the two elements.

Note that we can analogously define *word length* and *growth* for semi-groups:

Definition 2.2. Let M be a semi-group and let S be a generating set of M. We define the *word length* $l_S(m)$ of an element $m \in M$ to be the length of the shortest decomposition $g = s_{i_1} \cdots s_{i_n}$. The *growth function*, denoted by γ_M^S, is a map from $\mathbb{N}$ to $\mathbb{N}$ with respect to the generating set S that sends each positive integer n to the number of elements $m \in M$ such that $l_S(m) \leq n$.

Theorem 2.3. *Any finitely-generated group which contains a free semi-group on two generators has exponential growth.*

Proof. Let M_2 be the free semi-group on two generators which we denote m_1, m_2 . The growth function γ_{M_2} based on the two generators satisfies

$$\gamma(n) = 2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$$

since the number of elements of length n is precisely the number of ways to form a n-letter word from a, b. Hence, $\gamma(n) \sim 2^n$.

Let G be a group that contains M_2. By Exercise 1.3, we only need to consider any one particular generating set. Pick a generating set S of G containing m_1, m_2. It follows that $\gamma_G^S(n) \gtrsim 2^n$, thus G has exponential growth. □

We now prove an analogue of the celebrated "Ping-Pong Lemma" (see Chapter II.B from [2]) for free semi-groups.

Theorem 2.4. *Let G be a group acting on a set X. Suppose we have $g_1, g_2 \in G$ and subsets $X_1, X_2 \subset X$ such that*

$$X_1 \cap X_2 = \emptyset, \qquad g_1(X_1 \cup X_2) \subset X_1, \qquad g_2(X_1 \cup X_2) \subset X_2.$$

Then, g_1, g_2 generate a free semi-group and G has exponential growth.

Proof. We will prove this by exhibiting an injective map from the free semi-group M_2 generated by m_1, m_2 to G. Let $\varphi : M_2 \to G$ be the map that sends m_1, m_2 to g_1, g_2 respectively. Consider two elements $w, w' \in M_2$ such that $\varphi(w) = \varphi(w')$. We need to show that $w = w'$, which we will prove by induction on the length of w.

Suppose w is the empty word. For the sake of a contradiction, without loss of generality we assume w' begins with m_1. Then, it also follows that $\varphi(w')X_2 \subset X_1$. But we have $\varphi(w')X_2 = \varphi(w)X_2 = X_2$ so $X_1 \cap X_2 \neq \emptyset$, which is a contradiction.

We now consider the inductive step. Suppose our statement holds for all w where $|w| < n$. For w of length n, note that we can rewrite w, w' as

$$w = av, \qquad w' = a'v'$$

where $a, a' \in \{m_1, m_2\}$.

By the same reasoning as before, it follows that $a = a'$. So, we have

$$\varphi(w) = \varphi(a)\varphi(v) \text{ and } \varphi(w') = \varphi(a)\varphi(v').$$

The equation implies $\varphi(v) = \varphi(v')$, and by our inductive hypothesis we have $v = v'$.

It follows from Theorem 2.4 that G has exponential growth. □

Example 2.5. The subgroup G of $GL(2, \mathbb{R})$ generated by

$$s = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

has exponential growth.

Proof. Note that

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} s = \begin{pmatrix} 2a & b \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} s^{-1} = \begin{pmatrix} \frac{1}{2}a & b \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} t = \begin{pmatrix} a & a+b \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} t^{-1} = \begin{pmatrix} a & a-b \\ 0 & 1 \end{pmatrix}.$$

Hence,

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a = 2^k \text{ where } k \in \mathbb{Z}, b \in \mathbb{Z}\left[\frac{1}{2}\right] \right\}.$$

We define a group action of G on $\mathbb{R}$ by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} x = ax + b.$$

Note that each element of this group has a unique fixed point given by $\frac{b}{1-a}$ if and only if $a \neq 1$. We now pick elements s_1, s_2 with different fixed points such that $s_i = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix}$, where $a_i < 1$.

Pick two disjoint open intervals I_1, I_2 containing the fixed points of s_1 and s_2 respectively, and pick an interval I that contains both intervals. Let $f : \mathbb{R} \to \mathbb{R}$ be the function $f(x) = s_1 x$. For any point $x \in \mathbb{R}$ we have

$$\lim_{n\to\infty} f^n(x) = \frac{b_1}{1 - a_1}.$$

This means that for some $k \in \mathbb{N}$, we have $s_1^k(I)$. By the same argument, we can find some $k' \in \mathbb{N}$ where $s_2^{k'}(I_2) \subset I_2$.

We can now apply Theorem 2.4 to obtain our result. □

Recall from Definition 1.11 the Baumslag-Solitar groups $B(m, n)$. We will now prove that a certain class of them have exponential growth.

Proposition 2.6. *The Baumslag-Solitar Groups $B(m, n) = \langle s, t | st^m s^{-1} = t^n \rangle$ where $1 \leq m < n$ have exponential growth.*

Proof. We first consider the case by considering the case where m, n are coprime. As in the proof of Proposition 1.12, we denote by $G_{n/m}$ the subgroup of $GL(2, \mathbb{R})$ generated by

$$\begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Using the method outlined in Example 2.5, one can show that

$$G_{n/m} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| a = \left(\frac{n}{m}\right)^k \text{ where } k \in \mathbb{Z}, b \in \mathbb{Z}\left[\frac{1}{m}\right] \right\}$$

and also that $G_{n/m}$ contains a free semi-group on two generators.

It remains to show that $G_{n/m}$ is a quotient of $B(m, n)$. Note that

$$\begin{aligned} \begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{m}{n} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{m}{n} & m \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n. \end{aligned}$$

Let $\varphi : B(m, n) \to G_{n/m}$ be the map such that

$$\varphi(s) = \begin{pmatrix} \frac{n}{m} & 0 \\ 0 & 1 \end{pmatrix} \qquad \varphi(t) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

One can check that φ is well-defined. By Exercise 1.14, we know the growth rate of $B(m, n)$ is exponential.

We finally need to consider the case where $m = rm' < n = rn'$ for some $r > 1$ and p', q' are coprime. From the first case, we know that $B(m', n')$ has exponential growth. One can show that $B(m', n')$ is a quotient of $B(m, n)$, and by Exercise 1.14 this proves our claim. □

3. Polynomial Growth

Proposition 3.1. *The additive groups $\mathbb{Z}^k$ are of polynomial growth.*

Proof. For any $\mathbb{Z}^k$, consider the standard generating set $S = \{e_1, e_2, \ldots, e_k\}$, the standard orthogonal basis for $\mathbb{R}^k$. The set of words of length less than n are precisely the words of the form $e_1^{i_1} e_2^{i_2} \ldots e_k^{i_k}$ where $\sum_j i_j \leq n$. It is clear that $\gamma(n) \leq n^k$. So, γ is polynomial. □

We see that for any finite abelian group G that is generated by k many elements, the growth rate of G is slower than that of $\mathbb{Z}^k$. Hence, this proves the following corollary:

Corollary 3.2. *Every finitely-generated abelian group is of polynomial growth.*

Definition 3.3. The *Heisenberg group* is the group

$$\langle x, y, z \mid [x, z] = 1, [y, z] = 1, [x, y] = u \rangle,$$

which is equivalent to the group of matrices

$$\left\{ \left(\begin{array}{ccc} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{array} \right) \middle| \, a, b, c \in \mathbb{Z} \right\}$$

generated by the elements

$$x = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{array} \right) \quad y = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \quad z = \left(\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right).$$

The equivalence of these two definitions is left as an exercise to the reader.

Note that each element g in this group can be uniquely expressed in the form $g = x^a y^b z^c$, where

$$g = \left(\begin{array}{ccc} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{array} \right).$$

Exercise 3.4. Check that

$$\begin{aligned} (x^a y^b z^c)x &= x^{a+1} y^b z^{c+b} & (x^a y^b z^c)x^{-1} &= x^{a-1} y^b z^{c-b} \\ (x^a y^b z^c)y &= x^a y^{b+1} z^c & (x^a y^b z^c)y^{-1} &= x^a y^{b-1} z^c \\ (x^a y^b z^c)z &= x^a y^b z^{c+1} & (x^a y^b z^c)z^{-1} &= x^a y^b z^{c-1}. \end{aligned}$$

Lemma 3.5. *Let $|g|$ be the word length for an element g in the Heisenberg group. Then we have the following inequalities:*

(1) $|x^a y^b z^c| \leq |a| + |b| + 6\sqrt{|c|}$.

(2) $|x^a y^b z^c| \leq n \Rightarrow \left\{ \begin{array}{l} |a| + |b| \leq n \\ |c| \leq n^2 \end{array} \right.$.

Proof. To prove the first claim, note that

$$\begin{aligned} x^a y^{-b} x^{-a} y^b &= ((x^a y^{-b}) x^{-a}) y^b \\ &= ((x^{a-1} y^{-b}) x^{-a+1} z^b) y^b \\ &\vdots \\ &= y^{-b} z^{ab} y^b \\ &= z^{ab}. \end{aligned}$$

For any natural number c, consider the integer portion i of $\sqrt{c}$ and the difference $j = c - i^2$, where $j \leq 2\sqrt{c}$. Since $x^i y^{-i} x^{-i} y^i z^j = z^c$, it follows that $|z^c| \leq 2\sqrt{m}$. The proof is similar for $c < 0$.

For the second claim, the first inequality follows immediately. The second inequality can be shown by induction, since $n^2 + n \leq (n+1)^2$. □

Proposition 3.6. *The Heisenberg Group has polynomial growth. More precisely, we have*

$$\gamma(n) \sim n^4.$$

Proof. To show $\gamma(n) \gtrsim n^4$, consider $|a| \leq \frac{n}{8}, |b| \leq \frac{n}{8}$ and $|c| \leq \left(\frac{n}{8}\right)^2$. By the first claim of Lemma 3.5, we have $|x^a y^b z^c| \leq n$. So, $\gamma(n) \geq (\frac{n}{8})(\frac{n}{8})(\frac{n}{8})^2$. To show $\gamma(n) \lesssim n^4$, the second claim of Lemma 3.5 tells us that $\gamma(n) \leq (n+1)^2(2n^2+1)$. □

Proposition 3.7. *For any $n \in \mathbb{N}$, the group of upper triangular $n \times n$ matrices of the form*

$$\left\{ \left(\begin{array}{ccccc} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ \vdots & & \ddots & \ddots & \vdots \\ & & & 1 & a_{(n-1)n} \\ 0 & 0 & \dots & 0 & 1 \end{array} \right) \middle| \, a_{ij} \in \mathbb{Z} \right\}$$

has polynomial growth.

Proof. (Outline). The method of this proof is similar to the proof of Proposition 3.6.

We denote our group of matrices by G. Let S be the set of generators

$$S = \{X_{ij} | X_{ij} = I_n + e_{ij}\}$$

where I_n is the $n \times n$ identity matrix and e_{ij} is the matrix with zeroes everywhere except for a 1 in the ij-th coordinate.

With the set of generators S, as in the Heisenberg group, we have a simple way of representing each element of the group uniquely. It is left as an exercise for the reader to check that

$$X_{(n-1)n}^{a_{(n-1)n}} X_{(n-2)(n-1)}^{a_{(n-2)(n-1)}} X_{(n-2)n}^{a_{(n-2)n}} \dots X_{1n}^{a_{1n}} = \left(\begin{array}{ccccc} 1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ \vdots & & \ddots & \ddots & \vdots \\ & & & 1 & a_{(n-1)n} \\ 0 & 0 & \dots & 0 & 1 \end{array} \right).$$

One can extend the proof of the Proposition 3.6 to show that

$$|X_{(n-1)n}^{a_{(n-1)n}} \dots X_{1n}^{a_{1n}}| \leq n \Rightarrow a_{ij} \leq n^{2^{(j-i)-1}}.$$

Since the bound on each a_{ij} is polynomial, the product of these is also polynomial. Hence, we can find a sufficiently large c such that $\gamma(n) \leq n^c$. □

Using the above examples, one can prove that every finitely-generated virtually nilpotent group is of polynomial growth by showing that one can embed a nilpotent group into one of these matrix groups. A discussion of the details of these proofs would require some knowledge of Lie Algebra and Topology and hence is beyond the scope of this paper.

The First Grigorchuk Group: A Group of Intermediate Growth

The First Grigorchuk Group, which we will denote by $\mathbb{G}$, is the first example of a group that has intermediate growth. This group is generated by elements of the automorphism group of the rooted binary tree. We will begin by describing the rooted binary trees, then constructing the First Grigorchuk group.

4. Rooted Binary Trees

A *rooted binary tree* is an (undirected) tree T with an initial vertex (the root) where every vertex has a left and right child. More formally, the *rooted binary tree* is a a tree $T = (V, E)$ such that the set V of vertices is in bijection with the set of finite 0-1 strings $v = x_1x_2 \dots x_k$ where $x_i \in \{0, 1\}, k \in \mathbb{N}$. For this paper, we will denote each vertex by its corresponding word.

We call the empty string the *root*. There is an edge between two vertices v, v' if $v' = w0, v' = v1$ or vice versa.

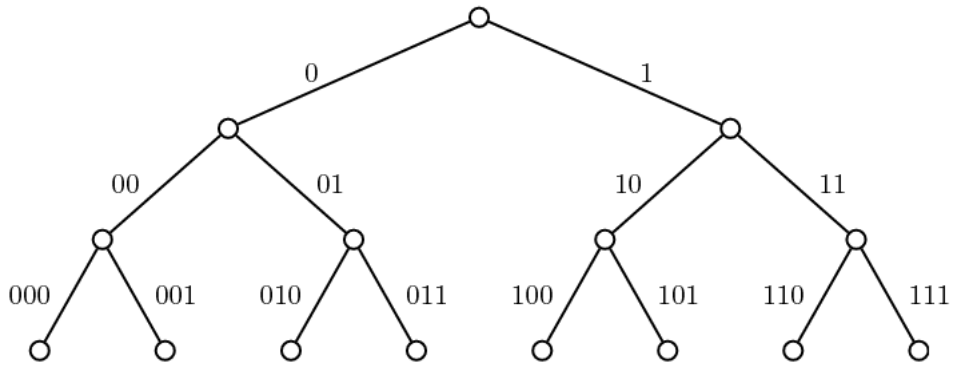

Figure 1. The zeroth to third levels of the Rooted Binary Tree

Notation 4.1. T_v is the subtree of T where we take v as the root. i.e. the set of all words with initial vertex v and their associated edges.

Notation 4.2. The *level* of a vertex is its length. The n-th level of the tree is the set of vertices with word length n.

Definition 4.3. The tree $T(k)$ is the finite subtree of T spanned by the vertices of level at most k. Alternatively, it is the set of all 0-1 strings of k or less length and their associated edges.

Consider the *automorphism group* of the tree $\mathrm{Aut}(T)$. This is the group of bijections φ from V to V such that $(v, v') \in E \Leftrightarrow (\varphi(v), \varphi(v')) \in E$. This means that every automorphism preserves the child-parent relations between vertices and hence, preserves the level of all vertices.

Notation 4.4. A *swap* is an automorphism φ of T where there exists a 0-1 word w such that

$$\varphi(v) = \begin{cases} w\overline{x_1}x_2\ldots & \text{if } v = wx_1x_2\ldots \qquad x_i \in \{0,1\} \\ v & \text{otherwise} \end{cases}$$

where $\overline{x_i} = 1 - x_i$

This paper will frequently mention swaps in the context of exchanging the two child subtrees of a vertex. One can check that every element φ of $\mathrm{Aut}(T)$ is composed of swaps.

Theorem 4.5. *$Aut(T)$ is uncountable.*

Proof. We want to form an injection from the uncountable set of all countably infinite 0-1 strings to $\mathrm{Aut}(T)$. Order all the vertices in ascending length and label them $\{v_1, v_2, \ldots\}$. We map an infinite string $x_1x_2\ldots, x_i \in \{0,1\}$ to the automorphism φ that swaps the two subtrees associated with the children of the i-th vertex if and only if $x_i = 1$, and the swap is only performed only after all the swaps corresponding to $x_j, j < i$ have occurred. Each string corresponds to a unique element in $\mathrm{Aut}(T)$, and since the number of these strings is uncountable, the claim follows. □

We now introduce the concept of *wreath products* of groups to allow us to obtain an upper bound on the index of certain subgroups.

Definition 4.6. Let A, B be two groups and let X be a set that A acts on. Let B^X denote the group of functions from X to B with pointwise product. Then, A acts on B^X by

$$a \cdot (f)(x) = f(a^{-1}x) \text{ for all } a \in A, f \in B^X \text{ and } x \in X$$

The *wreath product* of B by A according to action of A on X is the semi-direct product

$$B \wr_X A = B^X \rtimes A$$

This means that we have

$$(f, a)(f', a') = ((f)(a \cdot f'), aa') \text{ for all } f, f' \in B^X \text{ and } a, a' \in A$$

where

$$((f)(a \cdot f'))(x) = f(x)f'(a^{-1}x)$$

For the purposes of this paper, we only need to consider the wreath product of a group G by $Sym(2)$ with $Sym(2)$ acting on the set $\{0,1\}$. Since $G^{\{0,1\}} \cong G \times G$, we can more clearly state this particular wreath product as follows.

Notation 4.7. Let G be a group. The wreath product $G \wr Sym(2)$ is the semi-direct product $(G \times G) \rtimes Sym(2)$, with $Sym(2)$ acting by swapping the two G.

Definition 4.8. The subgroup $St_T(k)$ of $\mathrm{Aut}(T)$ is the subgroup of all automorphisms that fix any vertex of length $\leq k$.

We can see this as the group of all automorphisms that are composed only of swaps on children of vertices of level k or higher. One can check that these subgroups are normal in T.

Proposition 4.9. *We have*

(1) $T/St_T(1) \cong \mathbb{Z}_2$
(2) $T/St_T(k) \cong (T/St_T(k-1)) \wr \mathbb{Z}_2$
(3) $|T/St_T(k)| = 2^{2^m-1}$

Proof. The group $T/St_T(k)$ is isomorphic to the subgroup of all automorphisms that are only composed of swaps on children of vertices with level $< k$:

$$T/St_T(k) \cong \mathrm{Aut}(T(k))$$

For $k = 1$ the isomorphism is clear. For $k > 1$, one can verify that

$$\mathrm{Aut}(T(k)) \cong (\mathrm{Aut}(T(k-1)) \times \mathrm{Aut}(T(k-1))) \rtimes \mathrm{Sym}(2).$$

since each automorphism in $\mathrm{Aut}(T(k))$ is determined by how it permutes the elements within the subtrees T_0, T_1 and if it swaps the two subtrees.

As a direct consequence, we have $|T/St_T(k)| = 2^{2^m-1}$. □

Here we leave one last exercise for the reader.

Exercise 4.10. $Aut(T) \cong Aut(T) \wr \mathbb{Z}_2$

Hint. Definition 7.1 provides an explicit way of constructing the isomorphism.

5. Construction of the First Grigorchuk Group and Basic Properties

Every automorphism in $St_T(1)$ can be represented by how it acts on the subtrees T_0, T_1. We can denote $\varphi \in St_T(1)$ as (φ_0, φ_1) such that

$$\varphi(v) = \begin{cases} 0\varphi_0(w) & \text{if } v = 0w \\ 1\varphi_1(w) & \text{if } v = 1w \end{cases}$$

where $w \in T$.

We can formally define the above notions as follows:

Notation 5.1. Let $\psi : St_T(1) \to \mathrm{Aut}(T) \times \mathrm{Aut}(T)$ be the map such that $\psi(\varphi) = (\varphi_0, \varphi_1)$ as in the definition above.

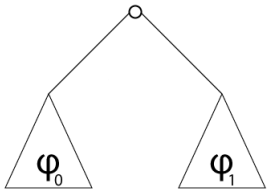

Figure 2. Each $\varphi \in St_T(1)$ can be represented as a pair of automorphisms (φ_0, φ_1)

Construction 5.2. The *First Grigorchuk Group* is the group $\mathbb{G} = \langle a, b, c, d \rangle$, where a, b, c, d are elements of $\mathrm{Aut}(T)$ and

(1) The automorphism a swaps the subtrees T_0 and T_1. This means for a vertex $v = x_1 x_2 \dots x_k$, we have $a(v) = \overline{x_1} x_2 \dots x_k$.
(2) The automorphisms b, c, d are recursively defined by

$$b \to (a, c) \qquad c \to (a, d) \qquad d \to (I, b).$$

Figure 3 provides a graphical representation of these elements. The triangles represent subtrees where we apply a.

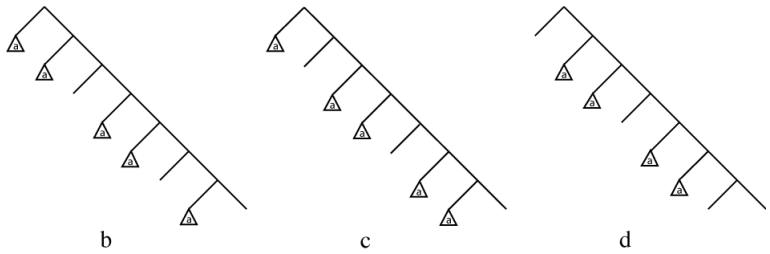

FIGURE 3. The elements $b, c, d \in \mathbb{G}$

Exercise 5.3. b, c, d have order 2.

Exercise 5.4. $bc = cb = d$, $cd = dc = b$ and $bd = db = c$. Hence $\mathbb{G}$ is 3-generated.

Exercise 5.5. The subgroup generated by $b, c, d \in St_T(1)$ is isomorphic to $\mathbb{Z}_2^2$.

Exercise 5.6. $(ad)^4 = (ac)^8 = (ab)^{16} = I$.

Before we can begin to talk about the growth rate of $\mathbb{G}$, we first need to verify that $\mathbb{G}$ is an infinite group.

Notation 5.7. Let $St_{\mathbb{G}}(k)$ denote the subgroup of $\mathbb{G}$ that contains all automorphisms that fix any vertex of length $\leq k$: $St_{\mathbb{G}}(k) = \mathbb{G} \cap St_T(k)$.

Exercise 5.8. Check that every element $g \in St_{\mathbb{G}}(k)$ can be expressed as a 2^k-tuple $(g_{0\dots00}, g_{0\dots01}, \dots, g_{1\dots10}, g_{1\dots11})$ where the subscripts correspond to the vertices of length k, such that:

(1) the automorphism g_v corresponds to how h acts on subtree T_v. i.e. for $w \in T, w = vw'$ for some $v \in T(k)$, we have

$$g(w) = v g_v(w').$$

(2) $g_v \in \mathbb{G}$.

Hint. Use ψ to recursively define how h acts on subtrees of higher levels.

Proposition 5.9. $[\mathbb{G} : St_{\mathbb{G}}(k)] \leq [T : St_T(k)] = 2^{2^k - 1}$

Proof. One can check that $St_{\mathbb{G}}(k)$ is normal in $\mathbb{G}$. The group $\mathbb{G}/St_{\mathbb{G}}(k)$ is isomorphic to a subgroup of $T/St_T(k)$, and our claim follows. □

Notation 5.10. Let $\mathbb{H} = St_{\mathbb{G}}(1)$. This is called the *fundamental subgroup* of $\mathbb{G}$.

Lemma 5.11. *For the fundamental subgroup $\mathbb{H}$, we have*

(1) $[\mathbb{G} : \mathbb{H}] = 2, \mathbb{H} \triangleleft \mathbb{G}$
(2) $\mathbb{H} = \langle b, c, d, aba, aca, ada \rangle$

Proof. The first claim is a direct consequence of Proposition 5.9 and the fact that $\mathbb{H}$ is a proper subgroup of $\mathbb{G}$.

Consider the set of words in $\{a, b, c, d\}$. It follows from the Exercise 5.4 that every word composed of b, c, d only can be reduced to a single letter. So every word w in $\mathbb{G}$ can be reduced to the form $w = x * a * a * \ldots * a * y$ where each $*$ can (independently) be any of $\{b, c, d\}$ and $x, y \in \{I, a\}$. A word w is in $\mathbb{H}$ if and only if the total number of a is even - this is true since the automorphisms swaps 0 and 1 if and only the number of a's is odd.

Note that a word has an even number of a's if and only if it can be expressed in a combination of $*$ and $a * a$, i.e. $w = (a * a) * (a * a) \ldots (a * a) *$. This proves the second claim. □

Lemma 5.12. *The image $\psi(\mathbb{H})$ is a subgroup of $\mathbb{G} \times \mathbb{G}$ such that the projection of $\psi(\mathbb{H})$ onto $\mathbb{G} \times 1$ and $1 \times \mathbb{G}$ are surjective.*

Proof. Firstly, Lemma 5.11 implies that $\psi(\mathbb{H})$ is indeed a subgroup of $\mathbb{G} \times \mathbb{G}$. Then, we have

$$b \to (a, c) \qquad aba \to (c, a)$$
$$c \to (a, d) \qquad aca \to (d, a)$$
$$d \to (1, b) \qquad ada \to (b, 1)$$

Since the projection of $\psi(\mathbb{H})$ onto $\mathbb{G} \times 1$ contains all the generators $(a, 1)$ to $(d, 1)$, it is surjective. The same argument holds for $1 \times \mathbb{G}$. □

Proposition 5.13. $\mathbb{G}$ *is infinite.*

Proof. This is a consequence of the previous lemmas. Since we have a surjective map from a proper subgroup of $\mathbb{G}$ to $\mathbb{G}$, the group must be infinite. □

6. Superpolynomial Growth

The purpose of this section is to prove that $\mathbb{G}$ has superpolynomial growth. In order to do so, we want to show that all *multilateral groups* have superpolynomial growth, then prove that $\mathbb{G}$ itself is multilateral.

Definition 6.1. Let G, H, be groups. We say that G and H are *commeasurable*, denoted by $G \approx H$. if they contain isomorphic subgroups of finite index:

$$G' \subset G, H' \subset H \text{ such that } G' \cong H' \text{ and } [G : G'], [H : H'] < \infty$$

One can check that commeasurability is an equivalence relation.

Example 6.2. Trivial examples of commeasurability include the set of all finite groups are commeasurable (since the trivial group is always a subgroup of finite order) and any group with a subgroup of finite index.

Exercise 6.3. Prove that $\mathbb{Z}$ and $\mathbb{Z}^2$ are *not* commeasurable.

Definition 6.4. A group G is *multilateral* if $|G| = \infty$ and $G \approx G^k$ for some $k \geq 2$.

Lemma 6.5. *(Lower Bound Lemma). Let $f : \mathbb{N} \to \mathbb{R}^+$ be a strictly increasing function such that $\lim_{n\to\infty} f(n) = \infty$. If $f \gtrsim f^m$ for some $m > 1$, then $f(n) \gtrsim \exp(n^\nu)$ for some $\nu > 0$.*

Since this lemma is analytic in nature, we will leave the proof of this to the end of the paper.

Theorem 6.6. *Let G be a group. If G is multilateral, then G has superpolynomial growth.*

Proof. Since G is multilateral, we have $G' \subset G$, $\widetilde{G} \subset G^k$ such that $G' \cong \widetilde{G}$ and $[G : G'], [G^k : \widetilde{G}] < \infty$. By Theorem 1.11, we know that $\gamma_G \sim \gamma_{G'} \sim \gamma_{\widetilde{G}} \sim \gamma_{G^k}$. This means that $\gamma_G \gtrsim \gamma_{G^k} = (\gamma_G)^k$. We can then apply the Lower Bound Lemma. □

Now, all we have left to show is that $\mathbb{G}$ is multilateral. In order to do so, we again make use of the fundamental subgroup $\mathbb{H}$. We already know that $\mathbb{H}$ is of finite index in $\mathbb{G}$. We will be done once we show that the image $\psi(\mathbb{H})$ is a finite index subgroup of $\mathbb{H} \times \mathbb{H}$.

Notation 6.7. We denote by $\mathbb{B}$ the normal closure of b in $\mathbb{G}$:

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

Lemma 6.8. *The index of the normal subgroup $\mathbb{B}$ divides 8.*

Proof. Consider the quotient $\mathbb{G}/\mathbb{B}$. By Exercise 5.4, we know that $\mathbb{G} = \langle a, b, d \rangle$. Under the quotient map, we know that $b \to 1$, and since in $\mathbb{G}$ we have $bc = cb = d$, it follows that the image of c and d are the same. This means $\mathbb{G}/\mathbb{B}$ is generated by the images of a and d, so the order of $\mathbb{G}/\mathbb{B}$ divides $|\langle a, d \rangle|$, which was shown to be 8 in Exercise 5.6. □

Lemma 6.9. $\mathbb{B} \times \mathbb{B} \subset \psi(\mathbb{H}) \subset \mathbb{H} \times \mathbb{H}$.

Proof. From Lemma 5.12, we know that $\psi(\mathbb{H})$ contains the two generators $(1, b)$ and $(b, 1)$. Pick h in $\mathbb{H}$ and let $\psi(h) = (h_0, h_1)$. Then:

$$\begin{aligned} \psi(h^{-1}dh) &= \psi(h^{-1})\psi(d)\psi(h) \\ &= (h_0^{-1}, h_1^{-1}))(I, b)(h_0, h_1) \\ &= (I, h_1^{-1}bh_1) \end{aligned}$$

Since the generators of $\mathbb{H}$ allow us to pick any $h_1 \in \mathbb{G}$, the image $\psi(\mathbb{H})$ contains all the generators of $1 \times \mathbb{B}$. By the same logic, it also contains all the generators of $\mathbb{B} \times 1$. This proves our claim. □

Proposition 6.10. $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$.

Proof. This is the result of a simple calculation. By Lemma 6.8 we have

$$[\mathbb{G} \times \mathbb{G} : \psi(\mathbb{H})] \leq [\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}] = [\mathbb{G} : \mathbb{B}]^2 = 64$$

So we have $[\mathbb{G} \times \mathbb{G} : \psi(\mathbb{H})] < \infty, [\mathbb{G} : \mathbb{H}] < \infty$ (Proposition 4.9) and $\mathbb{H} \cong \psi(\mathbb{H})$, which implies the claim. □

Since $\mathbb{G}$ is infinite, the key result of this section follows immediately.

Corollary 6.11. $\mathbb{G}$ *has superpolynomial growth.*

7. Rewriting Rules

The key concept behind proving that $\mathbb{G}$ has subexponential growth is understanding how one can express elements of $\mathbb{G}$ in terms of words in a, b, c, d and manipulate them. To do so we need to introduce the concept of *rewriting rules*. We begin by extending the domain of our function ψ from $St_T(1)$ to $Aut(T)$.

Definition 7.1. Let $\overline{\psi} : Aut(T) \to Aut(T) \wr Sym(2)$ where

$$\overline{\psi}(\varphi) = \begin{cases} (\psi(\varphi); I) & \text{if } \varphi \in St_T(1) \\ (\psi(\varphi a); \sigma) & \text{otherwise} \end{cases}$$

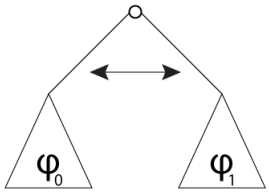

FIGURE 4. Each automorphism of T can be viewed as an element of $Aut(T) \wr Sym(2)$.

Note that the definition of $\overline{\psi}$ allows us to restrict it to $\mathbb{G}$ i.e. $\overline{\psi} : \mathbb{G} \to \mathbb{G} \wr Sym(2)$.

At this point it would be a good exercise for the reader to check that this is indeed an isomorphism by constructing the inverse map.

We now introduce a simple method of obtaining $\overline{\psi}$ for any $g \in \mathbb{G}$. Recall from the proof of lemma 5.10 that we can express every element in G as a word $w = x * a * a * \ldots * a * y$, where each $*$ can be any of $\{b, c, d\}$ and $x, y \in \{I, a\}$.

Construction 7.2. We introduce functions which we will term *rewriting rules*.

(1) $\Phi_0(w)$ is the word formed by the following replacements:
   (a) each a is replaced with I
   (b) for each b, c, d preceded by an **even** number of a's
   $$b \to a, \qquad c \to a, \qquad d \to I$$
   (c) for each b, c, d preceded by an **odd** number of a's
   $$b \to c, \qquad c \to d, \qquad d \to b$$

(2) $\Phi_1(w)$ is the word formed by the following replacements:
   (a) each a is replaced with I
   (b) for each b, c, d preceded by an **even** number of a's
   $$b \to c, \qquad c \to d, \qquad d \to b$$
   (c) for each b, c, d preceded by an **odd** number of a's
   $$b \to a, \qquad c \to a, \qquad d \to I$$

Example 7.3. We will demonstrate a few examples of the rewriting rules.

(1) $w = aba$:

$$\Phi_0(w) = c \qquad\qquad \Phi_1(w) = a$$

(2) $w = abacad$:

$$\Phi_0(w) = cab \qquad \Phi_1(w) = ad$$

Exercise 7.4. Consider $g \in \mathbb{G}$ and let w be a word in a, b, c, d representing g. Then

$$\overline{\psi}(g) = \begin{cases} ((\Phi_0(w), \Phi_1(w)); I) & g \in \mathbb{H} \\ ((\Phi_0(w), \Phi_1(w)); \sigma) & \text{otherwise} \end{cases}$$

Hint. Show that we only need to consider g in $\mathbb{H}$ and prove by induction on the length of g.

Notation 7.5. Consider the word w and a vertex $v \in T$. We recursively define w_v to be the **reduced** word obtained from

(1) $\Phi_0(w_{v'})$, if $v = v'0$.
(2) $\Phi_1(w_{v'})$, if $v = v'1$.

Exercise 7.6. Let $l(g)$ be the length of $g \in \mathbb{H}$. Let $\psi(g) = (g_1, g_2)$, where $g_0, g_1 \in \mathbb{G}$. Then, we have $l(g_v) \leq \frac{1}{2}(l(g) + 1)$. Similarly, for any word w representing an element in $\mathbb{H}$, we have $|w_0| + |w_1| \leq \frac{1}{2}(|w| + 1)$.

As an interesting aside, in 1902 William Burnside asked if a finitely generated group where every element had finite order had to be finite. This problem remained unresolved until 1964, when Golod and Shafarevich constructed a counterexample. One can also show that the First Grigorchuk group is also a counterexample by using the rewriting rules:

Exercise 7.7. Prove by induction on the length of elements that $\mathbb{G}$ is a 2-group: for any $g \in \mathbb{G}$, $|g| = 2^k$ for some $k \in \mathbb{N}$.

Historical and mathematical curiosity out of the way, we now return to our main endeavor.

8. Subexponential Growth

We will proceed to introduce another analytic lemma that would help us obtain our upper bound. This proof is again left for the end of the paper.

Definition 8.1. Let $f : \mathbb{N} \to \mathbb{R}^+$ be a strictly increasing function. We define $f^{\star k}$ by:

$$f^{\star k}(n) = \sum_{n_1 + \ldots + n_k \leq n} f(n_1) \ldots f(n_k)$$

where $n_i \in \mathbb{N}$.

Lemma 8.2. *(Upper Bound Lemma). Let $f : \mathbb{N} \to \mathbb{R}^+$ be a strictly increasing function such that $\lim_{n\to\infty} f(n) = \infty$. If $f(n) \leq Cf^{\star k}(\alpha n)$ for some for some $k \geq 2$ and $0 < \alpha < 1$, then $f(n) \lesssim \exp(n^\beta)$ for some $\beta < 1$.*

Consider an element $g \in St_{\mathbb{G}}(3)$. Recall from Exercise 5.8, that the automorphism g can be expressed as $(g_{000}, g_{001}, \ldots, g_{111})$, where g_v represents how g acts on the subtree T_v and $g_v \in \mathbb{G}$.

Lemma 8.3. *(Rewriting Lemma). Let $g \in St_{\mathbb{G}}(3)$. Given the notion from Exercise 5.8, we have:*

$$l(g_{000}) + l(g_{001}) + \ldots + l(g_{111}) < \frac{5}{6} l(g) + 8$$

Proof. We begin by generalizing Exercise 7.6. Observe that for any v of length ≤ 2,

$$l(g_{v0}) + l(g_{v1}) \leq l(g_v) + 1.$$

This recursively gives us:

$$l(g_{00}) + \ldots + l(g_{11}) \leq l(g_0) + l(g_1) + 2$$
$$l(g_{000}) + \ldots + l(g_{111}) \leq l(g_{00}) + \ldots + l(g_{11}) + 4.$$

Pick a shortest reduced word w representing g. Let $|w|$ represent the length of w and let $|w|_a, |w|_b, |w|_c$ represent the number of a's, b's and c's respectively in the word w. By the rewriting rules, since there are least $\frac{|w|-1}{2}$ many a's in w and every d in w is rewritten as I in either $\Phi_0(w)$ or $\Phi_1(w)$, we have

$$|w_0| + |w_1| \leq |w| + 1 - |w|_d. \tag{8.4}$$

Consider every c in w. Each c gets rewritten as d in $\Phi_0(w)$ or $\Phi_1(w)$. Each of these d's are either removed when we reduce $\Phi_i(w)$ to w_i for $i \in \{0, 1\}$, or are rewritten as I in one of $\Phi_0(w_i)$ or $\Phi_1(w_i)$. This means that

$$|w_{00}| + |w_{01}| + \ldots + |w_{11}| \leq |w| + 3 - |w|_c. \tag{8.5}$$

By the same argument on b, it also follows that

$$|w_{000}| + |w_{001}| + \ldots + |w_{111}| \leq |w| + 7 - |w|_b. \tag{8.6}$$

Applying the result of the second part of Exercise 7.6 to Equations 8.4 and 8.5, we have

$$|w_{000}| + |w_{001}| + \ldots + |w_{111}| \leq |w| + 7 - |w|_d. \tag{8.7}$$
$$|w_{000}| + |w_{001}| + \ldots + |w_{111}| \leq |w| + 7 - |w|_c. \tag{8.8}$$

By combining Equations 8.6, 8.7 and 8.8, we get

$$\sum_{i,j,k \in \{0,1\}} |w_{ijk}| \leq |w| + 7 - \max_{* \in \{b,c,d\}} |w|_*.$$

Since $|w|_b + |w|_c + |w|_d \geq \frac{|w|-1}{2}$, we finally conclude that

$$\begin{aligned}\sum_{i,j,k \in \{0,1\}} l(g_{ijk}) \leq \sum_{i,j,k \in \{0,1\}} |w_{ijk}| &\leq |w| + 7 - \max_{* \in \{b,c,d\}} |w|_* \\ &\leq |w| + 7 - \frac{|w| - 1}{6} \\ &< \frac{5}{6}|w| + 8.\end{aligned}$$

□

Proposition 8.9. *The First Grigorchuk group $\mathbb{G}$ has subexponential growth.*

Proof. Every element $g \in \mathbb{G}$ can be written as $g = u \cdot h$ where $h \in St_{\mathbb{G}}(3)$ and u is a coset representative of $\mathbb{G}/St_{\mathbb{G}}(3)$. By Proposition 5.9, we have $|\mathbb{G}/St_{\mathbb{G}}(3)| \leq 128$, so we have at most 128 such u. Let α be the maximum word length of the u's. The decomposition $h = u^{-1}g$ gives us the inequality

$$l(h) \leq l(g) + \alpha. \tag{8.10}$$

The Rewriting Lemma then gives us

$$\sum_{i,j,k\in\{0,1\}} l(h_{ijk}) < \frac{5}{6}l(h) + 8 \leq \frac{5}{6}(l(g)+\alpha) + 8 = \frac{5}{6}l(g) + \beta \tag{8.11}$$

where $\beta = \frac{5}{6}\alpha + 8$. With Equation 8.11 in mind, we will now count the number of ways we can obtain g of length $\leq n$. For any such g, notice that by Equation 8.10 we are restricted to considering $h \in St_{\mathbb{G}}(3)$ where h has word length $n+\alpha$. Since h is completely determined by $h_{001}, \ldots, h_{111}$, we have:

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

such that (by Equation 8.11):

$$n_1 + \ldots n_8 = \sum l(h_{ijk}) < \frac{5}{6}n + \beta.$$

We want to use the upper bound lemma on our inequalities. In the notation of Definition 8.1, we can rewrite the above two inequalities as

$$\gamma(n) < 128 \cdot \gamma^{\star 8}(\frac{5}{6}n + \beta).$$

Pick a sufficiently large $m = n + c$ such that $\frac{5}{6}n + \beta < \frac{5}{6}m$. This gives us our final inequality:

$$\begin{aligned}\gamma(m) = \gamma(n+c) \leq \gamma(n)\gamma(c) &\leq \gamma(n)\cdot 4^c \\ &\leq 4^c \cdot 128 \cdot \gamma^{\star 8}(\frac{5}{6}n + \beta) \\ &\leq 4^c \cdot 128 \cdot \gamma^{\star 8}(\frac{5}{6}m).\end{aligned}$$

By the Upper Bound Lemma, we have $\gamma(n) \leq \exp(n^i)$ for some $i < 1$, proving our claim. □

Finally, we prove the main result of the second half of the paper. Since the growth rate of $\mathbb{G}$ is both superpolynomial (Corollary 6.11) and subexponential (Proposition 8.9), it follows directly that:

Corollary 8.12. *The First Grigorchuk group $\mathbb{G}$ has intermediate growth.*

9. Proof of Upper and Lower Bound Lemmas

We will now prove Lemmas 6.4 and 7.8 using analytic methods.

Proposition. *(Lower Bound Lemma). Let $f : \mathbb{N} \to \mathbb{R}^+$ be a strictly increasing function such that $\lim_{n\to\infty} f(n) = \infty$. If $f \gtrsim f^m$ for some $m > 1$, then $f(n) \gtrsim \exp(n^\nu)$ for some $\nu > 0$.*

Proof. Suppose f satisfies $f \gtrsim f^m$. Then for some $C, \alpha > 0$, we have $f(n) \geq C \cdot f^m(\alpha n)$. Without loss of generality, we suppose that $f(e) \geq e$. We will need this later in the proof.

We begin by extending f to the positive real line by letting $f(x) = f(\lfloor x \rfloor)$. Let $g : \mathbb{R}^+ \to \mathbb{R}$ be defined as $g(n) = \ln(f(n))$. The function g is a monotone increasing function which satisfies

$$g(n) \geq c + m \cdot g(\alpha n) \tag{9.1}$$

where $c = \ln C$.

We can show that $\alpha < 1$. Suppose for contradiction that $\alpha \geq 1$. Then, Equation 9.1 gives us:

$$-c \geq m \cdot g(\alpha n) - g(n) > m \cdot g(n) - g(n) = (m-1)g(n) \to \infty$$

as $n \to \infty$. This is a contradiction. So $\alpha < 1$, which means that for any $k \in \mathbb{N}$ we have $0 < \alpha^k < 1$.

We can now reiterate the inequality in Equation 9.1 to get:

$$\begin{aligned} g(n) &\geq c + m \cdot g(\alpha n) \\ &\geq c + m(c + m \cdot g(\alpha^2 n) \\ &\vdots \\ &\geq c(1 + m + \ldots + m^{k-1}) + m^k \cdot g(\alpha^k n), \end{aligned}$$

where $\alpha^k n < n$.

We need to consider the cases where $c \geq 0$ and $c < 0$. Suppose $c \geq 0$. We take k to be $\lfloor \ln n - 1/\ln(\frac{1}{a}) \rfloor$. By change of bases for logarithms, we have

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

This means that

$$\begin{aligned} g(n) \geq m^k &\geq m^{((\ln n - 1)/\ln(1/\alpha)) - 1} \\ &= m^{-1} \cdot (m^{\ln n} m^{-1})^{1/\ln(1/\alpha))} \\ &= m^{(1/\ln \alpha) - 1} \cdot (m^{\ln n})^{1/\ln(1/\alpha))} \\ &= m^{(1/\ln \alpha) - 1} \cdot (n^{\ln m})^{1/\ln(1/\alpha))}. \end{aligned}$$

For the case where $c < 0$, note that $g(n) \geq m^k(g(\alpha^k n) + c)$. We take k to be $\lfloor (\ln n) + c - 1/\ln(\frac{1}{a}) \rfloor$. Repeating the same process as above, we obtain

$$g(\alpha^k n) + c = \ln(\alpha^k n) + c \geq \ln(e) - c + c = 1$$

and

$$g(n) \geq m^k \geq m^{c/\ln \alpha} \cdot (n^{\ln m})^{1/\ln(1/\alpha))}.$$

In both cases, we have $f(n) = \exp(g(n)) \geq \exp(A \cdot n^\nu)$ for some $A, \nu > 0$, which proves the claim. □

Proposition. *(Upper Bound Lemma). Let $f : \mathbb{N} \to \mathbb{R}^+$ be a strictly increasing function such that $\lim_{n\to\infty} f(n) = \infty$. If $f(n) \leq Cf^{\star k}(\alpha n)$ for some $k \geq 2$ and $0 < \alpha < 1$, then $f(n) \lesssim \exp(n^\beta)$ for some $\beta < 1$.*

Proof. Suppose $f(n) \leq Cf^{\star k}(\alpha n)$ for some $k \geq 2$ and $0 < \alpha < 1$. We will prove using induction on n that $f(n) \leq A \cdot n^\nu$ for some $A > 0$ and $0 < \nu < 1$.

We begin by choosing ν. Notice that as $\nu \to 1$ we have $k(\frac{\alpha}{k})^\nu \to \alpha$. This means that we can pick ν such that $k(\frac{\alpha}{k})^\nu < 1$.

For $n = 0$, we can find $A > 0$ such that

$$f(0) \leq A \cdot \exp(0) = A. \tag{9.2}$$

Suppose the induction statement holds for all $n' < n$. By our initial assumption, we have

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

where $n_1 + \ldots + n_k \leq \alpha n$. Note that the number of terms in this summation is at most $(\alpha n)^k$ and each $n_i < n$. Let $g(n) = \ln f(n)$. For each term in our summation we have (by inductive hypothesis) that:

$$\begin{aligned}\ln(f(n_1)\ldots f(n_k)) &\leq g(n_1) + \ldots + g(n_k)\\ &\leq A(n_1^\nu + \ldots n_k^\nu)\\ &\leq A \cdot k\left(\frac{\alpha n}{k}\right)^\nu\\ &\leq A \cdot n^\nu \cdot \left(k\left(\frac{\alpha}{k}\right)^\nu\right)\end{aligned}$$

By our choice of ν, we can write $k(\frac{\alpha}{k})^\nu = 1 - \epsilon$ for some $\epsilon > 0$. It follows that

$$\begin{aligned}g(n) = \ln f(n) &\leq c + \ln(\alpha n)^k + A \cdot n^\nu \cdot (1-\epsilon)\\ &\leq (c + k\ln\alpha + k\ln n) + A \cdot n^\nu \cdot (1-\epsilon).\end{aligned}$$

For any A, given a sufficiently large n, we have $k\ln n < A\epsilon \cdot n^\nu$. This means that we can pick A such that

$$(c + k\ln\alpha + k\ln n) + A \cdot n^\nu \cdot (1-\epsilon) \leq A \cdot n^\nu \tag{9.3}$$

Finally, we can choose a large A to satisfy both Equations 9.2 and 9.3. This proves the inductive step. □

Acknowledgments

It is my pleasure to thank my mentor Khalid Bou-Rabee for suggesting this project and provide much valuable advice. I also thank Peter May for organizing the 2009 VIGRE REU program at the University of Chicago.

References

[1] R. Grigorchuk and I. Pak, *Groups of Intermediate Growth: an Introduction for Beginners.* Pre-print. arXiv:math/0607384v1. 2006.

[2] P. de la Harpe, *Topics in geometric group theory.* University of Chicago Press. 2000.