The First Grigorchuk Group and its Applications to Group-based Cryptography

Flora Golda Kiss

Bachelor's thesis
2026:K14

Lund University

Faculty of Science
Centre for Mathematical Sciences
Mathematics

Centrum Scientiarum Mathematicarum

Abstract

In this thesis, we study groups of superpolynomial growth, with a particular focus on the first Grigorchuk group. Introduced by Rostislav Grigorchuk in 1980, this group serves as a fundamental example of a finitely generated group of intermediate growth.

The main result concerns the superpolynomial growth of the first Grigorchuk group, illustrating its relevance for the conjugacy search problem as an application to group-based cryptography. This result contributes to understanding the connection between the growth rate of groups and algorithmic complexity required for public-key cryptographic protocols, which is briefly discussed here.

Popular scientific summary

Group theory can be regarded as the mathematical language for describing and measuring symmetry. Symmetry is defined as the property of an object to remain unchanged under certain transformations, and *groups* provide a natural way to study such transformations algebraically. The structure of a group is quite simple: take a set, and allow one operation on the elements of the set, such that they satisfy certain axioms. Despite this simplicity, groups are one of the fundamental structures in pure mathematics, but they play an important role in other physical sciences as well. For example, in chemistry symmetry is used to classify molecules by their shape, in physics group theory is applied in quantum mechanics and in biology it is used in molecular systems. Last but not least, public-key cryptography relies on group theory, specifically finite groups.

Now, what is public-key cryptography? Also known as asymmetric cryptography, this is a method of encrypting or signing data with a pair of mathematically related keys, a public key for encryption and a private key for decryption. It enables secure communication without requiring a shared secret key beforehand, as the public key can be openly distributed. Until the introduction of the asymmetric public-key cryptography in 1976, symmetric cryptography (where both parties need the same private key) was the dominant method for secure communication.

As a concrete example of cryptography, think of online banking, digital signatures, authentication protocols, or any similar process when information must be transferred safely - and to do this, information is encrypted through some algorithm, often based on mathematical problems that are easy to perform computationally but difficult to reverse without additional information. To ensure that the encryption process is as safe as possible, some mathematicians have come up with certain criteria regarding the elements (numbers, or even functions) used during the encryption of the data. One criteria concerns the so-called *growth rate* of the group from which these elements are taken from. In particular, the first Grigorchuk group is one which was shown to satisfy this growth requirement. What this means in practice is that considering this group as a basis for the encryption algorithm would possibly give a secure way to transfer data.

The purpose of this thesis is to study the growth rate of the first Grigorchuk group, and to discuss its relevance for some protocols in group-based cryptography.

Acknowledgements

I would like to thank all of my teachers and fellow students who have taught and inspired me throughout my studies. In particular, I would like to thank my advisor Anitha Thillaisundaram for her guidance and valuable advice.

I would also like to thank my friends and family for their encouragement during the writing process, and for pushing me to explain complicated concepts in a much more accessible way. A special thanks goes to my fiancé Raz for his constant support and for always being there to listen.

Contents

Chapter 1

Introduction

Symmetric cryptography was the dominant method for secure communication until the introduction of the (asymmetric) public-key cryptography in 1976, specifically with the Diffie-Hellman key exchange [1]. Since then, many widely used public-key cryptosystems, such as RSA, have relied on the infeasibility of certain problems from number theory. These problems can naturally be formulated in the context of algebraic structures, including finite abelian groups.

This connection has motivated the study of algebraic methods in cryptography, leading to the development of group-based cryptographic protocols. An early example is the Wagner-Magyarik cryptosystem (1984), which makes use of the computational complexity of the word problem in finitely presented groups. More generally, recent approaches have focused on so-called decision and search problems from combinatorial group theory, such as the word and conjugacy problems, particularly in non-abelian groups. These developments highlight the relevance of algorithmic questions in group theory, which serves as a general background motivation of this thesis.

In parallel with these algorithmic questions, another important way to study groups is through their growth properties. Since the 1960s, the study of growth in finitely generated groups has revealed a range of possible asymptotic behaviors, from polynomial to exponential. It remained unknown for many years whether groups having intermediate (that is, faster than polynomial but slower than exponential) growth existed, until the first example of a finitely generated group of intermediate growth was constructed in 1980 by Rostislav Grigorchuk [3].

In Chapter 2 we begin by introducing the necessary preliminaries from group theory, including basic definitions, group presentations, and algorithmic problems such as the word and conjugacy problems. In particular, we examine the conjugacy search problem and discuss the potential relevance of the first Grigorchuk group as a platform for a secure public-key cryptographic protocol. This group has solvable word problem, highly nontrivial structure and superpolynomial growth, as we will see later on.

In Chapter 3 we first study growth in groups, then introduce the first Grigorchuk group $\mathbb{G}$ via its action on the binary rooted tree and look into some of the group's structural properties. In particular, we show here that $\mathbb{G}$ is an infinite group.

Finally, Chapter 4 is devoted to the analysis of the growth of the first Grigorchuk group, culminating in the proof that it has superpolynomial growth. For this proof, we first show that all multilateral groups have superpolynomial growth, and then prove that $\mathbb{G}$ is multilateral.

Chapter 2

Preliminaries

In this chapter, we closely follow [9, Sections 2.1-2.3.2, 4.1].

2.1 Basic definitions and notation

For a group G, write $H \leq G$ if H is a subgroup of G, and $H \trianglelefteq G$ if H is normal in G. For a subset $A \subseteq G$, denote by $\langle A \rangle$ the subgroup of G generated by A. More explicitly,

$$\langle A \rangle = \{a_{i_1}^{\varepsilon_1} \cdots a_{i_n}^{\varepsilon_n} \mid a_{i_j} \in A, \varepsilon_j \in \{1, -1\}, n \in \mathbb{N}\}.$$

Given an arbitrary set X, a *word* w in X is a finite (and possibly empty) sequence of elements, written as $w = y_1 \cdots y_n$, with $y_i \in X$. The integer n corresponds to the *length* of the word w, denoted by $|w|$. We write ε for the empty word, with $|\varepsilon| = 0$.

Also, put $X^{-1} = \{x^{-1} \mid x \in X\}$, where x^{-1} is simply a formal expression obtained from x and -1. For each $x \in X$, the symbols x and x^{-1} are said to be *literals* in X. The set of all literals in X is denoted by $X^{\pm 1} = X \cup X^{-1}$.

An expression of the form $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$, where $x_{i_j} \in X$, $\varepsilon_j \in \{1, -1\}$ is called a *group word* in X. In other words, a group word in X is just a word in the alphabet $X^{\pm 1}$.

A group word $w = y_1 \cdots y_n$ is said to be *reduced* if for any $i = 1, \ldots, n-1$, $y_i \neq y_{i+1}^{-1}$, that is, w does not contain a subword of the form yy^{-1} for any literal $y \in X^{\pm 1}$. By convention, the empty word ε is reduced.

If $X \subseteq G$, then every group word $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ in X determines a unique element of G, given by the product $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ of the elements $x_{i_j}^{\varepsilon_j} \in G$. By convention, the empty word ε determines the identity element $1 \in G$.

Definition 2.1.1. A group G is called a *free group* if there is a generating set X of G such that every nonempty reduced group word in X defines a nontrivial element of G.

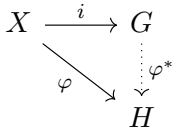
In this case X is called a *free basis* of G, and G is said to be the *free group on* X, or the *group freely generated by* X, and we denote it by $F(X)$. It follows from the definition that every element of a free group $F(X)$ on X can be defined by a reduced group word in X. Moreover, different reduced words in X define different elements of G.

We have the following *universal property* for free groups:

Theorem 2.1.2. *Let G be a group with a generating set $X \subseteq G$. Then G is free on X if and only if the following universal property holds: every map $\varphi : X \to H$ from X into a group H can be extended to a unique homomorphism*

$$\varphi^* : G \to H,$$

so that the diagram below is commutative:



where $X \xrightarrow{i} G$ is the natural inclusion of X into G.

Corollary 2.1.3. *Let G be a free group on X. Then the identity map $X \to X$ extends to an isomorphism $G \to F(X)$.*

This corollary makes it possible to identify a free group freely generated by X with the group $F(X)$ of reduced group words in X.

2.2 Presentation of groups

Using the universal property of free groups, it is possible to describe arbitrary groups in terms of *generators* and *relators*, as follows.

Let G be a group with a generating set X. By the universal property of free groups, there exists a homomorphism $\psi : F(X) \to G$ such that $\psi(x) = x$ for $x \in X$. It follows that ψ is onto, so by the first isomorphism theorem,

$$G \cong F(X)/\ker(\psi).$$

In this case any group word $w \in \ker(\psi)$ is called a *relator* of G in generators X, and $\ker(\psi)$ is viewed as the set of relators of G. If a subset $R \subseteq \ker(\psi)$ generates $\ker(\psi)$ through normal closure in G, then R is called a set of *defining relators* of G relative to X.

Definition 2.2.1. The pair $\langle X \mid R \rangle$ is called a *presentation* of a group G, and it determines G uniquely up to isomorphism. The presentation $\langle X \mid R \rangle$ is said to be $finite$, if both sets X and R are finite.

More generally, a group is *recursively presented* if it admits a presentation $\langle X \mid R \rangle$ where X is finite and the set of relators R is recursively enumerable, that is, there exists an algorithm which lists all elements of R.

Presentations provide a universal method to describe groups, and a group is *finitely presented* if it admits at least one finite presentation. Clearly, every finitely presented group is recursively presented, but there are recursively presented groups that cannot be finitely presented. Recursive presentations play an important role in algorithmic group theory, particularly in the study of decision problems such as the word problem and conjugacy problem, as we will see in the next section.

Example 2.2.2. The free groups $F(X)$ for finite set X are finitely presented groups. For instance, the free group on two generators may be written as

$$F_2 = \langle a, b \mid \emptyset \rangle = \langle a, b \rangle,$$

where the empty set of relators indicates that no relations are imposed on the generators. This is due to the fact that for a free group, there are absolutely no relations other than the ones required by the basic group axioms.

Another important example is given by all finitely generated abelian groups - a group G is *abelian*, if $ab = ba$ for all $a, b \in G$. For instance,

$$\mathbb{Z}^2 = \langle a, b \mid ab = ba \rangle = \langle a, b \mid aba^{-1}b^{-1} = 1 \rangle;$$

$$\mathbb{Z}/n\mathbb{Z} = \langle a \mid a^n = 1 \rangle;$$

$$V_4 = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle : \text{the Klein four-group.}$$

More generally, every finitely generated abelian group admits a finite presentation.

Presentations may also describe non-abelian groups. For example, the dihedral group of order 8,

$$D_8 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle,$$

represents the symmetries of a square, where a corresponds to rotation and b to reflection.

2.3 Algorithmic problems in group theory

Symmetric cryptography was the only existing method for transmission of encoded information until 1976, when W. Diffie and M. Hellman introduced a new approach [1], leading to today's public-key cryptography. Symmetric cryptography uses a single (private) key for the encryption and decryption of messages, which also means that the same algorithm is used for both encoding and decoding information.

On the other hand, public-key (or asymmetric) cryptography relies on a so-called one-way function f for encryption: this is a function such that it is easy to compute the value of $f(x)$ for each argument x in the domain of f, but it is very hard to compute the value of $f^{-1}(y)$ for most y in the range of f. The most celebrated one-way function gave rise to the RSA protocol, which is one of the most common public-key cryptosystem in use today. The efficacy of this protocol depends on the complexity of the abelian group $\mathbb{Z}$.

The idea of using the complexity of infinite non-abelian groups in cryptography emerged in 1985 with the proposal of the Wagner-Magyarik cryptosystem, a public-key protocol based on the presumed unsolvability of the word problem for finitely presented groups. More recently, there has been an increased interest in applications of non-abelian group theory to cryptography.

Most suggested protocols are based on search problems, which are variants of more traditional decision problems of combinatorial group theory. Protocols based on search problems fit in with the general paradigm of a public-key protocol based on a one-way function, while decision problems allow to construct cryptographic protocols with new properties.

The algorithmic problems in group theory considered in this section fall into two categories:

(i) *Decision problems*: given a property $\mathcal{P}$ and an object $\mathcal{O}$, determine whether or not the object $\mathcal{O}$ has the property $\mathcal{P}$.

(ii) *Search problems*: given a property $\mathcal{P}$ and the information that there are objects with the property $\mathcal{P}$, find at least one particular object with the property $\mathcal{P}$.

We now proceed by discussing some particular algorithmic problems in group theory which have applications in non-commutative cryptography.

2.3.1 The word problem

> The *word problem* (WP) is as follows: given a recursive presentation of a group G and an element $g \in G$, find out whether or not $g = 1$ in G.

It is clear from the formulation of the word problem that it naturally splits into two cases, corresponding to whether the answer is affirmative or negative, which we refer to as the "yes" and "no" parts of the word problem. For a group given by a recursive presentation in terms of generators and relators, the "yes" part of the word problem has a recursive solution, as follows.

Proposition 2.3.1. *Let $\langle X \mid R \rangle$ be a recursive presentation of a group G. Then the set of all words $g \in G$ such that $g = 1$ in G is recursively enumerable.*

> The *word search problem* (WSP) is as follows: given a recursive presentation of a group G and an element $g = 1$ in G, find a representation of g as a product of conjugates of defining relators and their inverses.

Note that the word search problem always admits a recursive solution, since one can recursively enumerate all products of defining relators, their inverses and their conjugates.

However, the number of factors in such a product required to express a word w of length n representing the identity 1 in G, may be extremely large compared to n. In particular, there exist groups G with efficiently *solvable word problem*, such as the Grigorchuk groups [3].

Moreover, if the word problem is *recursively unsolvable* in a group G, then the length of any proof verifying that $w = 1$ in G can not bounded by any recursive function $f(|w|)$ of the length of w, since otherwise the word problem would admit a solution.

2.3.2 The conjugacy problem

> The *conjugacy problem* (CP) is as follows: given a recursive presentation of a group G and two elements $g, h \in G$, find out whether or not there is an element $x \in G$ such that $x^{-1}gx = h$.

Analogously to the word problem, the conjugacy problem can be divided into "yes" and "no" parts. The "yes" part is always recursive, since it is possible to systematically enumerate all conjugates of a given element.

> The *conjugacy search problem* (CSP) is as follows: given a recursive presentation of a group G and two conjugate elements $g, h \in G$, find a particular element $x \in G$ such that $x^{-1}gx = h$.

As previously mentioned, the conjugacy search problem is always recursively solvable, as all conjugates of a given element can be enumerated. However, as in the case of the word search problem, this approach can be extremely inefficient.

2.4 Protocols based on the conjugacy search problem

Let G be a group with solvable word problem. For $w, a \in G$, the notation w^a stands for $a^{-1}wa$. Rephrasing then the *conjugacy decision problem* for G, we have the following: given two elements $u, v \in G$, find out whether there is $x \in G$ such that $u^x = v$.

Similarly, the rephrased *conjugacy search problem* is as follows: given two elements $a, b \in G$ and the information that $a^x = b$ for some $x \in G$, find at least one particular element x like that.

The conjugacy decision problem is of fundamental importance in group theory, while the conjugacy search problem is mainly relevant from the perspective of complexity theory. Indeed, if you know that a is conjugate to b, you can try to find a conjugating element x by simply going over words of the form a^x and checking whether $a^x = b$, until you get a match. This approach relies on the observation that solvability of the conjugacy problem implies solvability of the word problem in the given group.

However, this straightforward algorithm is at least exponential-time in the length of b, and is therefore considered infeasible for practical purposes. So if no other algorithm is known for the conjugacy search problem in a group G, then the map $x \mapsto a^x$ can reasonably be treated as a one-way function, and used as the foundation to build a (public-key) cryptographic protocol.

Key establishment protocols are ways for two parties, traditionally called Alice and Bob, to establish a common secret key without any prior arrangement. We begin with a simple protocol, due to Ko, Lee et al. [6, Section 3.2], who suggested a non-abelian version of the Diffie-Hellman key agreement system [1]:

1. An element $w \in G$ is published.
2. Alice picks a private $a \in G$ and sends w^a to Bob.
3. Bob picks a private $b \in G$ and sends w^b to Alice.
4. Alice computes $(w^b)^a = w^{ba}$, and Bob computes $(w^a)^b = w^{ab}$.

If a and b are chosen from commuting subset of the group G, then $ab = ba$, and therefore, Alice and Bob both obtain a common private key $w^{ab} = w^{ba}$. In practice, this is implemented by taking two public subgroups A and B of the group G, each given by a (finite) generating sets, such that $ab = ba$ for any $a \in A$, $b \in B$.

Determining a suitable platform group for the above protocol is a very nontrivial problem. Some requirements on such a group were outlined in [11, Section 6]:

(P1) The word problem in G should have a fast (linear- or quadratic-time) solution by a deterministic algorithm. Better yet, there should be an efficiently computable "normal form" for elements of G.

This is necessary to enable efficient derivation of a shared secret key between legitimate participants in a key establishment protocol, or for the verification step in an authentication protocol.

(P2) The conjugacy search problem should *not* have a subexponential-time solution by a deterministic algorithm. Moreover, the group has to be well known, that is, the conjugacy search problem in the group either has to be well studied or can be reduced to a well-known problem - perhaps, in some other area of mathematics.

Note that *proving* a group to have (P2) would be extremely difficult, if not impossible. This property needs therefore to be considered together with the second point, i.e. the only realistic evidence of a group G having the property (P2) can be the fact that sufficiently many people have been studying the conjugacy search problem in G over a sufficiently long time.

(P3) There should be a way to disguise elements of G so that it would be impossible to recover x from $x^{-1}wx$ just by inspection.

One way to achieve this is to have a *normal form* for elements of G. This usually means that there is an algorithm that transforms any input u_{in} into an output u_{out}, where both u_{in} and u_{out} are words in the generators of G, such that $u_{in} = u_{out}$ in G, but this is hard to detect by inspection.

In the absence of a normal form, say if G is just given by means of generators and relators without any additional information about properties of G, then at least some of these relations should be very short.

(P4) The group G should be a group of superpolynomial growth, i.e. exponential or "intermediate" growth. This means that the number of elements of length n in G should grow faster that any polynomial in n - this is needed to prevent attacks by complete exhaustion of the key space.

Here, "length n" is typically just the length of a word representing a group element, but in a more general situation this could be the length of some other description, i.e. "information complexity".

There are groups that have (P1) and (P4), most likely have (P2), and to a reasonable extent have (P3). These are groups with solvable word problem but unsolvable conjugacy problem. However, since the conjugacy search problem is of no independent interest in group theory, it has received little attention once the conjugacy problem was shown to be algorithmically unsolvable. In the context of cryptography however, where computational complexity is desirable, such groups may provide suitable platforms and therefore deserve renewed attention.

A possible candidate proposed in [10] is the first Grigorchuk group, which has solvable word problem satisfying (P1), as first observed in [3], superpolynomial growth satisfying (P4), and highly nontrivial structure, as we will see later in this thesis. However, subsequent work has shown that the conjugacy search problem in the first Grigorchuk group can in fact be solved in polynomial time [8], and consequently, the group is no longer regarded as a promising candidate for the cryptographic protocol described above, which relies on the complexity of the conjugacy search problem (P2).

Nevertheless, the first Grigorchuk group remains of significant mathematical interest as the first known example of a finitely generated group of intermediate growth. This thesis is focused on the growth properties of the group and the proof of its superpolynomial growth, while the cryptographic discussion serves primarily as motivation and historical context.

Chapter 3

Growth of groups and the first Grigorchuk group

It has been known since the 1960s that all finitely generated groups have either polynomial or exponential growth, but it remained uncertain whether groups of intermediate growth existed. The first such examples were only constructed in 1980 by Rostislav Grigorchuk [3].

In this chapter we start by introducing some concepts about the growth rate of groups, and then the binary rooted tree, in order to construct the first Grigorchuk group. All groups mentioned here are assumed to be finitely generated, unless stated otherwise.

3.1 Growth rate of groups

Definition 3.1.1. Consider a group G and a generating set $S = \{s_1, s_2, \dots, s_k\}$. 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.

Example 3.1.2. A trivial example is given by the group $G = \mathbb{Z}$, which has generating set $S = \{1\}$. Then $l_S(m) = |m|$ for any $m \in \mathbb{Z}$, and so it follows that

$$\gamma_G^S(n) = |\{m \in \mathbb{Z} \mid |m| \leq n\}| = |\{-n, -(n-1), \dots, -1, 0, 1, \dots, n-1, n\}| = 2n + 1.$$

Next, consider the group $G' = \mathbb{Z}^2$ with generating set $S' = \{(1,0), (0,1)\}$. Every element $(a,b) \in \mathbb{Z}^2$ may be written as $(a,b) = (1,0)^a (0,1)^b$, with word length $l_{S'}((a,b)) = |a| + |b|$. Hence,

$$\gamma_{G'}^{S'}(n) = \left|\{(a,b) \in \mathbb{Z}^2 \mid |a| + |b| \leq n\}\right| = 2n^2 + 2n + 1.$$

Remark 3.1.3. It is important to distinguish between the *word length* $l(g)$ of an element g and the length $|w|$ of the word w representing g. In general, the word w need not be the shortest decomposition of g, and therefore it follows that $|w| \geq l(g)$.

Proposition 3.1.4 (Basic properties of word lengths and growth functions)**.** [4, Exercises 1.1, 1.2]

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

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

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

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

(iii) *The word length l_S is subadditive and the 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 $m, n \geq 1$:

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

Proof. (i) An element $g \in G$ with word length $l_S(g) \leq n$ can be represented by a word of length at most n in the alphabet $S \cup S^{-1} = \{s_1^{\pm 1}, \ldots, s_k^{\pm 1}\}$, having $2k$ letters since $|S| = k$. So for a fixed length i, there are exactly $(2k)^i$ words of length i in this alphabet.

However, not all of these correspond to distinct elements of G, so every element $g \in G$ with $l_S(g) = i$ is represented by at least one such word. Hence the number of group elements with word length $\leq n$ is at most the total number of words of length $\leq n$, proving the statement.

(ii) If $\gamma_G^S(n+1) = \gamma_G^S(n)$, then equivalently

$$|\{g \in G \mid l_S(g) \leq n+1\}| = |\{g \in G \mid l_S(g) \leq n\}|.$$

This would imply that multiplying the elements of $\{g \in G \mid l_S(g) \leq n\}$ by generators does not produce any new elements, which would contradict the fact that S generates G unless $\{g \in G \mid l_S(g) \leq n\} = G$. Therefore, each step adds at least one new element, until the whole group is reached.

(iii) Let $g_1 = s_{i_1}^{\pm 1} \cdots s_{i_m}^{\pm 1}$ and $g_2 = s_{j_1}^{\pm 1} \cdots s_{j_n}^{\pm 1}$ be shortest decompositions, so $m = l_S(g_1)$ and $n = l_S(g_2)$. Then $g_1 g_2 = s_{i_1}^{\pm 1} \cdots s_{i_m}^{\pm 1} s_{j_1}^{\pm 1} \cdots s_{j_n}^{\pm 1}$ is a decomposition of $g_1 g_2$ of length $m+n$. Now since $l_S(g_1 g_2)$ is the shortest such decomposition, it follows that $l_S(g_1 g_2) \leq l_S(g_1) + l_S(g_2)$, as required.

Every element g with length $l_S(g) \leq m+n$ can be written as a product $g = g_1 g_2$ where $l_S(g_1) \leq m$ and $l_S(g_2) \leq n$ - taking the shortest word for g and splitting it after the first m letters. Hence

$$B(m+n) \subseteq B(m) \cdot B(n), \text{ where } B(r) = \{g \in G \mid l_S(g) \leq r\}.$$

Taking cardinalities, $\gamma_G^S(m+n) = |B(m+n)| \leq |B(m)|\,|B(n)| = \gamma_G^S(m)\gamma_G^S(n)$. □

We proceed by introducing terms and definitions required for classifying groups according to their growth rates.

Definition 3.1.5. Let f and g be functions from $\mathbb{N}$ to $\mathbb{R}^+$. We say that f *dominates* g, denoted by $g \lesssim f$, if there exist constants $\alpha, C > 0$ such that

$$g(n) \leq C \cdot f(\alpha n) \text{ for all } n \geq 0.$$

Furthermore, we say that f and g are *equivalent*, written as $f \sim g$, if both $f \lesssim g$ and $g \lesssim f$.

It can be verified that this notion of equivalence of growth is an equivalence relation. Indeed, we check that the relation $\sim$ satisfies reflexivity, symmetry and transitivity for all functions $f, g, h : \mathbb{N} \to \mathbb{R}^+$, as follows.

To show that $f \sim f$, we simply take $\alpha = 1, C = 1$. Then $f(n) \leq 1 \cdot f(1 \cdot n)$ clearly holds for all $n \geq 0$, hence $f \lesssim f$. Since this holds in both directions trivially, it follows that $f \sim f$.

To show symmetry, suppose $f \sim g$. By definition, this means $f \lesssim g$ and $g \lesssim f$, and so clearly $g \sim f$, since these conditions are symmetric in f and g.

Finally for transitivity, suppose $f \sim g$ and $g \sim h$. Then again from the definition we have that $f \lesssim g$, so there exist α_1, C_1 such that $f(n) \leq C_1 \cdot g(\alpha_1 n)$ for all $n \geq 0$. Similarly, $g \lesssim h$ implies that there are α_2, C_2 such that $g(n) \leq C_2 \cdot h(\alpha_2 n)$ for all $n \geq 0$. Now substituting, we obtain the following:

$$f(n) \leq C_1 \cdot g(\alpha_1 n) \leq C_1 C_2 \cdot h(\alpha_2 \alpha_1 n) \quad \forall n \geq 0,$$

which implies that $f(n) \leq C \cdot h(\alpha n) \quad \forall n \geq 0$, where $C = C_1 C_2, \alpha = \alpha_1 \alpha_2$. Hence $f \lesssim h$. Similarly, since $h \lesssim g$ and $g \lesssim f$, it follows that $h \lesssim f$. Therefore $f \sim h$, proving transitivity of the relation $\sim$. We can therefore conclude that the equivalence of growth $\sim$ is indeed an equivalence relation.

Proposition 3.1.6. [4, Exercise 1.3] [7, Proposition 1.3] *Given finite generating sets S and S' of a group G, their respective growth functions γ_G^S and $\gamma_G^{S'}$ are equivalent.*

Proof. Let $S = \{s_1, s_2, \ldots, s_k\}$ and $S' = \{s'_1, s'_2, \ldots, s'_l\}$. Since S is a generating set of G, all elements of S' and their inverses can be expressed as words in $S \cup S^{-1} = \{s_1, \ldots, s_k, s_1^{-1}, \ldots, s_k^{-1}\}$. Set α to be the length of the longest such word. Then

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

from which it follows that $\gamma_G^{S'}(n) \lesssim \gamma_G^S(\alpha n)$.

Following the same argument we have $\gamma_G^S(n) \lesssim \gamma_G^{S'}(\alpha' n)$ for some α'. Hence $\gamma_G^S \sim \gamma_G^{S'}$, concluding the proof. □

Since we have seen in the above proposition that the growth of a group G is invariant under the choice of its generating set, in the following we will simplify the notation by occasionally omitting the superscript S from γ_G^S. If no ambiguity arises around the choice of G, then the subscript G will be omitted as well.

Definition 3.1.7. 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 $\gamma(n) \gtrsim e^n$.

It follows from Proposition 3.1.6 that we can speak of *groups with polynomial* and *exponential growth*. As seen in Example 3.1.2, the group $\mathbb{Z}^2$ is a group of polynomial growth.

Definition 3.1.8. A growth function $\gamma : \mathbb{N} \to \mathbb{R}^+$ is said to be *subexponential* if $\lim_{n\to\infty} \frac{\ln \gamma(n)}{n} = 0$. Likewise, a growth function γ is *superpolynomial* if $\lim_{n\to\infty} \frac{\ln \gamma(n)}{\ln n} = \infty$.

If a growth function γ is both subexponential and superpolynomial, then we say that γ has *intermediate growth*.

Remark 3.1.9. If a function is superpolynomial then it is not polynomial. Similarly, if a function is subexponential then it is not exponential.

In general, it should be noted that these three categories do not cover all functions from $\mathbb{N}$ to $\mathbb{R}^+$. For example, while n^e is polynomial, 2^n is exponential, and $e^{\sqrt{n}}$ is of intermediate growth, we have the function $e^n \sin(\pi n)$ which fluctuates between being 0 and exponential, and is hence neither of the two. Further examples include n^n with superpolynomial growth and $e^{n/\log n}$ with subexponential growth.

On the other hand, it is in fact possible to neatly categorize finitely generated groups into three types depending on whether they have *polynomial, exponential* or *intermediate growth*. We have from Proposition 3.1.6 that all growth functions of a group G are equivalent, and we will soon show with Theorem 3.1.11 that all growth functions have either *exponential* or *subexponential growth*.

Lemma 3.1.10 (Fekete Lemma)**.** [5, Proposition VI.56(i)] *Let $\alpha(n)$ be a subadditive sequence of non-negative numbers, that is, $\alpha(m+n) \leq \alpha(m) + \alpha(n) \quad \forall m, n \in \mathbb{N}$. Then the sequence $(\frac{\alpha(n)}{n})$ converges, and*

$$\lim_{n\to\infty} \frac{\alpha(n)}{n} = \inf_{n\in\mathbb{N}} \frac{\alpha(n)}{n}.$$

Proof. For any positive integer a, we can express every $n \in \mathbb{N}$ as $n = qa + r$ with $q \geq 0$ and $0 \leq r < a$. Equivalently, write $q = \left\lfloor \frac{n}{a} \right\rfloor$ and $r = n - \left\lfloor \frac{n}{a} \right\rfloor a$. Now since $\alpha(n)$ is subadditive, we have that

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

Using the second notation, it is clear that

$$\lim_{n\to\infty} \frac{\alpha(r)}{qa} = \lim_{n\to\infty} \frac{\alpha(n - \left\lfloor \frac{n}{a} \right\rfloor a)}{\left\lfloor \frac{n}{a} \right\rfloor a} = 0;$$

indeed, since a is fixed, as $n \to \infty$ we have that $\lfloor \frac{n}{a} \rfloor$ is approximately n.

From the above, it follows that $\limsup_{n\to\infty} \frac{\alpha(n)}{n} \leq \frac{\alpha(a)}{a}$ for each $a \geq 1$. This implies that $\limsup_{n\to\infty} \frac{\alpha(n)}{n} \leq \inf_{a\geq 1} \frac{\alpha(a)}{a}$. Also, for each $n \in \mathbb{N}$ we know that $\inf_{a\geq 1} \frac{\alpha(a)}{a} \leq \frac{\alpha(n)}{n}$. It then follows that $\lim_{n\to\infty} \frac{\alpha(n)}{n} = \inf_{n\in\mathbb{N}} \frac{\alpha(n)}{n}$. □

Theorem 3.1.11. [4, Exercise 1.6] [7, 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. Hence all growth functions have either exponential or subexponential growth.

Proof. By Proposition 3.1.4(iii), we know that γ is a submultiplicative function. So for all $m, n \geq 1$ it holds that

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

Hence the function $\ln \gamma$ is subadditive, and since it defines a subadditive sequence we can directly apply Lemma 3.1.10 to prove the existence of the stated limit, and since $\gamma(n) \geq 1$, we have that the limit is nonnegative.

Now, if $\lim_{n\to\infty} \frac{\ln \gamma(n)}{n} = 0$ then by definition $\gamma(n)$ has subexponential growth. On the other hand, for exponential growth we have to verify that the limit being strictly positive implies $\gamma(n) \gtrsim e^n$. So suppose that $L := \lim_{n\to\infty} \frac{\ln \gamma(n)}{n} > 0$, and choose $\varepsilon > 0$ such that $L - \varepsilon > 0$. By the definition of the limit, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, it holds that $\frac{\ln \gamma(n)}{n} > L - \varepsilon$. Therefore, $\ln \gamma(n) > (L-\varepsilon)n$, and equivalently, $\gamma(n) > e^{(L-\varepsilon)n}$ for all $n \geq n_0$. Now since $L - \varepsilon > 0$, setting $\alpha := L - \varepsilon$ gives $\gamma(n) \geq e^{\alpha n}$ and hence $\gamma(\frac{n}{\alpha}) \geq e^n$ for all sufficiently large n. Therefore $\gamma(n) \gtrsim e^n$, that is, $\gamma(n)$ has exponential growth in this case, as required. □

Theorem 3.1.12. [4, Exercise 1.5] *Let H be a subgroup of G of finite index. Then, H is finitely generated and $\gamma_H \sim \gamma_G$. In other words, a finite-index subgroup of G has growth equivalent to the growth of the group itself.*

Proof. The proof is omitted as it is beyond the scope of this thesis. It follows by applying the *Fundamental Observation of Geometric Group Theory*, found in [5, Theorem IV.23]. □

The *first Grigorchuk group*, which we will denote by $\mathbb{G}$, is the first group proven to have intermediate growth. As we will see, this group is generated by elements of the automorphism group of the binary rooted tree. We begin by introducing the binary rooted tree and then proceed by constructing the first Grigorchuk group in the next section.

3.2 Binary rooted tree

Definition 3.2.1. A *tree* is an undirected graph in which every pair of distinct vertices is connected by exactly one path.

The *binary rooted tree* is a tree with an initial vertex (the root) where every vertex has a left and a right child. More formally, it defined as a tree $T = (V, E)$ such that the set V of vertices is in bijection with the set of finite 0-1 strings $v = x_1 x_2 \cdots x_k$, where $x_k \in \{0, 1\}, k \in \mathbb{N}$. In this thesis, we will denote each vertex by its corresponding (binary) word.

We call the empty string the *root*. There is an edge between two vertices v, v' if $v' = v0$ or $v' = v1$ or vice versa.

Definition 3.2.2. The tree 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. Clearly, T_v is isomorphic to T [4, Section 4].

The *level* of a vertex v is its length, and is denoted by $l(v)$. The n-th level of the tree is the set of vertices with word length n.

Definition 3.2.3. 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 length k or less, and their associated edges.

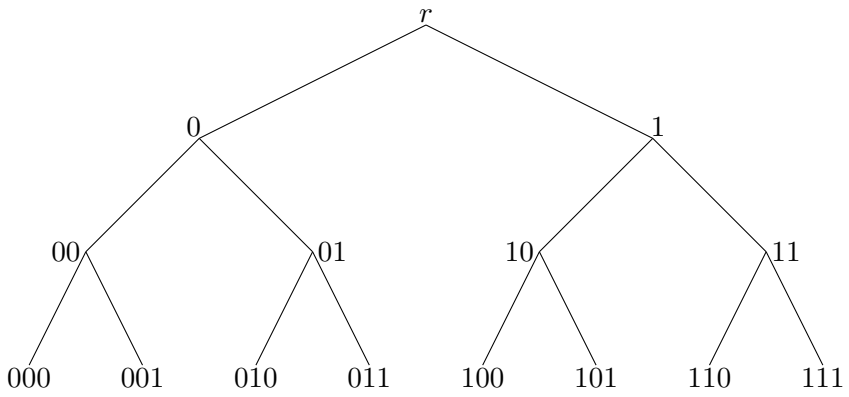


Figure 3.1: The first few levels of the binary rooted tree.

Consider the *automorphism group* $\mathrm{Aut}(T)$ of the tree T: this is the group of bijections $\varphi : V \to V$ such that $(v, v') \in E \iff (\varphi(v), \varphi(v')) \in E$. It can be shown through induction on the level of vertices that every automorphism preserves the child-parent relations between vertices, and therefore also their levels.

Definition 3.2.4. A *swap* is an automorphism φ of T where there exists a binary word w such that

$$\varphi(v) = \begin{cases} w\overline{x_1}x_2\cdots & \text{if } v = wx_1x_2\cdots \text{ with } x_i \in \{0,1\}, \text{ where } \overline{x_i} = 1 - x_i, \\ v & \text{otherwise.} \end{cases}$$

In other words, a swap exchanges the left and right subtrees below a fixed vertex and does not change anything elsewhere.

It can be verified that every element φ of $\mathrm{Aut}(T)$ is composed of swaps.

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

Definition 3.2.5. 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 the action of A on X is the semi-direct product

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

where the multiplication is defined by

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

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

In the following, we will only consider the wreath product of a group G by Sym(2), with Sym(2) acting on the set {0,1}. We can state this particular wreath product more clearly, since $G^{\{0,1\}} \cong G \times G$, as follows.

Notation: For a group G, the wreath product $G \wr_{\{0,1\}} \mathrm{Sym}(2)$ corresponds to the semi-direct product $(G \times G) \rtimes \mathrm{Sym}(2)$, with $\mathrm{Sym}(2) \cong \mathbb{Z}_2$ acting by swapping the two G.

Definition 3.2.6. The subgroup $\mathrm{St}_{\mathrm{Aut}(T)}(k)$ of $\mathrm{Aut}(T)$ is the subgroup of all automorphisms that fix any vertex of level $\leq k$. In other words, this is the group of all automorphisms which are only composed of swaps on children of vertices of level k or higher. It can be checked that these subgroups are normal in $\mathrm{Aut}(T)$.

Proposition 3.2.7. [5, Proposition VIII.5] [7, Proposition 4.9] *The following hold:*

(i) $\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(1) \cong \mathbb{Z}_2$;

(ii) $\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k) \cong (\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k-1)) \wr \mathbb{Z}_2$;

(iii) $\left|\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k)\right| = 2^{2^k-1}$.

Proof. We begin by showing that the group $\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k)$ is isomorphic to the subgroup of all automorphisms which are only composed of swaps on children of vertices with level $< k$:

$$\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k) \cong \mathrm{Aut}(T(k)). \tag{3.2.1}$$

To do this, we need an embedding map

$$\pi_k : \mathrm{Aut}(T) \to \mathrm{Aut}(T(k)),$$

which sends an automorphism to its action on the first k levels, and has $\ker(\pi_k) = \mathrm{St}_{\mathrm{Aut}(T)}(k)$. Then the above claim follows by the First Isomorphism Theorem.

Now for the case when $k = 1$, the isomorphism is clear, since $\mathrm{Aut}(T(1))$ is defined by the way it acts on the two subtrees: it either swaps the two subtrees, or it does not swap them (equivalently, it swaps them twice). Hence $\mathrm{Aut}(T(1)) \cong \mathbb{Z}_2$.

For $k > 1$, it can be verified that

$$\mathrm{Aut}(T(k)) \cong (\mathrm{Aut}(T(k-1))) \times \mathrm{Aut}(T(k-1))) \rtimes \mathbb{Z}_2,$$

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

Finally, note that $\mathrm{Aut}(T(k)) = 2^{2^k-1}$. This is because each element in $\mathrm{Aut}(T(k))$ corresponds to a binary choice, either swapping or not, and each such choice is independent of the other ones. There are exactly 2^{k-1} vertices in a binary rooted tree of level k, i.e. choices, hence it follows from (3.2.1) that $\left|\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k)\right| = \mathrm{Aut}(T(k)) = 2^{2^k-1}$. □

3.3 Construction and properties of the first Grigorchuk group

Recalling the definition above for the particular case of $k = 1$, the group $\mathrm{St}_{\mathrm{Aut}(T)}(1)$ is the subgroup of $\mathrm{Aut}(T)$ of all automorphisms that fix any vertex of length ≤ 1. Now, every automorphism in $\mathrm{St}_{\mathrm{Aut}(T)}(1)$ is characterized by the way it acts on the subtrees T_0, T_1, as follows.

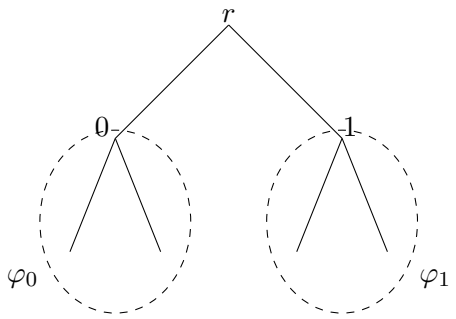


Figure 3.2: Each $\varphi \in \mathrm{St}_{\mathrm{Aut}(T)}(1)$ can be represented as a pair of automorphisms (φ_0, φ_1).

Definition 3.3.1. Denote $\varphi \in \mathrm{St}_{\mathrm{Aut}(T)}(1)$ as (φ_0, φ_1) such that

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

We can then define $\psi : \mathrm{St}_{\mathrm{Aut}(T)}(1) \to \mathrm{Aut}(T) \times \mathrm{Aut}(T)$ to be the map such that $\psi(\varphi) = (\varphi_0, \varphi_1)$, where $\varphi \in \mathrm{St}_{\mathrm{Aut}(T)}(1)$ is as above.

Definition 3.3.2. The *first Grigorchuk group* is the group $\mathbb{G} = \langle a, b, c, d \rangle$, where a, b, c, d are elements of $\mathrm{Aut}(T)$ such that

(i) the automorphism a swaps the subtrees T_0 and T_1. This means that for a vertex $v = x_1 x_2 \cdots x_k$, we have $a(v) = \overline{x_1} x_2 \cdots x_k$, where $\overline{x_i} = 1 - x_i$;

(ii) the automorphisms b, c, d are recursively defined by

$$b \mapsto (a, c) \qquad c \mapsto (a, d) \qquad d \mapsto (I, b),$$

where we used the decomposed automorphism notation, according to the definition above, or more exactly: $g \mapsto (g_0, g_1)$ means that g does not swap the two main subtrees T_0 and T_1, and it acts as g_0 on T_0 and as g_1 on T_1.

More explicitly, the action of these automorphisms a, b, c, d on some vertex $v = x_1 x_2 \cdots x_k$ in V is as follows:

$$a(v) = a(x_1 x_2 \cdots x_k) = \overline{x_1} x_2 \cdots x_k = \begin{cases} 1 x_2 x_3 \cdots x_k & \text{if } x_1 = 0, \\ 0 x_2 x_3 \cdots x_k & \text{if } x_1 = 1. \end{cases}$$

$$b(v) = b(x_1 x_2 \cdots x_k) = \begin{cases} 0a(x_2 x_3 \cdots x_k) & \text{if } x_1 = 0, \\ 1c(x_2 x_3 \cdots x_k) & \text{if } x_1 = 1. \end{cases} = \begin{cases} 01 x_3 \cdots x_k & \text{if } x_1 = 0, x_2 = 0 \\ 00 x_3 \cdots x_k & \text{if } x_1 = 0, x_2 = 1 \end{cases},$$

$$c(v) = c(x_1 x_2 \cdots x_k) = \begin{cases} 0a(x_2 x_3 \cdots x_k) & \text{if } x_1 = 0, \\ 1d(x_2 x_3 \cdots x_k) & \text{if } x_1 = 1. \end{cases} = \begin{cases} 01 x_3 \cdots x_k & \text{if } x_1 = 0, x_2 = 0 \\ 00 x_3 \cdots x_k & \text{if } x_1 = 0, x_2 = 1 \end{cases},$$

$$d(v) = d(x_1x_2\cdots x_k) = \begin{cases} x_1x_2x_3\cdots x_k & \text{if } x_1 = 0, \\ 1b(x_2x_3\cdots x_k) & \text{if } x_1 = 1. \end{cases}$$

A graphical representation of these elements is shown in Figure 3.3 below, where one can clearly see the subtrees on which a is applied.

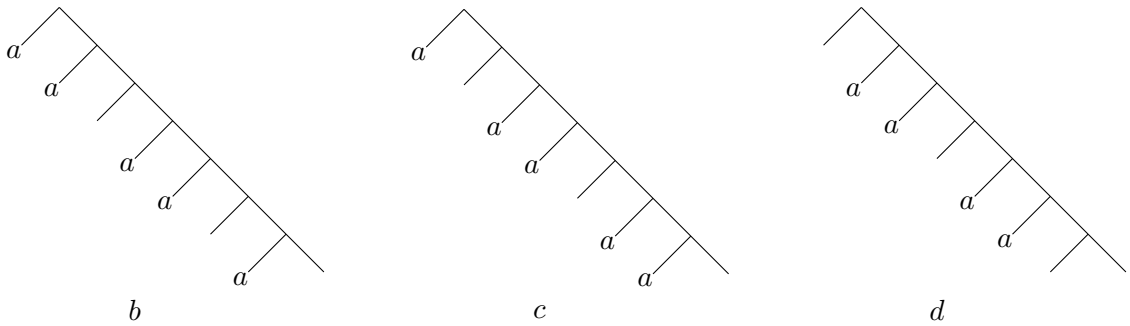


Figure 3.3: Representation of the automorphisms $b, c, d \in \mathbb{G}$.

Example 3.3.3. Some explicit examples include:

$$a(1101101) = 0101101;$$

$$b(1101101) = 1c(101101) = 11d(01101) = 1101101;$$

$$c(1101101) = 1d(101101) = 11b(01101) = 110a(1101) = 1100101;$$

$$d(1101101) = 1b(101101) = 11c(01101) = 110a(1101) = 1100101.$$

Remark 3.3.4. Since the first Grigorchuk group is defined recursively, this definition provides an algorithm solving the word problem (see Section 2.4) for $\mathbb{G}$ by reducing elements to their actions on subtrees. So to determine whether a given word w corresponds to the identity in $\mathbb{G}$, we check whether w fixes the first level of the tree. If it does, we decompose it into two induced actions on the subtrees and repeat the procedure recursively. If at any stage a nontrivial action appears, the word is not the identity.

Proposition 3.3.5. [4, Exercise 4.3] [12, Proposition 2.3] *The automorphisms a, b, c, d all have order 2, that is, $a^2 = b^2 = c^2 = d^2 = I$.*

Proof. First observe that $a^2 = I$, since a swaps the two subtrees, and swapping twice equals to the action of the identity automorphism. More specifically, for any vertex $v = x_1x_2\cdots x_k$ in V,

$$a^2(v) = a(a(x_1x_2\cdots x_k)) = a(\overline{x_1}x_2\cdots x_k) = x_1x_2\cdots x_k = v.$$

Now we consider b, c and d, and we show by induction on n that all the vertices v on level $l(v) = n$ are held constant by b^2, c^2, or d^2. By the definition of each of these, the claim holds for $n = 1$, that is, for any vertex $v = x_1$. Now assume that v is held constant for any $l(v) = k$ with $k < n$ when b^2, c^2 or d^2 is applied. We know that $(x, y)^2 = (x^2, y^2)$ since performing automorphisms on different subtrees' vertices is commutative. This means that

$$b^2 = (a, c)^2 = (a^2, c^2) = (I, c^2)$$

$$c^2 = (a^2, d^2) = (I, (I^2, d^2)) = (I, (I, d^2))$$
$$d^2 = (I^2, b^2) = (I, b^2).$$

Now consider a vertex $\tilde{v} = j_1 j_2 \cdots j_n$ where $l(\tilde{v}) = n$. Either $\tilde{v} = 0 j_2 \cdots j_n$, or $\tilde{v} = 1 j_2 \cdots j_n$. Taking $b^2(\tilde{v})$, we get $(0, I(j_2 \cdots j_n)) = \tilde{v}$ or $(I, c^2(j_2 \cdots j_n))$, respectively. The first is trivially $\tilde{v}$, while the second is $\tilde{v}$ by the inductive hypothesis, since $j_2 \cdots j_n$ is a sequence of length $n - 1 < n$.

It can be shown with similar arguments that also the automorphisms c and d have order 2, as claimed. □

Proposition 3.3.6. [4, Exercise 4.3] [12, Proposition 2.4] *We have the following relations in* $\mathbb{G}$*:*

$$bc = cb = d \qquad cd = dc = b \qquad bd = db = c.$$

Hence $\mathbb{G}$ *is* 3*-generated.*

Proof. We use induction on the level of the tree, or equivalently, the length of words in the tree.

Begin by noting that the above relations hold trivially for any vertex with word of length 1, since b, c, d act trivially on the root, which is the only vertex with word of length 1. So assume that these relations hold for all words of length $n - 1$.

Since automorphisms on different subtrees are commutative, we have the following:

$$bc = (a, c)(a, d) = (a^2, cd) = (I, cd);$$
$$cd = (a, d)(I, b) = (a, db);$$
$$db = (I, b)(a, c) = (a, bc).$$

Considering now a vertex $v = x_1 x_2 \cdots x_n$ of length n in V, we have that

$$bc(v) = \begin{cases} 0x_2 \cdots x_n = v = d(v) & \text{if } x_1 = 0, \\ 1cd(x_2 \cdots x_n) = 1b(x_2 \cdots x_n) = d(v) & \text{if } x_1 = 1, \end{cases}$$

where we used the definition of d for the last equality in both cases, and for the case $x_1 = 1$ the second equality follows by the induction hypothesis since $l(x_2 \cdots x_k) < n$.

Similar arguments can be made for the other stated relations. Then clearly $\mathbb{G}$ is 3-generated, as any element in the group can be expressed as a finite product (composition) of a and any other two elements out of $\{b, c, d\}$ - for instance, $\mathbb{G} = \langle a, b, c \rangle$ since $bc = d$. This concludes the proof. □

Proposition 3.3.7. [4, Exercise 4.3] *The subgroup generated by* $b, c, d \in \mathrm{St}_{\mathrm{Aut}(T)}(1)$ *is isomorphic to* $\mathbb{Z}_2^2 = \mathbb{Z}_2 \times \mathbb{Z}_2$*.*

Proof. From Proposition 3.3.6 we have that $\mathbb{G} = \langle a, b, c \rangle = \langle a, c, d \rangle = \langle a, b, d \rangle$, and $d = bc$. Consider the subgroup $H = \langle b, c, d \rangle$ of $\mathbb{G}$. Then since $d = bc$ it follows that H is actually generated by two elements, $H = \langle b, c \rangle$ as d can be expressed as product of the other two generators. Furthermore, we know from Proposition 3.3.5 that $b^2 = c^2 = d^2 = I$, that is, both b, c have order 2, and also that

$$d = bc \quad \Longrightarrow \quad d^2 = (bc)^2 = I.$$

Therefore $H = \langle b, c\rangle$ is generated by two elements of order 2, with the relation $(bc)^2 = I$, or equivalently, $bc = cb$.

Now recall the presentation of the Klein-4 group: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle x, y \mid x^2 = y^2 = I, xy = yx\rangle$. From this it is clear that there is an isomorphism between this group and $H = \langle b, c \mid b^2 = c^2 = I, bc = cb\rangle$, hence the result. □

Recall Definition 3.3.1: Denote $\varphi \in \mathrm{St}_{\mathrm{Aut}(T)}(1)$ by $\varphi = (\varphi_0, \varphi_1)$ such that

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

Then define $\psi : \mathrm{St}_{\mathrm{Aut}(T)}(1) \to \mathrm{Aut}(T) \times \mathrm{Aut}(T)$ such that $\psi(\varphi) = (\varphi_0, \varphi_1)$, where $\varphi \in \mathrm{St}_{\mathrm{Aut}(T)}(1)$ is as above.

Now rephrasing the definition of the first Grigorchuk group according to this notation, we have that $\mathbb{G} = \langle a, b, c, d\rangle$ where

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

In particular, $\varphi_0(b) = a$ and $\varphi_1(b) = c$, and so on. Finding ψ for other elements requires some more computation.

Lemma 3.3.8. [12, Lemma 2.8] *The following hold:*

$$\psi(aba) = (c, a) \qquad \psi(aca) = (d, a) \qquad \psi(ada) = (b, I).$$

Proof. To show that $\psi(aba) = (c, a)$, consider first separately $0x_2 \cdots x_k$ and $1x_2 \cdots x_k \in T$:

$$aba(0x_2 \cdots x_k) = ab(1x_2 \cdots x_k) = a(1c(x_2 \cdots x_k)) = 0c(x_2 \cdots x_k),$$

$$aba(1x_2 \cdots x_k) = ab(0x_2 \cdots x_k) = a(0a(x_2 \cdots x_k)) = 1a(x_2 \cdots x_k).$$

So we see that $\varphi_0(aba) = c$, while $\varphi_1(aba) = a$. Hence $\psi(aba) = (c, a)$.

The other two results can be shown through similar calculations. □

Proposition 3.3.9. [4, Exercise 4.4] [12, Proposition 3.2] *We have that* $(ad)^4 = (ac)^8 = (ab)^{16} = I$.

Proof. By Propositions 3.3.5 and 3.3.6, we know that any pairing of elements of $\{b, c, d\}$ can be reduced to a single letter, and any repeated letter corresponds to the identity. We will use these relations in the following computations, together with the preceding lemma - here, $\psi(ada)$ and ada are considered to be the same automorphism.

(1) First consider ad and da:

$$(ad)^4 = ((ad)(ad))^2 = ((ada)d)^2 = ((b, I)(I, b))^2 = (b, b)^2 = (b^2, b^2) = I,$$

$$(da)^4 = ((da)(da))^2 = ((dad)a)^2 = ((I, b)(b, I))^2 = (b, b)^2 = (b^2, b^2) = I.$$

So both ad and da have order dividing 4.

(2) Next,

$$(ac)^2 = (ac)(ac) = (aca)c = (d, a)(a, d) = (da, ad),$$

$$(ca)^2 = (ca)(ca) = (cac)a = (a,d)(d,a) = (ad,da).$$

Since ad and da were shown in (1) to have order dividing 4, it follows from the calculations above that ac and ca have order dividing 8, as required.

(3) Lastly,

$$(ab)^2 = (ab)(ab) = (aba)b = (c,a)(a,c) = (ca,ac),$$
$$(ba)^2 = (ba)(ba) = (bab)a = (a,c)(c,a) = (ac,ca).$$

Since ac and ca were shown in (2) to have order dividing 8, the calculations above give that ab and ba have order dividing 16, concluding the proof. □

Before we begin to talk about the growth rate of $\mathbb{G}$, we first need to verify that $\mathbb{G}$ is an infinite group. This will be needed for showing that $\mathbb{G}$ has superpolynomial growth.

Definition 3.3.10. We denote by $\mathrm{St}_{\mathbb{G}}(k)$ the subgroup of $\mathbb{G}$ that contains all automorphisms that fix any vertex of length $\leq k$, that is, $\mathrm{St}_{\mathbb{G}}(k) = \mathbb{G} \cap \mathrm{St}_{\mathrm{Aut}(T)}(k)$.

Proposition 3.3.11. [7, Exercise 5.8] *Every element $g \in \mathrm{St}_{\mathbb{G}}(k)$ can be expressed as a 2^k-tuple*

$$(g_{0\ldots00}, g_{0\ldots01}, \ldots, g_{1\ldots10}, g_{1\ldots11}),$$

where the subscripts correspond to the vertices of length k, such that:

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

$$g(w) = vg_v(w');$$

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

Proof. Let $T(k)$ be the set of vertices at level k, that is, words of length k. For $v \in T(k)$, recall that T_v is the subtree rooted at v, isomorphic to T.

From the definition above, we have that $\mathrm{St}_{\mathbb{G}}(k) = \{g \in \mathbb{G} : g(v) = v \text{ for each } v \in T(k)\}$. Note that the Grigorchuk group admits an embedding

$$\psi : \mathrm{St}_{\mathbb{G}}(1) \hookrightarrow \mathbb{G} \times \mathbb{G}, \quad \text{given by } \psi(g) = (g_0, g_1),$$

where $g(0w) = 0g_0(w)$ and $g(1w) = 1g_1(w)$ with $g_0, g_1 \in \mathbb{G}$. So ψ is an injective function, and it expresses how an element g acts on the two subtrees below the root.

First consider the base case, with $k = 1$, so let $g \in \mathrm{St}_{\mathbb{G}}(1)$. Then, it follows from the definition of ψ that $g = (g_0, g_1)$ where for $w = iw', g(w) = g(iw') = ig_i(w')$ with $i \in \{0,1\}$. Thus the tuple is (g_0, g_1), with $g_i \in \mathbb{G}$. So the statement holds for this case.

Next assume that it holds for all words of length k, i.e. that each $h \in \mathrm{St}_{\mathbb{G}}(k)$ can be written as $h = (h_v)_{v \in T(k)}, h_v \in \mathbb{G}$. Now take $g \in \mathrm{St}_{\mathbb{G}}(k+1)$, then in particular $g \in \mathrm{St}_{\mathbb{G}}(1)$, so

$$\psi(g) = (g_0, g_1), \quad g_0, g_1 \in \mathbb{G}.$$

Observe that since g fixes all vertices at level $k+1$, each section g_0, g_1 fixes all vertices at level k. Thus $g_0, g_1 \in \mathrm{St}_{\mathbb{G}}(k)$.

By induction hypothesis, $g_0 = (g_{0v})_{v \in T(k)}$ and $g_1 = (g_{1v})_{v \in T(k)}$. Now define a 2^{k+1}-tuple indexed by $T(k+1)$, with $g_{iv} := (g_{iv})_{v \in T(k)}$, for $i \in \{0,1\}$. Indeed, for $i \in \{0,1\}, v \in T(k)$ and $w = ivw' \in T$, we have

$$g(w) = ig_i(vw') = ivg_{iv}(w'), \text{ where } g_{iv} \in \mathbb{G},$$

as required. □

Proposition 3.3.12. [4, Exercise 5.2] [7, Proposition 5.9] *We have*

$$[\mathbb{G} : \mathrm{St}_{\mathbb{G}}(k)] \leq [\mathrm{Aut}(T) : \mathrm{St}_{\mathrm{Aut}(T)}(k)] = 2^{2^k-1}.$$

Proof. One can check that $\mathrm{St}_{\mathbb{G}}(k)$ is normal in $\mathbb{G}$. Indeed, for

$$g \in \mathbb{G}, \quad h \in \mathrm{St}_{\mathbb{G}}(k) = \{g \in \mathbb{G} : g(v) = v \text{ for each } v \in T(k)\},$$

we show that $ghg^{-1} \in \mathrm{St}_{\mathbb{G}}(k)$: taking any vertex v of level k, we have

$$(ghg^{-1})(v) = g(h(g^{-1}(v))).$$

Now, note that $g^{-1}(v)$ is also a vertex of level k, since automorphisms preserve the levels of vertices, and h fixes all level-k vertices, so

$$h(g^{-1}(v)) = g^{-1}(v) \quad \Rightarrow (ghg^{-1})(v) = g(g^{-1}(v)) = v.$$

Hence $\mathrm{St}_{\mathbb{G}}(k)$ is normal in $\mathbb{G}$.

Next, to show that the group $\mathbb{G}/\mathrm{St}_{\mathbb{G}}(k)$ is isomorphic to a subgroup of $\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k)$, we begin by recalling that from the proof of Proposition 3.2.7 we already know that

$$\mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k) \cong \mathrm{Aut}(T(k)). \tag{3.3.1}$$

So define a map

$$\rho_k : \mathrm{Aut}(T) \to \mathrm{Aut}(T(k)),$$

which sends an automorphism to its action on the first k levels, and has kernel $\ker(\rho_k) = \mathrm{St}_{\mathrm{Aut}(T)}(k)$.

Now, restricting the map ρ_k to $\mathbb{G} \subseteq \mathrm{Aut}(T)$, we have $\rho_k|_{\mathbb{G}} : \mathbb{G} \to \mathrm{Aut}(T(k))$. The kernel of this restricted map is given by exactly those elements of $\mathbb{G}$ that act trivially on level k, that is,

$$\ker(\rho_k|_{\mathbb{G}}) = \mathrm{St}_{\mathbb{G}}(k),$$

so again by the First Isomorphism Theorem, $\mathbb{G}/\mathrm{St}_{\mathbb{G}}(k) \cong \rho_k(\mathbb{G})$, which is a subgroup of $\mathrm{Aut}(T(k))$. Since $\mathrm{Aut}(T(k)) \cong \mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k)$ by (3.3.1), we get that

$$\mathbb{G}/\mathrm{St}_{\mathbb{G}}(k) \hookrightarrow \mathrm{Aut}(T)/\mathrm{St}_{\mathrm{Aut}(T)}(k).$$

From this embedding it follows that $[\mathbb{G} : \mathrm{St}_{\mathbb{G}}(k)] \leq [\mathrm{Aut}(T) : \mathrm{St}_{\mathrm{Aut}(T)}(k)]$.

Finally, since $\mathrm{Aut}(T/\mathrm{St}_{\mathrm{Aut}(T)}(k) \cong \mathrm{Aut}(T(k))$ by (3.3.1), we only need to compute the order of $\mathrm{Aut}(T(k))$ to conclude the proof. From Proposition 3.2.7(iii), we directly have

$$|\mathrm{Aut}(T(k))| = 2^{2^k-1}. \qquad \square$$

Definition 3.3.13. We define the *fundamental subgroup of* $\mathbb{G}$ as $\mathbb{H} = \mathrm{St}_{\mathbb{G}}(1)$.

Lemma 3.3.14. [4, Lemma 5.1] *For the fundamental subgroup* $\mathbb{H}$ *of* $\mathbb{G}$*, we have*

(i) $[\mathbb{G} : \mathbb{H}] = 2, \quad \mathbb{H} \lhd \mathbb{G}$;

(ii) $\mathbb{H} = \langle b, c, d, aba, aca, ada \rangle$.

Proof. The first claim follows directly from Proposition 3.3.12, and the fact that $\mathbb{H}$ is a proper subgroup of $\mathbb{G}$. Indeed, applying the inequality from the above proposition, with $k = 1$ in this case because of how $\mathbb{H}$ was defined, we get

$$[\mathbb{G} : \mathbb{H}] = [\mathbb{G} : \mathrm{St}_{\mathbb{G}}(1)] \leq [\mathrm{Aut}(T) : \mathrm{St}_{\mathrm{Aut}(T)}(1)] = 2^{2^1-1} = 2.$$

So the index of $\mathbb{H}$ in $\mathbb{G}$ is either 1 or 2. Now $\mathbb{H}$ can not be an improper subgroup of $\mathbb{G}$, since every element in $\mathbb{H}$ fixes the two vertices 0 and 1, while the generator $a \in \mathbb{G}$ swaps them. Therefore $\mathbb{H} \neq \mathbb{G}$, and the index can not be 1, hence $[\mathbb{G} : \mathbb{H}] = 2$. The normality of $\mathbb{H}$ in $\mathbb{G}$ was shown in the proof of Proposition 3.3.12.

For the second claim, consider the set of words in $\{a, b, c, d\}$. It follows from Proposition 3.3.6 that every pairing of the elements b, c, d can be reduced to a single letter. Therefore every word $w \in \mathbb{G}$ can be reduced to the form $w = x * a * \cdots * a * y$, 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 - indeed, the automorphism w swaps 0 and 1 if and only if the number of a's is odd. Finally, note that a word has an even number of a's if and only if it can be expressed as a combination of $*$ and $a*a$, i.e. $w = (a*a)*(a*a)\cdots(a*a)*$. This proves the second claim. □

Lemma 3.3.15. [4, Lemma 5.3] *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 3.3.14 implies that $\psi(\mathbb{H})$ is indeed a subgroup of $\mathbb{G} \times \mathbb{G}$. Then, we have that ψ acts on the generators of $\mathbb{H}$ as follows:

$$\begin{aligned} b &\mapsto (a, c) & aba &\mapsto (c, a) \\ c &\mapsto (a, d) & aca &\mapsto (d, a) \\ d &\mapsto (1, b) & ada &\mapsto (b, 1). \end{aligned}$$

The first column is just the definition of the elements b, c, d, and the second column was shown in Lemma 3.3.8. Now, since the projection of $\psi(\mathbb{H})$ onto $\mathbb{G} \times 1$ contains all the generators $(a, 1)$ to $(d, 1)$ of $\mathbb{G} \times 1$, it is a surjective map. The same argument holds for $1 \times \mathbb{G}$. □

Proposition 3.3.16. [4, Corollary 5.4] *The group $\mathbb{G}$ is infinite.*

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

Indeed, suppose towards a contradiction that $\mathbb{G}$ is finite. Then $\mathbb{H} < \mathbb{G}$ and $[\mathbb{G} : \mathbb{H}] = 2$ imply that $|\mathbb{H}| < |\mathbb{G}|$. However, by the surjectivity of the map $\psi(\mathbb{H}) \to \mathbb{G} \times \mathbb{G}$, we have that $|\mathbb{H}| \geq |\mathbb{G}|$, leading to a contradiction. Therefore, the group $\mathbb{G}$ must be infinite. □

Chapter 4

Superpolynomial growth of the first Grigorchuk group

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

We then conclude by stating that the first Grigorchuk group actually has intermediate and not exponential growth.

Definition 4.0.1. Let G, H be groups. We say that G and H are *commensurable*, denoted by $G \approx H$, if they contain isomorphic subgroups of finite index. That is, if there exist

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

Note that commensurability is an equivalence relation. Indeed, we check that commensurability of groups is reflexive, symmetric and transitive, as follows.

To show reflexivity for some group G, take $G' = G$. Since G has finite index in itself and $G \cong G$, it follows that G is commensurable with itself.

Next for symmetry, suppose that a group G is commensurable to a group H. Then there exist some finite-index subgroups $G' \leq G, H' \leq H$ such that $G' \cong H'$. Since group isomorphism is symmetric, it also holds that $H' \cong G'$, and therefore H is commensurable with G.

Finally for transitivity, consider some groups G, H, K such that G is commensurable with H and H is commensurable with K. Then there exist finite-index subgroups $G' \leq G, H' \leq H$ such that $G' \cong H'$; at the same time, there exist $H'' \leq H, K' \leq K$ such that $H'' \cong K'$. Note that since both H' and H'' are finite-index subgroups of H, their intersection $\bar{H} = H' \cap H''$ is still a finite-index subgroup of H. Now, $[H' : \bar{H}], [H'' : \bar{H}] < \infty$, and $G' \cong H', K' \cong H''$. So let $\bar{G}$ be the preimage of $\bar{H}$ under the first isomorphism, and $\bar{K}$ be the preimage of $\bar{H}$ under the second isomorphism. Then we have that $[G : \bar{G}], [K, \bar{K}] < \infty$, while also $\bar{G} \cong \bar{H} \cong \bar{K}$. Hence G and K are commensurable. We can therefore conclude that commensurability of groups is indeed an equivalence relation.

Example 4.0.2. A trivial example of commensurability is given by the set of all finite groups: all finite groups are commensurable to each other, since the trivial group is always a subgroup of finite order.

Furthermore, any group is commensurable with each of its finite-index subgroups.

Proposition 4.0.3. [7, Exercise 6.3] *The groups $\mathbb{Z}$ and $\mathbb{Z}^2$ are not commensurable.*

Proof. First we would need to find two isomorphic subgroups of $\mathbb{Z}$ and $\mathbb{Z}^2$, respectively, each having finite index. However note that every subgroup of $\mathbb{Z}$ has the form $n\mathbb{Z} \cong \mathbb{Z}$, and is therefore cyclic.

On the other hand, finite-index subgroups of $\mathbb{Z}^2$ are not cyclic. Indeed, let $H \leq \mathbb{Z}^2$ a subgroup of finite index, and suppose towards a contradiction that H is cyclic. Then

$$H = \langle (a,b) \rangle = \langle k(a,b) : k \in \mathbb{Z} \rangle.$$

Thus $\mathbb{Z}^2/H$ would still contain infinitely many different cosets, and hence $[\mathbb{Z}^2 : H] = \infty$, contradicting the assumption. Therefore H cannot be cyclic. □

Definition 4.0.4. A group G is *multilateral* if $|G| = \infty$ and $G \approx G^k$ for some $k \geq 2$.

Example 4.0.5. Consider the group $G = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}$, given by the countable direct sum of copies of $\mathbb{Z}$. This is a free abelian group of countable rank, with a countable generating set $\{e_i\}_{i \in \mathbb{N}}$ [2, Chapter 14]. Partitioning $\mathbb{N}$ into k disjoint infinite subsets $\mathbb{N} = A_1 \sqcup \cdots \sqcup A_k$ induces a decomposition

$$G \cong \bigoplus_{j=1}^{k} \bigoplus_{i \in A_j} \mathbb{Z} \cong G^k.$$

Moreover, any finite-index subgroup of G is again a free abelian group of countable rank [2, Theorem 14.5], and therefore isomorphic to G itself. Hence $G \approx G^k$ for all $k \geq 1$, so G is multilateral.

Another example is given by the countable direct sum of cyclic groups of prime order. Consider the abelian group $H = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/p\mathbb{Z}$ for some prime p. Note that H is a vector space over the field $F_p = \mathbb{Z}/p\mathbb{Z}$, with countably infinite dimension. We know from linear algebra that any countably infinite-dimensional vector space over F_p is isomorphic to its finite direct powers, so here $H \cong H^k$ for some index k. Also, any finite-index subgroup has finite codimension, and therefore still has countably infinite dimension, hence is isomorphic to H. So again $H \approx H^k$, showing that H is multilateral.

Lastly, consider the group $\mathbb{Z}$. This group is infinite, but it is not multilateral. Indeed, every finite-index subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{N}$, and hence is isomorphic to $\mathbb{Z}$. However, similarly to what was shown in Proposition 4.0.3, for $k \geq 2$ we have that $\mathbb{Z}^k$ is not commensurable with $\mathbb{Z}$, since $\mathbb{Z}^k$ has rank k while $\mathbb{Z}$ has rank 1. This means that $\mathbb{Z}$ and $\mathbb{Z}^k$ do not contain isomorphic finite-index subgroups, so $\mathbb{Z} \not\approx \mathbb{Z}^k$. Hence $\mathbb{Z}$ is not multilateral.

Lemma 4.0.6 (Lower Bound Lemma)**.** [4, Lemma 2.1] *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. The proof is omitted as it is beyond the scope of this thesis. It can be found in [4, Section 12]. □

Theorem 4.0.7. [4, Lemma 6.4] *Let G be a group. If G is multilateral, then G has superpolynomial growth.*

Proof. Since G is assumed to be multilateral, there are subgroups $G' \subset G, \widetilde{G} \subset G^k$ such that $G' \cong \widetilde{G}$ and $[G : G'], [G^k : \widetilde{G}] < \infty$. Now recall that by Theorem 3.1.12, any finite-index subgroup of a group has equivalent growth. Therefore in this case we have that

$$\gamma_G \sim \gamma_{G'} \sim \gamma_{\widetilde{G}} \sim \gamma_{G^k}.$$

From the above, it follows that $\gamma_G \gtrsim \gamma_{G^k} = (\gamma_G)^k$. So we can now apply the lower bound lemma to conclude that G has indeed superpolynomial growth. □

Now, having shown that any multilateral group has superpolynomial growth, all there is left to show is that $\mathbb{G}$ is multilateral. In order to do so, we again make use of the fundamental subgroup $\mathbb{H}$ of $\mathbb{G}$. We already know that $\mathbb{H}$ is of finite index in $\mathbb{G}$, so we only need to show that the image $\psi(\mathbb{H})$ is a finite-index subgroup of $\mathbb{H} \times \mathbb{H}$.

Definition 4.0.8. We denote by $\mathbb{B}$ the normal closure of b in $\mathbb{G}$:

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

Lemma 4.0.9. [4, Lemma 6.2] *The index of the normal subgroup $\mathbb{B}$ divides* 8.

Proof. Consider the quotient group $\mathbb{G}/\mathbb{B}$, where all conjugates of b become trivial. In particular, $b \mapsto I$ in this quotient group.

Recall from Proposition 3.3.6 that $\mathbb{G} = \langle a, b, d \rangle$. Also, in $\mathbb{G}$ we have $bc = cb = d$, which then implies that the images of c and d are the same. So $\mathbb{G}/\mathbb{B}$ is generated by the images of a and d. Therefore the order of $\mathbb{G}/\mathbb{B}$ divides $|\langle a, d \rangle|$, which was shown to be equal to 8 in Proposition 3.3.9. □

Lemma 4.0.10. [4, Lemma 6.3] *We have*

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

Proof. We know already from Lemma 3.3.15 that $\psi(\mathbb{H})$ contains the two generators $(1, b)$ and $(b, 1)$ of $\mathbb{H}$. Taking any $h \in \mathbb{H}$ and letting $\psi(h) = (h_0, h_1)$, we observe that

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

This means that $\psi(\mathbb{H})$ contains elements of the form $(I, g^{-1}bg), g \in \mathbb{G}$. Since the generators of $\mathbb{H}$ allow us to pick any $h_1 \in \mathbb{G}$, the image $\psi(\mathbb{H})$ contains all elements of the form $(I, g^{-1}bg)$, i.e. all the generators of $1 \times \mathbb{B}$. By the same logic, it also contains all the generators of $\mathbb{B} \times 1$, and therefore $\mathbb{B} \times \mathbb{B} \subset \psi(\mathbb{H})$.

The second inclusion follows directly from the definition of ψ, as $\psi(h) = (h_0, h_1) \quad \forall h \in \mathbb{H}$, where $h_0, h_1 \in \mathbb{H}$. Hence $\psi(\mathbb{H}) \subset \mathbb{H} \times \mathbb{H}$, concluding the proof. □

Proposition 4.0.11. [4, Proposition 6.1] *We have $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$.*

Proof. We need a finite-index subgroup of $\mathbb{G}$ and one of $\mathbb{G} \times \mathbb{G}$, and an isomorphism between them, so take $\mathbb{H} \leq \mathbb{G}$ and $\psi(\mathbb{H}) \leq \mathbb{G} \times \mathbb{G}$. Then $\mathbb{H} \cong \psi(\mathbb{H})$ since ψ is a group isomorphism.

Finally, all there is left to do is to show that both subgroups have finite index. From Lemma 4.0.10 we know that $\mathbb{B} \times \mathbb{B} \subset \psi(\mathbb{H})$, and from Lemma 4.0.9 that $[\mathbb{G} : \mathbb{B}] \leq 8$. Therefore we have the following:

$$[\mathbb{G} \times \mathbb{G} : \psi(\mathbb{H})] \leq [\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}] = [\mathbb{G} : \mathbb{B}]^2 \leq 8^2 = 64.$$

So we see that $[\mathbb{G} \times \mathbb{G} : \psi(\mathbb{H})] < \infty$. Furthermore, $[\mathbb{G} : \mathbb{H}] < \infty$ by Lemma 3.3.14 (i). Hence $\mathbb{G}$ is commensurable with $\mathbb{G}^2$, as claimed. □

Now, since $\mathbb{G}$ is infinite, we conclude that it is a multilateral group, implying the following key result.

Corollary 4.0.12. [4, Corollary 6.5] *The group $\mathbb{G}$ has superpolynomial growth.*

To conclude, we note once again that the Grigorchuk group $\mathbb{G}$ was the first one shown to have intermediate growth, since it is both superpolynomial and subexponential. The proof of the latter is however beyond the scope of this thesis. It can be found in [4, Section 9].

Remark 4.0.13. As mentioned at the beginning of the thesis, the first Grigorchuk group has been proposed in [10] as a potential platform for group-based cryptographic protocols, partly due to its rich algebraic structure and superpolynomial growth. One proposed criterion for such platforms is that the conjugacy search problem should not admit a deterministic subexponential-time solution. However, subsequent work has shown that the conjugacy search problem in the first Grigorchuk group can in fact be solved in polynomial time [8]. Consequently, the first Grigorchuk group is no longer regarded as a promising candidate for cryptographic applications based on the complexity of the conjugacy search problem.

Nevertheless, the group remains of significant mathematical interest. As the first known example of a finitely generated group of intermediate growth, it continues to play a central role in geometric and combinatorial group theory. The present thesis focuses on the growth properties of the group and the proof of its superpolynomial growth, while the cryptographic discussion serves primarily as motivation and historical context.

Bibliography

[1] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[2] L. Fuchs, *Infinite Abelian Groups, Vol. I*, Academic Press, New York and London, 1970.

[3] R. Grigorchuk, *Burnside's problem on periodic groups*, Funct. Anal. Appl., vol. 14, pp. 41–43, 1980.

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

[5] P. de la Harpe, *Topics in Geometric Group Theory*, University of Chicago Press, Chicago and London, 2000.

[6] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park, *New public-key cryptosystem using braid groups*, Advances in Cryptology – CRYPTO 2000, Lecture Notes in Computer Science, vol. 1880, pp. 166–183, Springer, Berlin, 2000.

[7] C. H. Lim, *Growth rate of groups*, University of Chicago, Research Experience for Undergraduate Papers, 2009.
`https://math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Lim.pdf`

[8] M. Modi, M. Seedhom, A. Ushakov, *Linear time algorithm for the conjugacy problem in the first Grigorchuk group*, International Journal of Algebra and Computation, vol. 31, no. 4, pp. 789–806, 2021.

[9] A. Myasnikov, V. Shpilrain and A. Ushakov, *Group-based cryptography*, Birkhäuser Verlag, Basel, 2008.

[10] G. Petrides, *Cryptanalysis of the Public Key Cryptosystem Based on the Word Problem on the Grigorchuk Groups*, 9th IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science, vol. 2898, pp. 234–244, Springer, Berlin, 2003.

[11] V. Shpilrain, *Assessing security of some group based cryptosystems. Group theory, statistics, and cryptography*, Contemporary Mathematics, vol. 360, pp. 167–177, American Mathematical Society, 2004. arXiv:math/0311047.

[12] K. Waddle, *The Grigorchuk Group*, University of Chicago, Research Experience for Undergraduate Papers, 2008.
`https://math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Waddle.pdf`

Bachelor's Theses in Mathematical Sciences 2026:K14
ISSN 1654-6229

LUNFMA-4192-2026

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lu.se/