

GROWTH IN PRODUCT REPLACEMENT GRAPHS OF GRIGORCHUK GROUPS

ANTON MALYSHEV* AND IGOR PAK*

ABSTRACT. The product replacement graph $\Gamma_k(G)$ is the graph on the generating k -tuples of a group G , with edges corresponding to Nielsen moves. We prove the exponential growth of product replacement graphs $\Gamma_k(\mathbb{G}_\omega)$ of Grigorchuk groups, for $k \geq 5$.

1. INTRODUCTION

The *product replacement graphs* $\Gamma_k(G)$ are the graphs on generating k -tuples of a group G , with edges corresponding to multiplications of one generator by another (see below). These graphs play an important role in computational group theory (see e.g. [BL, NP, P1]), and are related to the Andrews–Curtis conjecture in algebraic topology (see e.g. [BKM, BLM, Met]). For infinite groups, proving non-amenability of graphs $\Gamma_k(G)$ is a major open problem, closely related to Kazhdan’s property (T) of $\text{Aut}(F_k)$. In this paper we establish a weaker property, the exponential growth of product replacement graphs, for the Grigorchuk group \mathbb{G} and its generalizations \mathbb{G}_ω .

Let us begin by stating the main conjecture we address in this paper.

Conjecture 1.1 (Main Conjecture). *Let G be an infinite group generated by d elements. Then the product replacement graphs $\Gamma_k(G)$ have exponential growth, for all $k \geq d + 1$.*

Formally speaking, graphs $\Gamma_k(G)$ can be disconnected, in which case we conjecture that *at least one* connected component has exponential growth.

The motivation behind our Main Conjecture is rather interesting, which makes the conjecture both natural and speculative. First, recall that $\Gamma_k(G)$ are Schreier graphs of $\text{Aut}(F_k)$, generated by Nielsen transformations [LP] (see also [LŽ, P1]). A well known conjecture states that $\text{Aut}(F_k)$ has *Kazhdan’s property (T)* for $k > 3$. If true, this would imply the following conjecture:

Conjecture 1.2. *For every infinite group G , product replacement graphs $\Gamma_k(G)$ are non-amenable, for k large enough.*

In particular, this conjecture implies that all connected components of $\Gamma_k(G)$ are infinite and have exponential growth, for all G and k large enough. We should mention that $\text{Aut}(F_k)$ does not have (T) for $k = 2$ and 3 (see [GL, Lub]). On the other hand, the non-amenability of $\Gamma_n(G)$ follows from a weaker property (τ) for an appropriate family of subgroups (see [LŽ]).

We approach the Main Conjecture by looking at the growth of groups. The conjecture is straightforward for groups of exponential growth. It can be shown that the conjecture holds for virtually nilpotent groups (see Section 3). By Gromov’s theorem, this implies the conjecture for all groups of polynomial growth.

Unfortunately, groups of intermediate growth lack the rigid structure of nilpotent groups, so much that even explicit examples are difficult to construct and analyze (see e.g. [dlH1, G3]). Even now, much remains open for the classical *Grigorchuk group* \mathbb{G} , the first example of a group of intermediate growth discovered by Grigorchuk (see [G1, G2]).

We present a new combinatorial technique which allows us to establish the conjecture for a large class of Grigorchuk groups \mathbb{G}_ω . This is the main result of this paper:

*Department of Mathematics, UCLA, Los Angeles, CA, 90095. Email: {amalyshev,pak}@math.ucla.edu.

Theorem 1.3. *Let \mathbb{G}_ω be a generalized Grigorchuk group. Then $\Gamma_n(\mathbb{G}_\omega)$ is connected for each $n \geq 4$, and has exponential growth for each $n \geq 5$.*

The techniques in this paper generalize fairly easily to several other groups of intermediate growth, such as the Gupta–Sidki p -groups [GS], as well as large families of Grigorchuk p -groups. Many groups of intermediate growth, such as the groups of oscillating growth defined in [KP], have, by construction, some \mathbb{G}_ω as a subgroup or a factor group. Such groups, then, also have exponential Nielsen growth (see Proposition 3.7).

In fact, the techniques in this paper apply to a general class of branch groups defined in [Bar] called *splitter-mixer groups*. Many known group of intermediate growth appears to be based on a splitter-mixer group. (An example that does not fall into this class is given in [Nek] and analyzed in [BP], but our techniques should apply there as well). The proofs will appear in [M2].

In summary, although we have yet to find proofs in all cases, we believe the Main Conjecture holds for all *known* constructions of groups of intermediate growth. In that sense the situation is similar to the “ $p_c < 1$ ” conjecture by Benjamini and Schramm [BS] for groups of superlinear growth. The conjecture is known to hold for groups of exponential and polynomial growth, and by an ad hoc argument for Grigorchuk groups and general self-similar groups [MP]. It remains open for general groups of intermediate growth (see [Pete]).

Let us mention that in a followup paper [M1], the first author establishes Conjecture 1.2 for several classes of groups of exponential growth, which include virtually solvable groups, linear groups, random finitely presented groups (in Gromov sense), and hyperbolic groups. He uses a technical extension of *uniform exponential growth* and *uniform non-amenability* (see [A+, BG, dlH2, Wil]).

Unfortunately, the explicit combinatorial approach in this paper, does not seem to be strong enough to establish Conjecture 1.2 for the Grigorchuk group, which we state as a separate conjecture of independent interest.

Conjecture 1.4. *Product replacement graphs $\Gamma_k(\mathbb{G})$ are non-amenable, for all $k \geq 5$.*

The rest of this paper is structured as follows. We begin with basic definitions of growth of groups and the product replacement graphs (Section 2). In Section 3 we present basic results on the growth and connectivity of graphs $\Gamma_k(G)$; we also present general tools for establishing the exponential growth results. In a technical Section 4 we describe general tools and techniques for working with subgroups $G \subset \text{Aut}(\mathbf{T}_2)$ and their product replacement graphs. In the next two sections 5 and 6 we establish the main result. First, we prove the exponential growth of $\Gamma_k(\mathbb{G})$ for $k \geq 5$; in this case the (technical) argument is the most lucid. We then generalize this approach to *all* Grigorchuk groups \mathbb{G}_ω . We conclude with final remarks and open problems (Section 7).

2. BACKGROUND AND DEFINITIONS

2.1. Notation. Let X be a finite set. We write $\#X$ or $|X|$ to denote the size of X . Throughout the paper we use \mathbb{Z}_n to denote the cyclic group $\mathbb{Z}/n\mathbb{Z}$.

Let Γ be a directed graph, which may have loops and repeated edges. We define $v \in \Gamma$ to mean that v is a vertex of Γ . Let v, w be vertices of Γ . We write $v \rightarrow w$ when there is an edge in Γ from v to w , and $v \rightsquigarrow w$ when there is a path in Γ from v to w . We say Γ is *symmetric* if for every edge $v \rightarrow w$ of Γ there is an *inverse edge* $w \rightarrow v$. Every graph considered in this paper is a symmetric directed graph, unless otherwise specified. When convenient, we think of a symmetric directed graph as an undirected graph by identifying every edge with its inverse.

Let G be a group, which may be finite or infinite. A *generating n -tuple* of G is an element $(g_1, \dots, g_n) \in G^n$, such that $G = \langle g_1, \dots, g_n \rangle$. Let $S = (g_1, \dots, g_n)$ be such an n -tuple. Consider a left action of G on a set X . The *Schreier graph* $\text{Schr}_S(G, X)$ of this action with respect to S , is the directed graph whose vertices are the elements of X , with edges $x \rightarrow g_i x$ and $x \rightarrow g_i^{-1} x$ for each $x \in X$, and each $0 \leq i \leq n$. Note that each vertex in $\text{Schr}_S(G, X)$ has $2n$ edges leaving it, and

each edge $v \rightarrow w$ in such a graph has an inverse edge $w \rightarrow v$. Thus, $\text{Schr}_S(G, X)$ is a $2n$ -regular symmetric directed graph.

The *Cayley graph* $\text{Cay}_S(G)$ is the Schreier graph $\text{Schr}_S(G, G)$ with respect to the left action of G on itself by multiplication. Clearly, the Cayley graph $\text{Cay}_S(G)$ is connected. Given $g \in G$, we define $\ell_S(g)$ to be the length of the shortest path from 1 to g in the Cayley graph of G .

When the context makes it clear what the generating n -tuple S is, we drop the subscript, and simply write $\text{Cay}(G)$, $\text{Schr}(G, X)$, and $\ell(g)$. We write $\text{Aut}(G)$ for the group of automorphisms of G . We write $H < G$ when H is a subgroup of G , and $H \subsetneq G$ when H is a proper subgroup of G . For an element $g \in G$, denote by $\text{ord}(g)$ the order of g . For $g_1, \dots, g_n \in G$, denote

$$\prod_{i=1 \dots n}^{\rightarrow} g_i = g_1 \cdots g_n.$$

2.2. Growth in graphs. Let Γ be a symmetric directed graph, and let $v \in \Gamma$. The ball of radius r centered at v , denoted $B_\Gamma(v, r)$, is the set of vertices $w \in \Gamma$ such that there is a path of length at most r between v and w . For example, suppose $\Gamma = \text{Cay}_S(G)$. Then $B_\Gamma(1, r)$ consists of the elements $g \in G$ for which $\ell_S(g) \leq r$.

We say Γ has *exponential growth from v* , if there is a constant $\alpha > 1$, such that $|B_\Gamma(v, r)| \geq \alpha^r$ for all r (equivalently, for sufficiently large r). Suppose Γ has exponential growth from w , and there is a path $v \rightsquigarrow w$ in Γ . Then Γ also has exponential growth from v . Thus, if Γ is connected and has exponential growth from some $v \in \Gamma$, it also has exponential growth from any $w \in \Gamma$. In this case, we say that Γ has *exponential growth*.

2.3. Growth in groups. Let G be a group, Let S be a generating n -tuple of G . Define $B_{G,S}(r) = B_\Gamma(1, r)$, where $\Gamma = \text{Cay}_S(G)$. When it is clear what S is, we simply write $B_G(r)$ instead. It is easy to verify that the following definitions are independent of the choice of generators S .

We say G has *exponential growth* if Γ has exponential growth. In other words, G has exponential growth if there is a constant $\alpha > 1$ such that $|B_G(r)| \geq \alpha^r$ for sufficiently large r . Equivalently G has exponential growth if and only if

$$\liminf_{r \rightarrow \infty} \frac{\log |B_G(r)|}{r} > 0.$$

Similarly, we say G has *polynomial growth* if there is a constant d with $|B_G(r)| \leq r^d$ for sufficiently large r . In other words, G has polynomial growth if

$$\limsup_{r \rightarrow \infty} \frac{\log |B_G(r)|}{\log r} < \infty.$$

Example 2.1. The group \mathbb{Z} has polynomial growth. With respect to the generating 1-tuple $S = (1)$, we have $B_{\mathbb{Z}}(r) = [-r, r]$, and hence $|B_{\mathbb{Z}}(r)| = 2r + 1$.

Example 2.2. The free group with two generators, $G = F_2 = \langle a, b \rangle$ has exponential growth. With respect to the generators $S = (a, b)$, we have $|B_G(r)| = 1 + 4 \cdot 3^{r-1}$ for $r \geq 1$.

We say G has *intermediate growth* if it has neither exponential nor polynomial growth. The first known example of a group of intermediate growth is the Grigorchuk group \mathbb{G} , which will be defined later, in Section 5. We refer to [dlH1, §VI] and [GP] for more on the growth of groups.

2.4. Product replacement graphs. Given a generating n -tuple of S a group G , we can take an element of S and multiply it, either on the left or the right, by another element or another element's inverse. Such an operation is called a *Nielsen move*. Formally, for each $1 \leq i, j \leq n$ with $i \neq j$, we define the Nielsen moves $R_{ij}^{\pm 1}, L_{ij}^{\pm 1}$ by

$$\begin{aligned} R_{ij}^{\pm 1}(g_1, \dots, g_i, \dots, g_j, \dots, g_n) &= (g_1, \dots, g_i, \dots, g_j g_i^{\pm 1}, \dots, g_n), \\ \text{and } L_{ij}^{\pm 1}(g_1, \dots, g_i, \dots, g_j, \dots, g_n) &= (g_1, \dots, g_i, \dots, g_i^{\pm 1} g_j, \dots, g_n). \end{aligned}$$

Clearly, if S is a generating n -tuple of G , then $R_{ij}S$, $R_{ij}^{-1}S$, $L_{ij}S$, and $L_{ij}^{-1}S$ are also generating n -tuples of G .

We define the *product replacement graph* $\Gamma_n(G)$ to be the directed graph whose vertices are the generating n -tuples of G , where there is an edge from S to $R_{ij}S$, $R_{ij}^{-1}S$, $L_{ij}S$, and $L_{ij}^{-1}S$, for each generating n -tuple S and each pair of integers $i \neq j$ satisfying $1 \leq i, j \leq n$. This is a $4n(n-1)$ -regular symmetric directed graph.

Observe that

$$\begin{aligned} R_{ij}L_{ji}^{-1}L_{ij}(g_1, \dots, g_i, \dots, g_j, \dots, g_n) &= R_{ij}L_{ji}^{-1}(g_1, \dots, g_i, \dots, g_i g_j, \dots, g_n) \\ &= R_{ij}(g_1, \dots, g_j^{-1}, \dots, g_i g_j, \dots, g_n) = (g_1, \dots, g_j^{-1}, \dots, g_i, \dots, g_n). \end{aligned}$$

Hence, a series of Nielsen moves can swap two elements in a generating n -tuple, inverting one of them. Doing this twice simply inverts both elements. This implies that Nielsen moves permit us to rearrange generators in an n -tuple, except that we may need to invert one element (see [P1]). Moreover, if $g_i = 1$ for some i , then we can use Nielsen moves invert any one element, and therefore we can rearrange the generators freely.

Example 2.3. The graph $\Gamma_2(\mathbb{Z})$ has a vertex for each pair of relatively prime integers (a, b) , with two edges from (a, b) to each of $(a, b+a)$, $(a, b-a)$, $(a+b, b)$ and $(a-b, b)$. It is easy to check that this graph has exponential growth: the subgraph induced by $\{(a, b) \in \mathbb{Z}^2 \mid a, b > 0, \gcd(a, b) = 1\}$ is a rooted binary tree.

Example 2.4. Let $G = \mathbb{Z}_p^n$, with p prime. Then $\Gamma_n(G)$ is the set of bases of \mathbb{Z}_p^n as a vector space over \mathbb{Z}_p . These bases are in one-to-one correspondence with matrices in $GL_n(\mathbb{Z}_p)$, and Nielsen moves correspond to elementary row operations. Row operations do not change the determinant of a matrix. It follows that there is one connected component for every value of the determinant. This implies that $\Gamma_n(\mathbb{Z}_p^n)$ has $p-1$ connected components (see [DG]).

2.5. Growth of $\Gamma_n(G)$. Let $S = (g_1, \dots, g_n) \in \Gamma_n(G)$. We write

$$S^{(m)} := (g_1, \dots, g_n, 1, \dots, 1) \in \Gamma_{n+m}(G),$$

and define $\Gamma_{n+m}(G, S)$ to be the connected component of $\Gamma_{n+m}(G)$ containing $S^{(m)}$.

We say G has *exponential Nielsen growth* if $\Gamma_n(G, S)$ has exponential growth for some n and some generating n -tuple S of G . It is easy to show that a finitely generated group G has exponential Nielsen growth if G is either an infinite group of polynomial growth, or a group of exponential growth (see Proposition 3.10). This suggests that every infinite finitely generated group has exponential Nielsen growth:

Conjecture 2.5. *For every infinite finitely generated group G , there is an generating n -tuple $S \in \Gamma_n(G)$ such that $\Gamma_n(G, S)$ has exponential growth.*

Note that this conjecture is a weaker version of Conjecture 1.2. Here we accounted for the possibility that there can be many connected components, and are working with only one of them. Our Main Conjecture 1.1 is also stronger; implicit in it is a reference to a conjecture that every generating k -tuple is connected to a redundant generating k -tuple in $\Gamma_k(G)$. For this and stronger conjectures on connectivity of $\Gamma_k(G)$, see [P1] (see also [BKM]).

3. BASIC RESULTS

3.1. Growth of graphs. We do not need to prove that $B_\Gamma(v, r)$ is large for every single r to conclude that Γ has exponential growth from v . As the following lemma shows, it suffices to prove it for a relatively sparse set of numbers r .

A sequence of positive integers r_1, r_2, \dots is called *log-dense* if it is increasing, and there is a constant β such that $r_{i+1} \leq \beta r_i$ for every $i \geq 1$. In other words, an increasing integer sequence (r_i) is log-dense if the gaps in the sequence $(\log r_i)$ are bounded above.

Lemma 3.1. *Let Γ be a symmetric directed graph, and let v be a vertex of Γ . Suppose that for some constant $\alpha > 1$, there is a log-dense sequence r_1, r_2, \dots such that $|B(v, r_i)| \geq \alpha^{r_i}$ for every $i \geq 1$. Then Γ has exponential growth from v .*

Proof. Since r_i is an increasing sequence of positive integers, we can conclude that for sufficiently large r , there is an i with $r_i \leq r \leq r_{i+1}$. Since $r_{i+1} \leq \beta r_i$, we have $r_i \geq r/\beta$. Thus,

$$|B(v, r)| \geq |B(v, r_i)| \geq \alpha^{r_i} \geq \alpha^{r/\beta},$$

which implies the result. \square

If a graph Γ is a covering of another graph Γ' , and Γ' has exponential growth, then so does Γ .

Proposition 3.2. *Let Γ' and Γ be symmetric directed graphs, and suppose $\phi : \Gamma' \rightarrow \Gamma$ maps the set of neighbors of each vertex $v \in \Gamma'$ surjectively onto the neighbors of $\phi(v)$. Suppose Γ has exponential growth from $\phi(w)$. Then Γ' has exponential growth from w .*

Proof. It suffices to show that ϕ maps $B_{\Gamma'}(w, r)$ onto $B_{\Gamma}(\phi(w), r)$ for all $r \geq 0$, since in that case

$$|B_{\Gamma'}(w, r)| \geq |B_{\Gamma}(\phi(w), r)|.$$

We prove this by induction on r . The base case $r = 0$ is trivial. Suppose

$$\phi(B_{\Gamma'}(w, r)) \supseteq B_{\Gamma}(\phi(w), r),$$

and consider $v \in B_{\Gamma}(\phi(w), r+1)$. We know that v has a neighbor $u \in B_{\Gamma}(\phi(w), r)$, which has a preimage $u' \in B_{\Gamma'}(w, r)$. Since v is a neighbor of u , we know that some neighbor of u' is mapped to v . Therefore, $v \in \phi(B_{\Gamma'}(w, r+1))$, as desired. \square

It is easy to see that if a graph Γ is a subgraph of Γ' , and Γ has exponential growth, so does Γ' . Moreover, we have the following stronger result:

Proposition 3.3. *Let Γ and Γ' be symmetric directed graphs, and suppose $\phi : \Gamma \rightarrow \Gamma'$ sends neighbors to neighbors. Suppose that there is a constant C such that $\#\phi^{-1}(v') \leq C$ for every vertex $v' \in \Gamma'$. Suppose that Γ has exponential growth from w . Then Γ' has exponential growth from $\phi(w)$.*

Proof. It suffices to show that ϕ maps $B_{\Gamma}(w, r)$ into $B_{\Gamma'}(\phi(w), r)$ for all $r \geq 0$, since in that case

$$|B_{\Gamma'}(\phi(w), r)| \geq |B_{\Gamma}(w, r)| / C.$$

We prove this by induction on r . The base case $r = 0$ is trivial. Suppose

$$\phi(B_{\Gamma}(w, r)) \subseteq B_{\Gamma'}(\phi(w), r),$$

and consider $v \in B_{\Gamma'}(\phi(w), r+1)$. We know that v has a neighbor $u \in B_{\Gamma'}(\phi(w), r)$, and $\phi(u) \in B_{\Gamma}(w, r)$. Since u and v are neighbors, and ϕ sends neighbors to neighbors, we see that $\phi(v)$ is a neighbor of $\phi(u)$. It follows that $\phi(v) \in B_{\Gamma}(w, r+1)$, as desired. \square

3.2. Growth of product replacement graphs. Observe that if $m \geq n$ then $\Gamma_n(G, S)$ embeds into $\Gamma_m(G, S)$. Therefore, by Lemma 3.3 if $\Gamma_n(G, S)$ has exponential growth, so does $\Gamma_m(G, S)$.

Moreover, if H is a finitely generated subgroup of G , then every product replacement graph of H embeds in some product replacement graph of G . We can conclude that if a subgroup of G has a product replacement graph of exponential growth, so does G . Formally:

Proposition 3.4. *Let H and G be finitely generated groups with $H < G$. Suppose some connected component of $\Gamma_m(H)$ has exponential growth, and let $S \in \Gamma_n(G)$. Then $\Gamma_{n+m}(G, S)$ has exponential growth. In particular, if $H < G$ and H has exponential Nielsen growth, then G also has exponential Nielsen growth.*

Proof. Let $S = (g_1, \dots, g_n) \in \Gamma_n(G)$. We know that $\Gamma_m(H)$ has exponential growth from some $T \in \Gamma_m(H)$. Let $T = (h_1, \dots, h_m)$. There is a graph embedding $\phi : \Gamma_m(H) \rightarrow \Gamma_{n+m}(G)$ given by

$$\phi(h'_1, \dots, h'_m) = (g_1, \dots, g_n, h'_1, \dots, h'_m).$$

Hence, $\Gamma_{n+m}(G)$ has exponential growth from $\phi(T)$. Since the g_i 's generate G , we know that each h_i is a product of g_i 's and their inverses. Thus, there is a sequence of Nielsen moves $S^{(m)} \rightsquigarrow \phi(T)$, where

$$S^{(m)} = (g_1, \dots, g_n, 1, \dots, 1), \text{ and } \phi(T) = (g_1, \dots, g_n, h_1, \dots, h_m).$$

Therefore, $\Gamma_{n+m}(G, S) = \Gamma_{n+m}(G, \phi(T))$, which implies that $\Gamma_{n+m}(G, S)$ has exponential growth. \square

Similarly, we can show that if a group quotient of G has a product replacement graph of exponential growth, then so does G .

Proposition 3.5. *Let G and H be finitely generated groups, and let $f : G \rightarrow H$ be a surjective group homomorphism. Let $S \in \Gamma_n(G)$. Then the following hold.*

- (1) *Suppose $\Gamma_n(H, f(S))$ has exponential growth. Then $\Gamma_n(G, S)$ has exponential growth.*
- (2) *Suppose some connected component of $\Gamma_m(H)$ has exponential growth. Then $\Gamma_{n+m}(G, S)$ has exponential growth.*
- (3) *Suppose H has exponential Nielsen growth. Then G also has exponential Nielsen growth.*

Proof. For (1), we extend f to a map $\Gamma_n(G) \rightarrow \Gamma_n(H)$ by making the following definition.

$$f(g_1, \dots, g_n) = (f(g_1), \dots, f(g_n)).$$

This map f sends the neighbors of every $T \in \Gamma_n(G)$ surjectively onto the neighbors of $f(T)$. Thus, since $\Gamma_n(H)$ has exponential growth from $f(S)$, we can apply Proposition 3.2, and conclude that $\Gamma_n(G)$ has exponential growth from S .

For (2), let $S = (g_1, \dots, g_n) \in \Gamma_n(G)$, and choose

$$T = (h_1, \dots, h_m) = (f(\tilde{h}_1), \dots, f(\tilde{h}_m)) \in \Gamma_m(H)$$

such that $\Gamma_m(H, T)$ has exponential growth. Then

$$\Gamma_{n+m}(H, (f(g_1), \dots, f(g_n), h_1, \dots, h_m))$$

also has exponential growth. Thus, by (1),

$$\Gamma_{n+m}(G, (g_1, \dots, g_n, \tilde{h}_1, \dots, \tilde{h}_m))$$

has exponential growth. Since the g_i 's generate G , we know that there is a path in $\Gamma_{n+m}(G)$

$$(g_1, \dots, g_n, \tilde{h}_1, \dots, \tilde{h}_m) \rightsquigarrow (g_1, \dots, g_n, 1, \dots, 1) = S^{(m)}.$$

Hence, $\Gamma_{n+m}(G)$ also has exponential growth from $S^{(m)}$, i.e. $\Gamma_{n+m}(G, S)$ has exponential growth. Finally, part (3) follows immediately from (2). \square

In a different direction, if G has a product replacement graph of exponential growth, so does every quotient of H by a finite subgroup.

Proposition 3.6. *Let G and H be finitely generated groups, and let $f : G \rightarrow H$ be a surjective group homomorphism with finite kernel. For every $S \in \Gamma_n(G)$, if $\Gamma_n(G, S)$ has exponential growth, then $\Gamma_n(H, f(S))$ has exponential growth. In particular, if G has exponential Nielsen growth, then H also has exponential Nielsen growth.*

Proof. We extend the map $f : G \rightarrow H$, to the map $f : \Gamma_n(G) \rightarrow \Gamma_n(H)$, given by

$$f(g_1, \dots, g_n) = (f(g_1), \dots, f(g_n)).$$

This map sends neighbors to neighbors, and the preimage of each vertex has bounded size. The graph $\Gamma_n(G)$ has exponential growth from S . Hence, by Proposition 3.3, $\Gamma_n(H)$ has exponential growth from $f(S)$. \square

We summarize the previous three results in the following proposition.

Proposition 3.7. *Let G and G' be finitely generated groups, and suppose G is a subgroup, quotient, or extension by a finite group of G' . If G has exponential Nielsen growth, then G' also has exponential Nielsen growth.*

Remark 3.8. Proposition 3.7 relates the Nielsen growth of a subgroup H of G to the Nielsen growth of G . We conjecture that for any finite index subgroup H of G , if $\Gamma_n(G)$ has exponential growth, then so does $\Gamma_k(H)$ of G , for sufficiently large k . This would imply that the property of having exponential Nielsen growth respects virtual isomorphism. More generally, it would be interesting to see if this property is an invariant under quasi-isometry.

The proposition gives us an easy way to prove that a fairly large class of groups have exponential Nielsen growth.

Lemma 3.9. *Let G be a finitely generated group. Suppose G contains an element of infinite order. For every $S \in \Gamma_n(G)$ and every $m \geq n + 2$, we have that $\Gamma_m(G, S)$ has exponential growth.*

Proof. By assumption, the group G contains a subgroup isomorphic to \mathbb{Z} . It is easy to see that $\Gamma_2(\mathbb{Z})$ has exponential growth (see Example 2.3). By Proposition 3.4, it follows that $\Gamma_{n+2}(G, S)$ has exponential growth, and hence so does $\Gamma_m(G, S)$ for every $m \geq n + 2$. \square

In particular, we can prove that groups of polynomial or exponential growth all have exponential Nielsen growth, which leaves Conjecture 2.5 open only for groups of intermediate growth.

Proposition 3.10. *Let G be an infinite finitely generated group. Suppose that either G has polynomial or exponential growth. Then G has exponential Nielsen growth.*

Proof. Suppose G has polynomial growth. By Gromov's theorem, G is virtually nilpotent [Gro]. It follows that some subgroup of G has infinite abelianization. Thus, G has an element of infinite order and, by Lemma 3.9, G has exponential Nielsen growth.

Now suppose G has exponential growth. Let $S = (g_1, \dots, g_n)$ be a generating n -tuple of G and denote $\Gamma = \Gamma_{n+1}(G, S)$. Let r be any positive integer. For any $g \in B_{G,S}(r)$, the distance between $S^{(1)} = (g_1, \dots, g_n, 1)$ and (g_1, \dots, g_n, g) in Γ is at most r , i.e. $(g_1, \dots, g_n, g) \in B_\Gamma(S, r)$. Thus,

$$|B_\Gamma(S, r)| \geq |B_{G,S}(r)|.$$

But $|B_{G,S}(r)|$ grows exponentially in r , and thus so does $|B_\Gamma(S, r)|$. That is, $\Gamma = \Gamma_{n+1}(G, S)$ has exponential growth, and therefore G has exponential Nielsen growth. \square

Remark 3.11. The Grigorchuk group \mathbb{G} does not have an element of infinite order, so Lemma 3.9 is not enough to show that its product replacement graphs have exponential growth. It can be shown that $\Gamma_n(G)$ has exponential growth for sufficiently large n as long as there are elements of G whose order is exponential in their word length (see [M2]). The Grigorchuk group \mathbb{G} does not satisfy this condition either, but some of the generalized Grigorchuk groups \mathbb{G}_ω do.

3.3. Effective results. The Grigorchuk group has no elements of infinite order, so Lemma 3.9 is not strong enough to prove it has exponential Nielsen growth. We use a different approach. It is enough to find large cubes in G , as follows.

Let G be any group, and let $(g_1, \dots, g_k) \in G^k$, we say the *cube spanned by* (g_1, \dots, g_k) is

$$\mathcal{C}(g_1, \dots, g_k) := \{g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} \mid \varepsilon_i \in \{0, 1\}\}.$$

Observe that $\#\mathcal{C}(g_1, \dots, g_k) \leq 2^n$. We say (g_1, \dots, g_k) is a *cubic k -tuple* if

$$\#\mathcal{C}(g_1, \dots, g_k) = 2^k.$$

Lemma 3.12. *Let G be a finitely generated group, and fix $S \in \Gamma_n(G)$. Let $\alpha > 1$ be a constant, and (k_i) be a log-dense sequence. Suppose for each $i \geq 1$, there is a path γ of length at most αk_i in $\Gamma_n(G)$, such that γ starts at S and visits some $S_1, \dots, S_{k_i} \in \Gamma_n(G)$ in that order. Suppose further that there is a cubic k_i -tuple (g_1, \dots, g_{k_i}) , where $g_j \in S_j$ for each $1 \leq j \leq k_i$. Then $\Gamma_m(G, S)$ has exponential growth for every $m \geq n + 1$.*

Proof. It is enough to show that $\Gamma_{n+1}(G, S)$ has exponential growth. Let $\Gamma = \Gamma_{n+1}(G)$, and $k = k_i$. By Lemma 3.1, it suffices to show that

$$\left| B_\Gamma(S^{(1)}, (\alpha + 1)k) \right| \geq 2^k.$$

Given $(\varepsilon_1, \dots, \varepsilon_k) \in \{0, 1\}^k$, we traverse the path γ in the first n coordinates of $\Gamma_{n+1}(G)$, but when we reach S_j , if $\varepsilon_j = 1$ we also apply a Nielsen transformation to multiply the last entry by g_j . This gives us a path γ' in $\Gamma_{n+1}(G)$ of length at most $\alpha k + k$. The path γ' ends at an element of $\Gamma_{n+1}(G)$ whose last entry is $g_1^{\varepsilon_1} \dots g_n^{\varepsilon_n}$. Since (g_1, \dots, g_k) is cubic, there are 2^k distinct such elements. Thus, we have constructed 2^k distinct elements of $B_\Gamma(S^{(1)}, \alpha k + k)$, as desired. \square

3.4. Connectivity of product replacement graphs. Recall the *Frattini subgroup* $\Phi(G)$,

$$\Phi(G) = \{g \in G \mid \text{if } H \not\leq G, \text{ then } \langle H, g \rangle \not\leq G\}.$$

(see e.g. [Hall, §10.4]). It is easy to see that $\Phi(G)$ is a normal subgroup of G . We need the following connectivity result by Evans (see [Eva, Theorem 4.3]).

Theorem 3.13 (Evans). *Suppose G is generated by some n -tuple. Let $m \geq n + 1$, and suppose $\Gamma_m(G/\Phi(G))$ is connected. Then $\Gamma_m(G)$ is connected.*

It is known that for any finite abelian group G with n generators, the product replacement graph $\Gamma_m(G)$ is connected for every $m > n$ [DG] (see also [P1]). We use only the following special case, which is easy to verify by hand.

Lemma 3.14. *The product replacement graph $\Gamma_m(\mathbb{Z}_2^n)$ is connected for every $m \geq n$.*

In particular, suppose $G/\Phi(G) \cong \mathbb{Z}_2^n$. Then $\Gamma_m(G)$ is connected for every $m > n$.

Remark 3.15. Theorem 3.13 is an analogue for infinite groups of the following result in [LP] (see also [P1]). Let G and H be finite groups with k generators, and $f : G \rightarrow H$ is a surjective group homomorphism, then the extension $f : \Gamma_k(G) \rightarrow \Gamma_k(H)$ is surjective. That is, every generating k -tuple of H lifts to a generating k -tuple of G . As a corollary, if $\Gamma_k(G)$ is connected, then so is $\Gamma_k(H)$. This claim is not true for infinite groups.

4. AUTOMORPHISMS OF THE ROOTED BINARY TREE

In this section, we introduce and discuss properties of the group $\text{Aut}(\mathbf{T})$ of automorphisms of a binary tree.

4.1. Definitions. Let $\mathbf{T} = \{0, 1\}^*$ denote the rooted binary tree consisting of finite strings over the alphabet $\{0, 1\}$, whose root is the empty string, where the children of the string s are $s0$ and $s1$. Define $\text{Aut}(\mathbf{T})$ to be the group of automorphisms of this tree. Formally, $\text{Aut}(\mathbf{T})$ consists of length preserving bijections g of \mathbf{T} such that for any $s, t \in \mathbf{T}$, $g(st)$ begins with $g(s)$. To avoid confusion with the bit 1, we let $\mathbf{i} \in \text{Aut}(\mathbf{T})$ denote the identity element. Let $g \downarrow_s$ denote the action of g on tails of strings beginning with s . In other words, we define it to satisfy $g(st) = g(s)g \downarrow_s(t)$.

Define $a \in \text{Aut}(\mathbf{T})$ to be the automorphism which flips the first bit of s . Formally, $a(0s) = 1s$ and $a(1s) = 0s$ for all $s \in \mathbf{T}$. Clearly, every element of $\text{Aut}(\mathbf{T})$ either fixes 0 and 1 or swaps them. Let g be an element that fixes them. Then $g(0s) = 0g \downarrow_0(s)$ and $g(1s) = 1g \downarrow_1(s)$. In this case, we write g in one of the following two forms, depending on which is more convenient:

$$g = (g \downarrow_0, g \downarrow_1) \quad \text{or} \quad g = \begin{pmatrix} g \downarrow_0 \\ g \downarrow_1 \end{pmatrix}.$$

On the other hand, suppose $g \in \text{Aut}(\mathbf{T})$ swaps 0 and 1. Then $g = a(g \downarrow_0, g \downarrow_1) = (g \downarrow_1, g \downarrow_0)a$. Thus, we can write every element $g \in \text{Aut}(\mathbf{T})$ in the form $(h, k)a^\varepsilon$, for some $h, k \in \text{Aut}(\mathbf{T})$ and some $\varepsilon \in \{0, 1\}$. Moreover $(h, k)a = a(k, h)$ for all $h, k \in \text{Aut}(\mathbf{T})$. In other words, we have $\text{Aut}(\mathbf{T}) = (\text{Aut}(\mathbf{T}) \times \text{Aut}(\mathbf{T})) \rtimes \mathbb{Z}_2$ where \mathbb{Z}_2 acts on $\text{Aut}(\mathbf{T}) \times \text{Aut}(\mathbf{T})$ by swapping the two coordinates.

Let $s \in \mathbf{T}$ be a given binary string. We say the *stabilizer* of s is the subgroup of $\text{Aut}(\mathbf{T})$ consisting of those elements $g \in \text{Aut}(\mathbf{T})$ which fix s :

$$\text{Stab}(s) := \{g \in \text{Aut}(\mathbf{T}) \text{ s.t. } g(s) = s\}.$$

The n -th *level stabilizer* is the subgroup of $\text{Aut}(\mathbf{T})$ consisting of those elements which fix the n -th level of \mathbf{T} :

$$\text{Stab}_n := \bigcap_{s \in \{0,1\}^n} \text{Stab}(s).$$

Let $g \in \text{Stab}_n$. The n -*support* of g is

$$\text{supp}_n(g) = \{s \in \{0,1\}^n \text{ s.t. } g \downarrow_s \neq \mathbf{i}\}.$$

Finally, given $s \in \{0,1\}^n$, we define the *rigid stabilizer* of s to be the subgroup

$$\text{Rist}(s) := \{g \in \text{Stab}_n \text{ s.t. } \text{supp}_n(g) \subseteq \{s\}\}.$$

In other words, $\text{Rist}(s)$ consists of those elements of $\text{Aut}(\mathbf{T})$ which fix every string that does not begin with s .

For a subgroup G of $\text{Aut}(\mathbf{T})$, define

$$\text{Stab}_G(s) = G \cap \text{Stab}(s) \quad \text{and} \quad \text{Rist}_G(s) = G \cap \text{Rist}(s).$$

Note that

$$\begin{aligned} \text{Rist}(0s) &= \{(g, \mathbf{i}) \mid g \in \text{Rist}(s)\} = \text{Rist}(s) \times \{\mathbf{i}\}, \\ \text{and} \quad \text{Rist}(1s) &= \{(\mathbf{i}, g) \mid g \in \text{Rist}(s)\} = \{\mathbf{i}\} \times \text{Rist}(s). \end{aligned}$$

4.2. Growth in subgroups of $\text{Aut}(\mathbf{T})$. For distinct $s, s' \in \{0,1\}^m$, elements of $\text{Rist}(s)$ and $\text{Rist}(s')$ have disjoint n -support. We use Nielsen transformations to reach many of these elements. This implies we can find a large cubic set, which lets us construct many different generating n -tuples.

Lemma 4.1. *Let $G < \text{Aut}(\mathbf{T})$ be finitely generated, and fix a generating n -tuple $S \in \Gamma_n(G)$. Suppose G acts transitively on every level of \mathbf{T} . Suppose there is a constant α such that for every $m \geq 1$, there is a string $s \in \{0,1\}^m$ and a nontrivial element $g \in \text{Rist}_G(s)$ with $\ell(g) \leq \alpha 2^m$. Then $\Gamma_k(G, S)$ has exponential growth for every $k \geq n + 2$*

Proof. Given m , define $L = \{0,1\}^m$ and $N = 2^m$. Fix $s \in L$ such that there is a nontrivial $g \in \text{Rist}_G(s)$, satisfying $\ell(g) \leq \alpha N$. Since G acts transitively on L , we have that the Schreier graph $\text{Schr}_S(G, L)$ is connected. Therefore, $\text{Schr}_S(G, L)$ has a spanning tree \mathcal{T} . Consider a depth-first traversal of \mathcal{T} with respect to the lexicographic order on L , starting at s . This is a path of length $2|L| - 2 < 2N$ which visits every element of L . Suppose it visits them in the order s_1, \dots, s_N . For each $1 \leq i \leq N$, define h_i to be the group element corresponding to the walk along this path from s to s_i , so that $(s_1, \dots, s_N) = (h_1(s), \dots, h_N(s))$. Then we have $\ell(h_2 h_1^{-1}) + \dots + \ell(h_N h_{N-1}^{-1}) \leq 2N = 2^{m+1}$, and $(h_1(s), \dots, h_N(s))$ is a permutation of the elements of L .

Since $g \in \text{Rist}_G(s)$, we have $h_i g h_i^{-1} \in \text{Rist}_G(h_i(s))$, for all $1 \leq i \leq N$. We claim that

$$(h_1 g h_1^{-1}, \dots, h_N g h_N^{-1})$$

is a cubic N -tuple, i.e.

$$\#\left\{ \overrightarrow{\prod}_{i=1 \dots N} (h_i g h_i^{-1})^{\varepsilon_i}, \text{ where } \varepsilon_i \in \{0,1\} \right\} = 2^N.$$

Indeed, the surjection $\phi : \{0,1\}^N \rightarrow \mathcal{C}(h_1 g h_1^{-1}, \dots, h_N g h_N^{-1})$ given by

$$\phi(\varepsilon) := \overrightarrow{\prod}_{i=1 \dots N} (h_i g h_i^{-1})^{\varepsilon_i}$$

is also injective, since $\varepsilon_i = 1$ if and only if $s_i \in \text{supp}_n \phi(\varepsilon)$. Hence $\#\mathcal{C}(h_1 g h_1^{-1}, \dots, h_N g h_N^{-1}) = 2^N$, as desired.

Since $\ell(g) \leq \alpha 2^m$, there is a path γ_1 in $\Gamma_{n+1}(G, S)$ of length at most $\alpha 2^m$

$$S^{(1)} = (g_1, \dots, g_n, 1) \rightsquigarrow (g_1, \dots, g_n, g) = (g_1, \dots, g_n, h_1 g h_1^{-1}).$$

Observe that the distance in $\Gamma_{n+1}(G, S)$ between $(g_1, \dots, g_n, h_i g h_i^{-1})$ and $(g_1, \dots, g_n, h_{i+1} g h_{i+1}^{-1})$ is at most $2\ell(h_{i+1} h_i^{-1})$. Since $\ell(h_2 h_1^{-1}) + \dots + \ell(h_N h_{N-1}^{-1}) \leq 2^{m+1}$, there is a path γ_2 in Γ_{n+1} of length at most 2^{m+2} which starts at (g_1, \dots, g_n, g) and visits each $(g_1, \dots, g_n, h_i g h_i^{-1})$, in that order.

Composing γ_1 and γ_2 , we see that there is a path in $\Gamma_{n+1}(G, S)$ of length at most $(\alpha + 4)2^m$ which starts at $S^{(1)}$ and visits generating $(n + 1)$ -tuples containing $h_1 g h_1^{-1}, \dots, h_N g h_N^{-1}$, in that order. These elements of G form a cubic 2^m -tuple. Applying Lemma 3.12 with $k_m = 2^m$, then, tells us that $\Gamma_k(G, S)$ has exponential growth for all $k \geq n + 2$. \square

Remark 4.2. We cannot replace $\ell(g) \leq \alpha 2^n$ in the hypotheses of this lemma with $\ell(g) \leq \alpha^n$ with some $\alpha > 2$. Roughly speaking, that would only let us reach a cubic 2^n -tuple in α^n steps. Thus, we can only generate an $r^{1/d}$ -cube in $B_\Gamma(S, r)$, where $d = \log_2 \alpha$, which is not sufficient to guarantee exponential growth. We can, however, replace the assumption that $\ell(g) \leq \alpha 2^n$ with the assumption that we can reach a generating $(n + 1)$ -tuple containing g in $\alpha 2^n$ Nielsen moves.

5. THE GRIGORCHUK GROUP

5.1. Definition. The Grigorchuk group $\mathbb{G} < \text{Aut}(\mathbf{T})$ is defined as $\mathbb{G} = \langle a, b, c, d \rangle$, where a flips the first bit of a string, and b, c , and d are defined recursively by the relations

$$\begin{aligned} b &:= (a, c) \\ c &:= (a, d) \\ d &:= (\mathbf{i}, b). \end{aligned}$$

It is easy to check that $a^2 = b^2 = c^2 = d^2 = bcd = \mathbf{i}$. Thus, \mathbb{G} is actually generated by just three elements: $\mathbb{G} = \langle a, b, c \rangle$.

Here is an explicit description of the action of these involutions on \mathbf{T} .

$$\begin{aligned} d(1^n) &= 1^n \\ d(1^n 0s) &= \begin{cases} 1^n 0s, & n \equiv 0 \pmod{3} \\ 1^n 0a(s), & n \equiv 1, 2 \pmod{3} \end{cases} \end{aligned}$$

In other words, d changes at most one bit in a string – the bit after the first 0. Specifically, d flips that bit if and only if the number n of 1's in the string up to that point is 1 or 2 (mod 3). Similarly, c flips it when $n \equiv 0, 2 \pmod{3}$, and b flips it when $n \equiv 0, 1 \pmod{3}$.

Theorem 5.1 (Gigorchuk). *The group \mathbb{G} has intermediate growth.*

The theorem was first proved by Grigorchuk in [G1] (see also [GP, dlH1]).

5.2. Connectivity of $\Gamma_n(\mathbb{G})$. We prove the following result:

Proposition 5.2. *For each $n \geq 4$, the product replacement graph $\Gamma_n(\mathbb{G})$ is connected (see also §7.1).¹*

Proof. Fix $n \geq 4$. It is known that $\mathbb{G}/\Phi(\mathbb{G}) \cong \mathbb{Z}_2^3$ (see [Per] and [G2, §6]). The graph $\Gamma_n(\mathbb{Z}_2^3)$ is connected by Lemma 3.14. Thus, by Lemma 3.13, $\Gamma_n(\mathbb{G})$ is connected. \square

¹After this paper was written, we learned that the proposition was independently derived in [Myr].

5.3. Exponential growth in $\Gamma_n(\mathbb{G})$. The goal of this section is to prove the following result:

Theorem 5.3. *For each $n \geq 5$, the product replacement graph $\Gamma_n(\mathbb{G})$ of the Grigorchuk group has exponential growth.*

The proof is based on Lemma 4.1. Roughly, our strategy is to find an element g of $\text{Rist}_{\mathbb{G}}(1^n)$ with length $O(2^n)$. In $O(2^n)$ more steps, we conjugate g to reach an element of $\text{Rist}_{\mathbb{G}}(s)$ for each s on the same level of \mathbf{T} . Then we can construct every product of these conjugates in $O(2^n)$ steps. There are 2^{2^n} such products, which gives us exponential growth.

Proof of Theorem 5.3. Fix $n \geq 5$. It is easy to check that \mathbb{G} acts transitively on the levels of \mathbf{T} (see e.g. [dlH1, §VIII] or Lemma 6.1, below). By Lemma 4.1, it suffices to show that for every $m \geq 0$, there is a nontrivial element of $\text{Rist}(1^m)$ of length at most 2^{m+4} with respect to the generating 3-tuple (a, b, c) .

Define $t_0 = abab$. Observe that $t_0^2(111) = 110$, and therefore $t_0^2 \neq \mathbf{i}$. We prove by induction on m that there is a $t_m \in \mathbb{G}$ of the form

$$(*) \quad t_m = \overrightarrow{\prod}_{i=1 \dots N} abax_i,$$

where $N = 2^m$, $x_i \in \{b, c, d\}$ for each $1 \leq i \leq 2^m$, such that $t_m^2 \in \text{Rist}_{\mathbb{G}}(1^m)$ and $t_m \downarrow_{1^m} = t_0$. The base case $m = 0$ is trivial.

Given t_m and (x_i) related by $(*)$, for each $0 \leq i \leq N$ we define $x'_i \in \{b, c, d\}$ by $x'_i = (a^{\varepsilon_i}, x_i)$ where $\varepsilon_i \in \{0, 1\}$. We define t_{m+1} by applying the rewriting rules $a \mapsto aba$, $b \mapsto d$, $c \mapsto b$, $d \mapsto c$ to t_m . Then we have

$$t_{m+1} = \left[\overrightarrow{\prod}_{i=1 \dots N} (aba)d(aba)x'_i \right] = \left[\overrightarrow{\prod}_{i=1 \dots N} \begin{pmatrix} c \\ a \end{pmatrix} \begin{pmatrix} \mathbf{i} \\ b \end{pmatrix} \begin{pmatrix} c \\ a \end{pmatrix} \begin{pmatrix} a^{\varepsilon_i} \\ x_i \end{pmatrix} \right] = \begin{pmatrix} a^\varepsilon \\ t_m \end{pmatrix},$$

Thus,

$$t_{m+1}^2 = (\mathbf{i}, t_m^2) \in \{\mathbf{i}\} \times \text{Rist}(1^m) = \text{Rist}(1^{m+1}),$$

and $t_{m+1}^2 \downarrow_{1^{m+1}} = t_m^2 \downarrow_{1^m} = t_0^2$.

Since $t_m^2 \downarrow_{1^m} = t_0^2 \neq \mathbf{i}$, we can conclude that $t_m^2 \neq \mathbf{i}$. Hence, for every $m \geq 0$, we have that t_m^2 is a nontrivial element of $\text{Rist}_{\mathbb{G}}(1^m)$, with $\ell_{\langle a, b, c \rangle}(t_m^2) \leq 2\ell_{\langle a, b, c, d \rangle}(t_m^2) \leq 2^{m+4}$, which concludes the proof. \square

6. THE GENERALIZED GRIGORCHUK GROUPS

In this section, we use the same approach to analyze growth in the product replacement graph of \mathbb{G}_ω . The same techniques apply, but the technical details are more involved.

6.1. Definition. Let ω be an infinite string in the alphabet² $\{b, c, d\}$. The *generalized Grigorchuk group* \mathbb{G}_ω is the group of automorphisms of $\{0, 1\}^n$ given by $\mathbb{G}_\omega = \langle a, b_0, c_0, d_0 \rangle$. Here, the element a flips the first digit of a string, and for each $x \in \{b, c, d\}$, the elements x_n are defined recursively by

$$x_n := (a^\varepsilon, x_{n+1}), \quad \text{where } \varepsilon = \begin{cases} 0, & x = \omega_n \\ 1, & \text{otherwise.} \end{cases}$$

For convenience, we write $b = b_0$, $c = c_0$, and $d = d_0$. As with \mathbb{G} , we have $a^2 = b^2 = c^2 = d^2 = bcd = 1$.

²The usual definition uses the alphabet $\{0, 1, 2\}$ but for our purposes it is more convenient to use $\{b, c, d\}$.

As before, we give a more explicit description of the action of \mathbb{G}_ω on \mathbf{T} . Given $x \in \{b, c, d\}$ and $s \in \mathbf{T}$,

$$x(1^n) = 1^n, \text{ and}$$

$$x(1^n 0s) = \begin{cases} 1^n 0s, & \omega_n = x \\ 1^n 0a(s), & \text{otherwise.} \end{cases}$$

Taking $\omega = dcbdcdbdcdb\dots$ gives the usual Grigorchuk group. The following fact is well-known, but we include a proof here for completeness.

Lemma 6.1. *The generalized Grigorchuk group \mathbb{G}_ω acts transitively on every level of \mathbf{T} .*

Proof. We prove that \mathbb{G}_ω acts transitively on the n -th level by induction on n . This is trivial for $n = 0$, and true for $n = 1$ because $a \in \mathbb{G}_\omega$. For $n > 1$, note that it suffices to show that for each $s \in \{0, 1\}^n$, there is a $g \in \mathbb{G}_\omega$ such that $g(s) = 1^{n-2}00$. Consider $s \in \{0, 1\}^n$. We know that $s = s'd$, for some $s' \in \{0, 1\}^{n-1}$ and $d \in \{0, 1\}$. By the induction hypothesis, \mathbb{G}_ω acts transitively on $\{0, 1\}^{n-1}$. Thus there is a $g \in \mathbb{G}_\omega$ with $g(s') = 1^{n-2}0$. Then either $g(s) = 1^{n-2}00$ or $g(s) = 1^{n-2}01$. In the latter case, there is an $x \in \{b, c, d\}$ such that $\omega_{n-2} \neq x$, and then $x(g(s)) = 1^{n-2}00$. In both cases, there is an $h \in \mathbb{G}_\omega$ with $h(s) = 1^{n-2}00$. \square

6.2. Exponential growth in $\Gamma_n(\mathbb{G}_\omega)$. To prove Theorem 1.3, we first need some lemmas about \mathbb{G}_ω . A standard computation shows that, under some weak assumptions on ω , every element of \mathbb{G}_ω has finite order. We will use the following more specialized result.

Lemma 6.2. *Suppose $\omega_{n-1} = d$. Then in \mathbb{G}_ω , we have $(ad_k)^{2^{n-k+1}} = \mathbf{i}$ for every $0 \leq k < n$.*

Proof. Since $\omega_{n-1} = d$, we have $d_{n-1} = (\mathbf{i}, d_n)$ and $ad_{n-1}a = (d_n, \mathbf{i})$. We prove the lemma by induction on $j = n - k$. When $j = 1$, i.e. $k = n - 1$, we have

$$(ad_k)^4 = [(ad_{n-1}a)d_{n-1}]^2 = \left[\begin{pmatrix} d_n \\ \mathbf{i} \end{pmatrix} \begin{pmatrix} \mathbf{i} \\ d_n \end{pmatrix} \right]^2 = \begin{pmatrix} d_n^2 \\ d_n^2 \end{pmatrix} = \mathbf{i}.$$

When $j > 1$, i.e. $k < n - 1$, the induction hypothesis tells us $(ad_{k+1})^{2^j} = \mathbf{i}$. Note that also $(d_{k+1})^{2^j} = \mathbf{i}$, since d_{k+1} has order 2. Then, for some $\varepsilon \in \{0, 1\}$, we have

$$(ad_k)^{2^{j+1}} = [(ad_k a)d_k]^{2^j} = \left[\begin{pmatrix} d_{k+1} \\ a^\varepsilon \end{pmatrix} \begin{pmatrix} a^\varepsilon \\ d_{k+1} \end{pmatrix} \right]^{2^j} = \begin{pmatrix} (a^\varepsilon d_{k+1})^{-2^j} \\ (a^\varepsilon d_{k+1})^{2^j} \end{pmatrix} = \mathbf{i}.$$

\square

Lemma 6.3. *Suppose $\omega \in \{b, c, d\}^*$ is not eventually constant. Then for each $n \geq 0$, there is a nontrivial $t \in \text{Rist}_{\mathbb{G}_\omega}(1^n)$ with $\ell(t) \leq 2^{n+2}$.*

Proof. This is trivial if $n = 0$. If $n > 1$, then by relabeling b , c , and d if necessary, we may assume $\omega_{n-1} = d$.

By induction on $j = n - k$ we show that for every $0 \leq k \leq n$, there is a t_k of the form

$$t_k = \prod_{i=1 \dots 2^{n-k}}^{\rightarrow} ax_i,$$

where $x_i \in \{b_k, d_k\}$ for each i , and there is an odd number of i 's with $x_i = d_k$, such that $t_k^2 \in \text{Rist}(1^{n-k})$, and $t_k^2 \neq \mathbf{i}$.

For $j = 0$, i.e. $k = n$, we define $t_n = ad_n$. We know that $d_n = (a^\varepsilon, d_{n+1})$ for some $\varepsilon \in \{0, 1\}$, and therefore we have

$$t_n^2 = (ad_n a)d_n = \begin{pmatrix} d_{n+1} \\ a^\varepsilon \end{pmatrix} \begin{pmatrix} a^\varepsilon \\ d_{n+1} \end{pmatrix} = \begin{pmatrix} d_{n+1} a^\varepsilon \\ (d_{n+1} a^\varepsilon)^{-1} \end{pmatrix}.$$

Since ω is not eventually constant, we know that there is an $m \geq n + 1$ with $\omega_m \neq d$. Therefore we have

$$d_{n+1}(1^{m-n-1}00) = 1^{m-n-1}d_m(00) = 1^{m-n-1}0a(0) = 1^{m-n-1}01.$$

Hence, $d_{n+1} \neq \mathbf{i}$. It follows that $d_{n+1}a^\varepsilon$ is nontrivial whether $\varepsilon = 0$ or $\varepsilon = 1$. Therefore, $t_n^2 \neq \mathbf{i}$.

For $j = 1$, i.e. $k = n - 1$, we define $t_k = ab_{n-1}ad_{n-1}$. We have $\omega_k = d$, hence $d_k = (\mathbf{i}, d_{k+1})$ and $b_k = (a, b_{k+1})$. Therefore, we have:

$$t_{n-1}^2 = [(ab_{n-1}a)d_{n-1}]^2 = \left[\begin{pmatrix} b_n \\ a \end{pmatrix} \begin{pmatrix} \mathbf{i} \\ d_n \end{pmatrix} \right]^2 = \begin{pmatrix} \mathbf{i} \\ (ad_n)^2 \end{pmatrix} = \begin{pmatrix} \mathbf{i} \\ t_n^2 \end{pmatrix}.$$

For $j > 1$, i.e. $k < n - 1$, let $N = 2^{n-k-1}$. We have

$$t_{k+1} = \overrightarrow{\prod}_{i=1 \dots N} ax_i$$

from the previous step. For each $1 \leq i \leq N$, we know that $x_i = b_{k+1}$ or d_{k+1} , and we define

$$x'_i = \begin{cases} b_k, & x_i = b_{k+1} \\ d_k, & x_i = d_{k+1}. \end{cases}$$

Then $x'_i = (a^{\varepsilon_i}, x_i)$ for some $\varepsilon_i \in \{0, 1\}$. We have three possibilities:

Case (i): $\omega_k = b$. Then $d_k = (a, d_{k+1})$ and $b_k = (\mathbf{i}, b_{k+1})$. Define

$$t_k = \overrightarrow{\prod}_{i=1 \dots N} ad_k ax'_i.$$

The product has an even number of terms, thus, we have not changed the parity of the number of d_k 's in the product, which implies it is still odd.

$$t_k = \overrightarrow{\prod}_{i=1 \dots N} (ad_k a)x'_i = \overrightarrow{\prod}_{i=1 \dots N} \begin{pmatrix} d_{k+1} \\ a \end{pmatrix} \begin{pmatrix} a^{\varepsilon_i} \\ x_i \end{pmatrix} = \begin{pmatrix} \overrightarrow{\prod} d_{k+1} a^{\varepsilon_i} \\ t_{k+1} \end{pmatrix},$$

where the final product runs over $i = 1 \dots N$. Observe that $\varepsilon_i = 1$ if and only if $x_i = d_i$. There are an odd number of such i , therefore $\overrightarrow{\prod} d_{k+1} a^{\varepsilon_i}$ is a product containing an odd number of a 's and an even number of d_{k+1} 's. The elements d_{k+1} and a have order 2, so the group $\langle d_{k+1}, a \rangle$ is a dihedral group in which they are both reflections. Hence, the product $\overrightarrow{\prod} d_{k+1} a^{\varepsilon_i}$ is also a reflection in that dihedral group, and thus it has order 2. Therefore, $t_k^2 = (\mathbf{i}, t_{k+1}^2)$.

Case (ii): $\omega_k = d$. Then $d_k = (\mathbf{i}, d_{k+1})$ and $b_k = (a, b_{k+1})$. Define

$$t_k = \overrightarrow{\prod}_{i=1 \dots N} ab_k ax'_i,$$

and argue as in case (i).

Case (iii): $\omega_k = c$. Then $d_k = (a, d_{k+1})$ and $b_k = (a, b_{k+1})$. Hence $x'_i = (a, x_i)$ for each $0 \leq i \leq N$. We can again define

$$t_k = \overrightarrow{\prod}_{i=1 \dots N} ad_k ax'_i.$$

Then

$$t_k = \overrightarrow{\prod}_{i=1 \dots N} (ad_k a)x'_i = \overrightarrow{\prod}_{i=1 \dots N} \begin{pmatrix} d_{k+1} \\ a \end{pmatrix} \begin{pmatrix} a \\ x_i \end{pmatrix} = \begin{pmatrix} (d_{k+1}a)^N \\ t_{k+1} \end{pmatrix}.$$

By Lemma 6.2, we have $(d_{k+1}a)^{2N} = (d_{k+1}a)^{2^{n-k}} = \mathbf{i}$. Hence, $t_k^2 = (\mathbf{i}, t_{k+1}^2)$.

In all three cases, $t_k^2 = (\mathbf{i}, t_{k+1}^2)$. It follows that t_k^2 is nontrivial and

$$t_k^2 \in \{\mathbf{i}\} \times \text{Rist}(1^{n-k-1}) = \text{Rist}(1^{n-k}).$$

Thus, we have a nontrivial $t_0^2 \in \text{Rist}(1^n) \cap \mathbb{G}_\omega$, with $\ell(t_0^2) \leq 2^{n+2}$, as desired. \square

Proof of Theorem 1.3. It is known that $\mathbb{G}_\omega/\Phi(\mathbb{G}_\omega) \cong \mathbb{Z}_2^k$ for some $k \leq 3$ [Per] (see also [G2, §6]). Recall from Lemma 3.14 that $\Gamma_n(\mathbb{Z}_2^k)$ is connected. Lemma 3.13 tells us that $\Gamma_n(\mathbb{G}_\omega)$ is connected for each $n \geq 4$.

Assume that ω is eventually constant. Then it is not hard to check that \mathbb{G}_ω has polynomial growth. In fact, G_ω is virtually abelian [G2, §2]. It follows that G_ω has an element of infinite order. The group \mathbb{G}_ω is generated by three elements, $\mathbb{G}_\omega = \langle a, b, c \rangle$. By Lemma 3.9, this implies that the product replacement graph $\Gamma_n(\mathbb{G}_\omega)$ has exponential growth for each $n \geq 5$.

Otherwise, if ω is not eventually constant, for every $m \geq 0$, Lemma 6.3 gives a nontrivial $t \in \text{Rist}_{\mathbb{G}_\omega}(1^m)$ of length at most 2^{m+2} . Since \mathbb{G}_ω acts transitively on the levels of \mathbf{T} , we can apply Lemma 4.1 to conclude that $\Gamma_6(\mathbb{G}_\omega)$ has exponential growth from $(a, b, c, d, 1, 1)$.

Moreover, note that the group \mathbb{G}_ω is generated by (a, b, c) , and rewriting t as a word in these generators at most doubles its length. Thus, we also have that $\Gamma_5(\mathbb{G}_\omega)$ has exponential growth from $(a, b, c, 1, 1)$. It follows that $\Gamma_n(\mathbb{G}_\omega)$ has exponential growth for each $n \geq 5$. \square

7. FINAL REMARKS

7.1. There are several other directions in which our Theorem 5.3 can be extended. First, there is the problem of smaller k : we believe that $\Gamma_3(\mathbb{G})$ is connected (cf. Lemma 3.14 and Proposition 5.2).³ Moreover, it is conceivable that both $\Gamma_3(\mathbb{G})$ and $\Gamma_4(\mathbb{G})$ have exponential growth, the cases missing from Theorem 5.3.

Similarly, in case Conjecture 1.4 proves too difficult, there is a weaker and perhaps more accessible open problem.

Conjecture 7.1. *The nearest neighbor random walk on $\Gamma_k(\mathbb{G})$ has positive speed, for all $k \geq 5$.*

The speed of r.w. is defined as the limit of $\mathbb{E}[\text{dist}(t)/t]$ as $t \rightarrow \infty$, where $\text{dist}(t)$ is the distance of the r.w. after t steps, from the starting vertex. It is known that non-amenable graphs have positive speed, but so do some amenable graphs, such as the standard Cayley graph of the lamplighter group $\mathbb{Z}_2 \wr \mathbb{Z}^3$ (see e.g. [Pete, Woe]). We believe it might be possible to extend our approach to establish the positive speed of r.w. on $\Gamma_k(\mathbb{G})$, and we intend to return to this problem.

7.2. It is easy to check that if $\text{Aut}(G)$ has a finitely generated subgroup $A = \langle \phi_1, \dots, \phi_k \rangle$ of exponential growth, then for any $S = (s_1, \dots, s_n) \in \Gamma_n(G)$, the graph $\Gamma_{2n}(G, S)$ has exponential growth. Indeed, for any $\psi \in A$ with $\ell(\psi) \leq r$, we have that $(\psi(s_1), \dots, \psi(s_n), 1, \dots, 1)$ is within $O(r)$ Nielsen moves of $(s_1, \dots, s_n, 1, \dots, 1)$, since there are paths of bounded length

$$\begin{aligned} (\psi(s_1), \dots, \psi(s_n), 1, \dots, 1) &\rightsquigarrow (\psi(s_1), \dots, \psi(s_n), \psi(\phi_i(s_1)), \dots, \psi(\phi_i(s_n))) \\ &\rightsquigarrow (1, \dots, 1, \psi(\phi_i(s_1)), \dots, \psi(\phi_i(s_n))) \\ &\rightsquigarrow (\psi(\phi_i(s_1)), \dots, \psi(\phi_i(s_n)), 1, \dots, 1). \end{aligned}$$

Unfortunately, this assumption does not hold for the Grigorchuk group (see [GS]).

³See also Corollary 1.2 and Question 1 in [Myr].

7.3. It is tempting to try to prove that the Grigorchuk group \mathbb{G} has exponential Nielsen growth by extending the observation in Subsection 7.2 to endomorphisms rather than automorphisms. In order to show that \mathbb{G} has exponential Nielsen growth, it is enough to show that some subgroup K of \mathbb{G} has exponential Nielsen growth. Indeed, there is a finite index subgroup $K = \langle t, v, w \rangle$ of \mathbb{G} which satisfies $K \times K \subset K$ (see [dlH1, §VIII.30]). It follows that K has a free monoid of endomorphisms, generated by ϕ_0 and ϕ_1 . Then, for any word ψ in ϕ_0 and ϕ_1 with $\ell(\psi) \leq r$, one might hope that $(t, v, w, \psi(t), \psi(v), \psi(w), 1, 1, 1)$ is within $O(r)$ Nielsen moves of $(t, v, w, 1, 1, 1, 1, 1, 1)$. This would be the case if the following paths had bounded length:

$$\begin{aligned} (t, v, w, \psi(t), \psi(v), \psi(w), 1, 1, 1) &\rightsquigarrow (t, v, w, \psi(t), \psi(v), \psi(w), \psi(\phi_i(t)), \psi(\phi_i(v)), \psi(\phi_i(w))) \\ &\rightsquigarrow^* (t, v, w, 1, 1, 1, \psi(\phi_i(t)), \psi(\phi_i(v)), \psi(\phi_i(w))) \\ &\rightsquigarrow (t, v, w, \psi(\phi_i(t)), \psi(\phi_i(v)), \psi(\phi_i(w)), 1, 1, 1). \end{aligned}$$

However, it is not clear that the “cleanup” step marked with $*$ can be done in a bounded number of Nielsen moves. Hence, unfortunately, the fact that \mathbb{G} has a finite index subgroup with a free monoid of endomorphisms is not enough to conclude that \mathbb{G} has exponential Nielsen growth.

7.4. The connectivity of product replacement graphs is delicate already for finite groups. For example, Dunwoody showed in [Dun], that if G is a finite solvable group with d generators, then $\Gamma_k(G)$ is connected, for every $k > d$ (see also [P1]). This property is conjectured to hold for all finite groups, but fails for infinite groups, even for metabelian groups (see [P1] and references therein).

As of now, is unknown whether for any finitely generated group G , graphs $\Gamma_k(G)$ are connected for all sufficiently large k . It is not even known that if $\Gamma_k(G)$ is connected then $\Gamma_{k+1}(G)$ is connected. The difficulty arises from the possibility that $\Gamma_{k+1}(G)$ has a connected component which consists of non-redundant generating $(k+1)$ -tuples. However, it is not hard to check that in $\Gamma_{2d}(G)$ every element of the form $(g_1, \dots, g_d, 1, \dots, 1)$ lies in the same connected component, which we may call $\Gamma_{2d}^*(G)$. Then if we know that some connected component of $\Gamma_d(G)$ has exponential growth, we know that $\Gamma_{2d}^*(G)$ has exponential growth.

7.5. Finally, let us mention that the notion of exponential Nielsen growth may be applicable to sequences of finite groups, which stabilize in a certain sense. Proving such a result would be a step towards proving expansion of product replacement graphs of general finite groups (see [P1, P2]). We refer to [Bla] for the notion of growth of finite groups, and to [Ell] for a recent conceptual approach.

Acknowledgements. The authors are grateful to Tatiana Nagnibeda who brought to our attention a question on connectivity and exponential growth of $\Gamma_k(\mathbb{G})$, and help with the references. We are also very thankful to Slava Grigorchuk and Martin Kassabov for interesting conversations on groups of intermediate growth, and to Yehuda Shalom for helpful remarks on uniform growth. The second author was partially supported by the BSF and the NSF.

REFERENCES

- [Adi] S. Adian, *The Burnside problem and identities in groups*, Springer, Berlin, 1979.
- [A+] G. N. Arzhantseva, J. Burillo, M. Lustig, L. Reeves, H. Short and E. Ventura, Uniform non-amenability, *Adv. Math.* **197** (2005), 499–522
- [Bar] L. Bartholdi, Groups of intermediate growth, [arXiv:0201293](https://arxiv.org/abs/0201293).
- [BL] H. Bäärnhielm and C. R. Leedham-Green, The product replacement prospector, *J. Symbolic Comput.* **47** (2012), 64–75.
- [BS] I. Benjamini and O. Schramm, Percolation beyond \mathbb{Z}^d , many questions and a few answers, *Electron. Comm. Probab.* **1** (1996), 71–82.
- [Bla] S. Black, Asymptotic growth of finite groups, *J. Algebra* **209** (1998), 402–426.
- [BKM] A. V. Borovik, E. I. Khukhro and A. G. Myasnikov, The Andrews-Curtis Conjecture and Black Box Groups, *Int. J. Algebra Comput.* **13** (2003), 415–436.

- [BLM] A. V. Borovik, A. Lubotzky and A. G. Myasnikov, The finitary Andrews-Curtis conjecture, in *Progr. Math.* **248**, Birkhäuser, Basel, 2005, 15–30.
- [BG] E. Breuillard and T. Gelander, Uniform independence in linear groups, *Invent. Math.* **173** (2008), 225–263.
- [BP] K. Bux and R. Pérez On the growth of iterated monodromy groups, *Contemp. Math.* **394** (2006), 61–76.
- [dlH1] P. de la Harpe, *Topics in Geometric Group Theory*, University of Chicago Press, Chicago, 2000.
- [dlH2] P. de la Harpe, Uniform growth in groups of exponential growth, *Geom. Dedicata* **95** (2002), 1–17.
- [DG] P. Diaconis and R. Graham, The graph of generating sets of an abelian group, *Colloq. Math* **80** (1999), 31–38.
- [Dun] M. J. Dunwoody, Nielsen transformations, in *Computational Problems in Abstract Algebra*, Pergamon Press, Oxford, 1970, 45–46.
- [Ell] J. S. Ellenberg, Superstrong approximation for monodromy groups, [arXiv:1210.3757](https://arxiv.org/abs/1210.3757).
- [Eva] M. J. Evans, Presentations of groups involving more generators than are necessary, *Proc. LMS* **67** (1993), 106–126.
- [G1] R. I. Grigorchuk, Degrees of growth of finitely generated groups, and the theory of invariant means, *Izv. Akad. Nauk SSSR Ser. Mat.* **48** (1984), 939–985.
- [G2] R. I. Grigorchuk, Solved and unsolved problems around one group, in *Infinite Groups: Geometric, Combinatorial and Dynamical Aspects*, Birkhäuser, Basel, 2005, 117–218.
- [G3] R. I. Grigorchuk, Some problems of the dynamics of group actions on rooted trees, *Proc. Steklov Inst. Math.* **273** (2011), 64–175.
- [GP] R. I. Grigorchuk and I. Pak, Groups of intermediate growth, an introduction, *L’Ens. Math.* **54** (2008), 251–272.
- [GS] R. I. Grigorchuk and S. N. Sidki, The group of automorphisms of a 3-generated 2-group of intermediate growth, *Internat. J. Algebra Comput.* **14** (2004), 667–676.
- [Gro] M. Gromov, Groups of polynomial growth and expanding maps, *IHES Publ. Math.* **53** (1981), 53–78.
- [GL] F. Grunewald and A. Lubotzky, Linear representations of the automorphism group of a free group, *Geom. Funct. Anal.* **18** (2009), 1564–1608.
- [GS] N. Gupta and S. Sidki, On the Burnside problem for periodic groups, *Math. Z.* **182** (1983), 385–388.
- [Hall] M. Hall, *The Theory of Groups*, Chelsea, New York, 1976.
- [KP] M. Kassabov and I. Pak, Groups of oscillating intermediate growth, *Ann. Math.* **177** (2013), 1113–1145.
- [Lub] A. Lubotzky, *Discrete Groups, Expanding Graphs, and Invariant Measures*, Birkhäuser, Basel, 1994.
- [LP] A. Lubotzky and I. Pak, The product replacement algorithm and Kazhdan’s property (T), *J. AMS* **14** (2001), 347–363.
- [LŽ] A. Lubotzky and A. Žuk, *On property (τ)* , monograph in preparation.
- [M1] A. Malyshev, Non-amenability of product replacement graphs, in preparation.
- [M2] A. Malyshev, *Combinatorics of finitely generated groups*, Ph.D. thesis, UCLA, in preparation.
- [Met] W. Metzler, On the Andrews-Curtis conjecture and related problems, in *Contemp. Math.* **44**, AMS, Providence, RI, 1985, 35–50.
- [Mil] J. Milnor, Growth of finitely generated solvable groups, *J. Diff. Geom.* **2** (1968), 447–449.
- [MP] R. Muchnik and I. Pak, Percolation on Grigorchuk groups, *Comm. Algebra* **29** (2001), 661–671.
- [Myr] A. Myropolska, Andrews–Curtis and Nielsen equivalence relations on some infinite groups, [arXiv:1304.2668](https://arxiv.org/abs/1304.2668).
- [Nek] V. Nekrashevych, Iterated monodromy groups, *London Math. Soc. Lecture Note Ser.* **387** (2011), 41–93.
- [NP] A. C. Niemeyer and C. E. Praeger, Complexity and computation in matrix groups, in *Aspects of Complexity*, de Gruyter, Berlin, 2001, 87–113.
- [P1] I. Pak, What do we know about the product replacement algorithm?, in *Groups and Computation III*, de Gruyter, Berlin, 2001, 301–347.
- [P2] I. Pak, The product replacement algorithm is polynomial, in *Proc. FOCS 2000*, IEEE Comput. Soc. Press, Los Alamitos, CA, 2000, 476–485.
- [Per] E. L. Pervova, Everywhere dense subgroups of one group of tree automorphisms, *Tr. Mat. Inst. Stekl.* **231** (2000), 356–367.
- [Pete] G. Pete, *Probability and Geometry on Groups*, Lecture notes for a graduate course, 2013, 203 pp.; available at <http://www.math.bme.hu/~gabor/PGG.pdf>
- [Wil] J. S. Wilson, On exponential growth and uniformly exponential growth for groups, *Invent. Math.* **155** (2004), 287–303.
- [Woe] W. Woess, *Random walks on infinite graphs and groups*, Cambridge U. Press, Cambridge, 2000.