RANDOMIZING AND DESCRIBING GROUPS

By

Meng-Che Ho

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2017

Date of final oral examination: April 19, 2016

The dissertation is approved by the following members of the Final Oral Committee:

Professor U. Andrews, Assistant Professor, Mathematics

Professor T. Dymarz, Assistant Professor, Mathematics

Professor S. Lempp, Professor, Mathematics

Professor J. S. Miller, Professor, Mathematics

Professor N. Boston, Professor, Mathematics and ECE

Abstract

In this work we study some topics in logic and group theory, and naturally, their intersection. One important theme in this work is the notion of random groups, which is informally the study of "what properties do 'most' groups satisfy?"

In Chapter 2, we are interested in the theory of a random group, i.e., the properties we are interested here are first-order properties. Knight conjectured that the limit of the theories of random groups should converge to the theory of the free groups. In this chapter, we establish some partial results in the one-quantifier case.

In Chapter 3, instead of looking at a random group, we focus our attention on only the class of nilpotent groups, and look at a random nilpotent group. We analyze the distribution of ranks of random nilpotent groups, and establish some threshold result on when a random nilpotent group will be finite and trivial.

In Chapter 4, we turn our attention to regular (non-random) groups, and we study the complexities of Scott sentences and the index sets of groups. We show that many groups that are "tame" in the sense of group theory have low-complexity Scott sentences and index sets.

Acknowledgments

First, I would like to thank my advisors Uri Andrews and Tullia Dymarz. They have been really supportive and allowed me to investigate whatever topics I liked, while also giving me valuable guidance for existing projects and providing me with ample opportunities to learn more. They were also the most important sources of my guilt and pressure, which kept me from procrastinating too much.

I would also like to thank Moon Duchin, who not only collaborated with me on all the work done in the Chapter 3, but also acted like my third advisor and gave me a lot of ideas in other projects. I also want to thank my other collaborators Andrew P. Sánchez, Yen Duong, and Matthew Cordes, who tolerated my lack of rigor. In particular, I want to thank Khalid Bou-Rabee for a short but very useful discussion we had.

Thanks to Julia Knight, Melanie Matchett Wood, Dylan Thurston, Ilya Kapovich, Larry Guth, Alexei Myasnikov, Arnold Miller, Nathan Dunfield, Nigel Boston, Will Cocke, Steffen Lempp, and Joseph Miller for their useful suggestions and other various forms of help. I also want to mention my office mates (and floor mates), including Ting-Ting Nan, Eric Ramos, and Nathan Clement for being so willing to chat with me no matter what the weather it was outside. Special thanks to James Waddington for copy-editing my thesis.

Last but no least, I want to thank all my friends, my family, my parents, and my wife Chi Chang. They made my happy hours a lot happier, and made my hard hours a lot less hard. Without them I would not have been able to finish my graduate degree.

Contents

Chapter 1

Introduction

This work is centered around logic and group theory. Historically, there has been a lot of interaction between the two areas, including many decision problems on groups, Tarski's problem, and the study of stable groups, just to name a few. The author is interested in both of these areas, and so naturally, very interested in the intersection of them.

This work includes the study of the theory of random groups in Chapter 2, the study of random nilpotent groups in Chapter 3, and the study of computability notions of groups in Chapter 4. Each of these chapters is written to be self-contained. However, we assume the reader to have the basic knowledge about groups and logic which is usually covered in a first graduate course on these topics.

One important background idea in this work is the notion of *random groups*. Here the word *random* is in the (geometric) group theory sense, which is usually quite different from the notion of randomness in the computability sense. Informally, we start with the free group F_m of rank m, and uniformly independently pick $R = R(\ell)$ random elements of length ℓ to be our relators. Then we can ask what is the (limit of the) probability (as $\ell \to \infty$) of the resulting group (or really, the group-valued random variable) has some given property.

We see that here, we are really choosing group presentations instead of isomorphism types. It is actually non-trivial (but true) that we do see different isomorphism types in this process. Also, we only see m-generated finitely-presented groups (for a fixed m) in this construction. In spite of these flaws, this is the standard model of random groups. In the case where $R(\ell)$ is a constant function, we have the *few-relator model*, which is the model that we will focus on in Chapter 2 and 3.

In Chapter 2, we study the theory of a random group, i.e., the properties that we are interested are the first-order properties. Knight conjectured that the limit of the theories of the random groups should be the theory of the free groups. Using some small cancellation theory, we show that this is indeed the case when we are looking at existential sentences, i.e., every existential sentences that is true in the free group is also true (asymptotically) in a random group. We also show this is true for some universal sentences, but we also show a negative result saying that if we take the countable conjunction of all universal sentences true in the free group (i.e. the universal theory), this countable conjunction is false (asymptotically) in a random group with enough relators.

Chapter 3 is joint work with Matthew Cordes, Moon Duchin, Yen Duong, and Andrew P. Sánchez. In this chapter, we are still interested in random groups, but instead of starting with a free group, we start with a free nilpotent group. Thus, we only see finitely-generated nilpotent groups of a certain rank and class as our random nilpotent groups. We are able to deduce statements about the distribution of ranks for random nilpotent groups as well as the probability that random nilpotent groups are abelian. Considering the abelianization also yields the precise vanishing threshold for random nilpotent groups—the analog of the famous density one-half theorem for random groups. A random nilpotent group is trivial if and only if the corresponding random group is perfect, i.e., is equal to its commutator subgroup, so this gives a precise threshold at which random groups are perfect.

In Chapter 4, we turn our attention to usual (non-random) groups, and we study the complexities of Scott sentences and index sets. A Scott sentence of a group is an $\mathcal{L}_{\omega_1,\omega}$ sentence whose countable models are isomorphic copies of the group. The index set of a group is the collection of the indices of the isomorphic copies of the group. This has been studied by Knight et al., and we generalize many of their results. We give computable Scott sentences for many groups, including polycyclic groups, certain solvable groups, and certain subgroups of $\mathbb{Q}$. In some of these cases, we also show that the Scott sentences we find are optimal. We also give an example showing d-$\Sigma_2 \subsetneq \Delta_3$ in the complexity hierarchy of pseudo-Scott sentences, contrasting the result saying d-$\boldsymbol{\Sigma}_2 = \boldsymbol{\Delta}_3$ in the complexity hierarchy of Scott sentences, which is related to the boldface Borel hierarchy.

Chapter 2

The 0-1 Conjecture for Groups

2.1 Introduction

The idea of random groups is motivated by a question of Gromov: What does a typical group look like? To make sense of this question, we need to put a measure on the class of all groups, and we usually call such a measure a *model* of random groups. To do this, we will restrict our attention to finitely-presented groups only, and we actually pick presentations instead of isomorphism types.

Definition 2.1. *Fix ℓ and a function $f : \mathbb{N} \to \mathbb{N}$. Let F_m denote the free group of rank m, and let $S_\ell \subset F_m$ be the set of elements of length ℓ. Randomly choose $f(\ell)$ elements from S_ℓ uniformly and independently. In the case where $f(\ell) = n$ is a constant function, this is the* few-relator (n-relator) model, *while if $f(l) = (2m-1)^{d\ell}$, this is called the* density model at density d. *We say* a random group has some property, *if the probability that the group F_m/R has said property goes to 1 as ℓ goes to infinity. In this chapter, we will focus our attention on the few-relator model.*

A random group behaves a lot like a free group. For example, a random group has the $C'(\lambda)$ small cancellation property for any $\lambda > 0$, thus is non-elementary hyperbolic and torsion-free [16]. A random group also contains many free subgroups [9].

Indeed, Knight conjectured that a random group also looks like a free group in the model-theoretic sense:

Conjecture 2.2 (0-1 conjecture of groups, Knight, 2013)**.** *For every first-order sentence ϕ (in the language of groups), if the free groups model the sentence, then the random group also models the sentence.*

Sela [34] and Kharlampovich-Myasnikov [19] independently proved that the elementary theories of non-abelian finitely-generated free groups are equivalent. Thus, it makes sense to say the free groups model a sentence without specifying the rank of the free groups.

Note that there is no a priori reason why the limit of the probability that a group modeling a sentence should equal to 0 or 1, or even converge at all, and the conjecture is also making the statement that these limits do converge.

In Section 2.2, we will give a quick review on some basic facts on small cancellation properties, then give a proof on the existential case of the conjecture. In Section 2.3, we give some partial results on the universal case.

2.2 Small Cancellation Theory and the Existential Case

There are various results on the existence of free subgroups of a random group. And if a group contains a free subgroup, then it certainly models all existential sentences that the free groups model. However, here we will give a proof of the conjecture in the case the ϕ is existential that does not depend on the free subgroup result. Instead, we will use small cancellation theory to prove it.

We first review the definition of the $C'(\lambda)$ small cancellation hypothesis and the Greendlinger's lemma. We refer the reader to [28] for more detail on small cancellation theory.

Definition 2.3. *Let $R \subset F_m$ be* symmetrized*, i.e. all elements of R are all cyclically reduced and R is closed under inverse and cyclic permutation.*

We say u is a piece *of R if there are two distinct elements $r, s \in R$ such that u is an initial segment of both r and s. We say R satisfies* small cancellation hypothesis $C'(\lambda)$ *if for every $r \in R$ and piece u that is also an initial segment of r, $|u| < \lambda|r|$.*

We also say a non-symmetrized $S \subset F_m$ satisfies small cancellation hypothesis $C'(\lambda)$ if R does, where R is obtained by taking the cyclic reduction of the words in S and is closed under inverse and cyclic permutation. We also say a group presentation satisfies small cancellation hypothesis $C'(\lambda)$ if its relator set does.

To show a random group satisfies small cancellation hypothesis, we can use a direct counting argument. There are $O((2m-1)^{n\ell})$ ways to pick n relators of length ℓ. However, the number of ways to have a "piece" of length $\lambda\ell$ in these relators is $O(n^2 l^2 (2m-1)^{n\ell-\lambda\ell})$. Thus, as $\ell \to \infty$, the probability of having a piece of length $\lambda\ell$ goes to 0, and we have the following result:

Theorem 2.4. *([28]) A random group satisfies small cancellation hypothesis $C'(\lambda)$ for any $0 < \lambda < 1$.*

One important consequence of a group satisfying the small cancellation property is Greendlinger's lemma, which basically says that in a small cancellation group, every word that is equal to the identity contains a big chunk of some relator.

Theorem 2.5 (Greendlinger's lemma, [24]). *Let $R \subset F_m$ satisfy $C'(\lambda)$ for some $\lambda < \frac{1}{6}$. Let $w \in \langle\!\langle R \rangle\!\rangle$ be a non-trivial, cyclically reduced word, where $\langle\!\langle R \rangle\!\rangle$ is the normal closure of R in F_m. Then there is a subword u of some $r \in R$ such that u is also a subword of w and $|u| > (1 - 3\lambda)|r|$.*

Theorem 2.6 (Existential case). *For every existential sentence ϕ, if $F_m \vDash \phi$, then a random group models ϕ.*

Proof. Without loss of generality, let $\phi = \exists \overline{x} \bigwedge (u_i(\overline{x}) = 0 \wedge v_i(\overline{x}) \neq 0)$, and let $\overline{a} \in F_m$ be a witness. Then in a (random) group $G = F/R$, $u_i(\overline{a})$ is always trivial, so $G \vDash \phi$ if $v_i(\overline{a}) \neq 0$.

By Greendlinger's lemma, the length of a nonzero word in the normal closure has to be no shorter than the length of the relators. Hence for each $v_i(\overline{a})$, as the length of the relators go to infinity, a random group will not kill the witness, hence models ϕ. □

2.3 The Universal Case

In this section, we take a look at certain universal sentences that are true in free groups, and see that they are also true in a random group. However, we also show that a random group (with enough relators) is not a limit group, i.e. it does not model the universal theory of the free group. Note that this does not disprove the conjecture – it could still be the case that the portions of groups that model each universal sentence that is true in the free groups are big, but the intersection of them are small (as there are countably many sentences).

We start by looking at some properties that are related to the universal theory of the free group.

Definition 2.7 ([33]). *We say a group G is a* limit group *if it is finitely-generated and G models the universal theory of the free groups.*

Definition 2.8. *We say a group G is* residually free *if for every $1 \neq g \in G$, there exists a homomorphism $f : G \to F_m$ such that $f(g) \neq 1$.*

Definition 2.9. *We say a group G is* commutative-transitive *if for every $x \neq 1$ and $y, z \in G$, if $[x, y] = [x, z] = 1$, then $[y, z] = 1$. Note that this is equivalent to the universal sentence $\forall x, y, z\,[(x \neq 1 \wedge [x, y] = 1 \wedge [x, z] = 1) \to [y, z] = 1]$.*

Theorem 2.10 (Baumslag, [2]). *A residually free commutative-transitive finitely-generated group is a limit group.*

We will now show that a random group is commutative-transitive, but not residually free, thus not a limit group. Recall that a random group is torsion-free. In the few-relator case, this can be shown using small cancellation theory and some counting. We will omit the proof here.

Theorem 2.11 ([16], [28]). *A random group is non-elementary torsion-free hyperbolic.*

Remark 2.12. *By a result of Sela [35], a non-elementary torsion-free hyperbolic group is stable (in the sense of model theory). Thus a random group is stable.*

Theorem 2.13. *A random group G has the following property: if $x, y \in G$ commute, then there is a $w \in G$ such that x and y are both powers of w. Therefore, a random group is commutative-transitive.*

Proof. If two non-trivial elements x and y of a random group commute, the subgroup generated by them is either $\mathbb{Z}^2$ or $\mathbb{Z}$, since a random group has no torsion elements.

However, being a torsion-free hyperbolic group, a random group does not have $\mathbb{Z}^2$ subgroups [6], so x and y generate a subgroup isomorphic to $\mathbb{Z}$. We can take w to be the generator of $\mathbb{Z}$, and the theorem follows. □

We now show that a random group (with enough relators) is not a limit group.

Theorem 2.14. *An m-generator, n-relator random group is not residually free if $m \leq n+1$. Therefore, it is not a limit group.*

Proof. It is well known that free groups are residually p-finite for all p, i.e. for every element g in the group, there is a homomorphism f from the group to a p-group such that $f(g) \neq 1$. Thus it suffices for us to prove that a random group is not residually p-finite for some p.

We first consider the abelianization of the relator of a random group. The abelianization of a random word is just an ℓ-step random walk on $\mathbb{Z}^m$, and the probability of the endpoints of n random walks being linearly independent goes to 1 as $\ell \to \infty$, because their distribution is normal and linear dependence is a codimension-one condition (see Chapter 3 for more on random walks in $\mathbb{Z}^m$.) Thus, the abelianization of a random group is either finite or is a direct product of $\mathbb{Z}$ with a finite group.

Fix a prime p that does not divide the order of the torsion part of the abelianization. Consider a homomorphism $f : G \to P$ for some p-group P. By replacing P by the image of f, we may assume f is surjective. Consider the following commuting diagram:

$$\begin{tikzcd}
G \arrow[r, two heads, "\mathrm{ab}_G"] \arrow[d, "f"] & \mathrm{ab}(G) \arrow[d, "g"] \\
P \arrow[r, two heads, "\mathrm{ab}_P"] & \mathrm{ab}(P)
\end{tikzcd}$$

Since P is a p-group, the torsion part of $\mathrm{ab}(G)$ does not contribute to the homomorphism g. Also, f, ab_P are both surjective, and so is g. Thus $\mathrm{ab}(P)$ is 1-generated. However, by a theorem of Magnus [25], any subset of a nilpotent group that generates its abelianization also generates the group itself. Thus, P is 1-generated.

Now since a random group is non-abelian, there is a nontrivial element $x \in G'$. Then for every homomorphism f from G to a p-group, the image is abelian, hence $f(x) = 1$, proving G cannot be residually p-finite. □

As was observed earlier, this theorem does not disprove the conjecture. It is still possible that for each of the universal sentences true in the free groups, the portion of groups modeling the sentence has density one, but the universal theory of the free groups, which is a "conjunction" of countably many universal sentences, is only modeled by a set of groups that has density zero.

In the future, we would like to investigate more in this direction, and try to either prove or disprove the conjecture, and understand more about the model theory of the random groups.

Chapter 3

Random Nilpotent Groups[0]

3.1 Introduction and background

3.1.1 Random groups

The background idea for the chapter is the models of random groups $\Gamma = F_m/\langle\langle R\rangle\rangle$, where F_m is the free group on some number m of generators, and R is a set of relators of length ℓ chosen by a random process. Typically one takes the number of relators $|R|$ to be a function of ℓ; for fixed ℓ, there are finitely many choices of R of a certain size, and they are all made equally likely. For instance, in the *few-relators model*, $|R|$ is a fixed constant, and in the standard *density model*, $|R| = (2m-1)^{d\ell}$ for a density parameter $0 < d < 1$. (When the number of relators has sub-exponential growth, this is often regarded as sitting in the density model at density zero.)

After fixing $|R|$ as a function of ℓ, we can write $\Pr(\Gamma \text{ has property } P) = p$ to mean that the proportion of such presentations for which the group has P tends to p as $\ell \to \infty$. In particular, we say that random groups have P asymptotically almost surely (a.a.s.) if the probability tends to 1.

The central result in the study of random groups is the theorem of Gromov–Ollivier

[0] **This chapter is a joint work with Matthew Cordes, Moon Duchin, Yen Duong, and Andrew P. Sánchez.**

stating that for $d > 1/2$ in the density model, Γ is a.a.s. isomorphic to either $\{1\}$ or $\mathbb{Z}/2\mathbb{Z}$ (depending on the parity of ℓ), while for $d < 1/2$, Γ is a.a.s. non-elementary hyperbolic and torsion-free [28, Thm 11]. In the rest of this chapter, we will choose our relators from those of length ℓ and $\ell - 1$ with equal probability in order to avoid the parity issue; with this convention, $\Gamma \cong \{1\}$ a.a.s. for $d > 1/2$.

The Gromov–Ollivier theorem tells us that the density threshold for trivializing a free group coincides with the threshold for hyperbolicity, which means that one never sees other kinds of groups, for example abelian groups, in this model. Indeed, because $\mathbb{Z}^2$ cannot appear as a subgroup of a hyperbolic group, one never sees a group with even one pair of commuting elements. To be precise, all finitely-generated groups are quotients of F_m, but the probability of getting a nontrivial non-hyperbolic group (or a group with torsion) is asymptotically zero at every density. Furthermore the recent paper [12] shows that this trivial/hyperbolic dichotomy seems to persist even at $d = 1/2$.

However, it is a simple matter to create new models of random groups by starting with a different "seed" group in place of the free group F_m. The r random strings in $\{a_1, \dots, a_m\}$ that are taken as relators in the Gromov model can be interpreted as elements of any other group with m generators. For instance, forming random quotients of the free abelian group $\mathbb{Z}^m$ in this way would produce a model of random abelian groups; equivalently, the random groups arise as cokernels of random $m \times r$ integer matrices with columns given by the Gromov process, and these clearly recover the abelianizations of Gromov random groups. Random abelian groups are relatively well-studied, and information pertaining to their rank distribution can be found in at least three distinct places: the important paper of Dunfield–Thurston testing the virtual Haken conjecture through random models [13, §3.14]; the recent paper of Kravchenko–Mazur–Petrenko on the generation of algebras by random elements [23]; and the preprint of Wang–Stanley on the Smith normal form distribution of random matrices [41]. These papers use notions of random matrices that differ from the one induced by the Gromov model, but we will explain below that they all produce the same distribution of groups. By contrast, there are many other ways that random abelian groups arise in mathematics: as class groups of imaginary quadratic fields, for instance, or as cokernels of graph Laplacians for random graphs (also known as *sandpile groups*). For a discussion of the heuristics for these various distributions and a useful survey of some of the random abelian group literature, see [42] and its references.

In this chapter we initiate a study of random nilpotent groups by beginning with the *free nilpotent group* $N_{s,m}$ of step s and rank m and adding random relators as above. Note that all nilpotent groups occur as quotients of appropriate $N_{s,m}$, just as all abelian groups are quotients of some $\mathbb{Z}^m$ and all groups are quotients of some F_m (here and throughout, groups are taken to be finitely-generated). By construction, these free nilpotent groups can be thought of as "nilpotentizations" of Gromov random groups; their abelianizations will agree with those described in the last paragraph (cokernels of random matrices), but they have more structure and therefore retain more information about the original random groups.

Below, we begin to study the typical properties of random nilpotent groups. For instance, one would expect that the threshold for trivialization occurs with far fewer relators than for free groups, and also that nontrivial abelian quotients should occur with positive probability at some range of relator growth.

The results of this chapter are summarized as follows:

- In the remainder of this section, we establish a sequence of group theory and linear algebra lemmas for the following parts.

- In Section 3.2, the properties of non-backtracking random walks are described in order to deduce arithmetic statistics of Mal'cev coordinates—this is necessary to use the prior literature on random lattices and matrices.

- We survey the existing results from which ranks of random abelian groups can be calculated; a theorem of Magnus guarantees that the rank of a nilpotent group equals the rank of its abelianization. (Section 3.3)

- We give a complete description of one-relator quotients of the Heisenberg group, and compute the orders of finite quotients with any number of relators. (Section 3.4)

- Using a Freiheitssatz for nilpotent groups, we study the consequences of rank drop, and conclude that abelian groups occur with probability zero for $|R| \leq m - 2$, while they have positive probability for larger numbers of relators. Adding relators in a stochastic process drops the rank by at most one per new relator, with statistics for successive rank drop given by number-theoretic properties of the Mal'cev coordinates. (Section 3.5)

- We give a self-contained proof that a random nilpotent group is a.a.s. trivial exactly if $|R|$ is unbounded as a function of ℓ. We show how information about the nilpotent quotient lifts to information about the LCS of a standard (Gromov) random group and observe that standard random groups are *perfect* under the same conditions. (Section 3.6, Section 3.7)

3.1.2 Nilpotent groups and Mal'cev coordinates

Nilpotent groups are those for which nested commutators become trivial after a certain uniform depth. We will adopt the commutator convention that $[a,b] = aba^{-1}b^{-1}$ and define nested commutators on the left by $[a,b,c] = [[a,b],c]$, $[a,b,c,d] = [[[a,b],c],d]$, and so on. Within a group we will write $[H,K]$ for the subgroup generated by all commutators $[h,k]$ with h ranging over $H \le G$ and k ranging over $K \le G$, so that in particular $[G,G]$ is the usual commutator subgroup of G. A group is *s-step nilpotent* if all commutators with $s+1$ arguments are trivial, but not all those with s arguments are. (The step of nilpotency is also known as the *class* of nilpotency.) With this convention, a group is abelian if and only if it is one-step nilpotent. References for the basic theory of nilpotent groups are [36, Ch 9], [11, Ch 10-12].

In the free group F_m of rank m, let

$$T_{j,m} = \left\{ \left[a_{i_1}, \dots, a_{i_j} \right] \mid 1 \le i_1, \dots, i_j \le m \right\}$$

be the set of all nested commutators with j arguments ranging over the generators. Then the *free s-step rank-m nilpotent group* is

$$N_{s,m} = F_m \big/ \langle\!\langle T_{s+1,m} \rangle\!\rangle = \langle\, a_1, \dots, a_m \mid [a_{i_1}, \dots a_{i_{s+1}}] \text{ for all } i_j \,\rangle,$$

where $\langle\!\langle R \rangle\!\rangle$ denotes the normal closure of a set R when its ambient group is understood. Just as all finitely-generated groups are quotients of (finite-rank) free groups, all finitely-generated nilpotent groups are quotients of free nilpotent groups. Note that the standard Heisenberg group $H(\mathbb{Z}) = \langle\, a, b \mid [a,b,a], [a,b,b] \,\rangle$ is realized as $N_{2,2}$. In the Heisenberg group, we will use the notation $c = [a,b]$, so that the center is $\langle c \rangle$.

The *lower central series* (LCS) for an s-step nilpotent group G is a sequence of subgroups inductively defined by $G_{k+1} = [G_k, G]$ which form a subnormal series

$$\{1\} = G_{s+1} \triangleleft \cdots \triangleleft G_3 \triangleleft G_2 \triangleleft G_1 = G.$$

(The indexing is set up so that $[G_i, G_j] \subseteq G_{i+j}$.) For finitely-generated nilpotent groups, this can always be refined to a *polycylic series*

$$\{1\} = CG_{n+1} \triangleleft CG_n \triangleleft \cdots \triangleleft CG_2 \triangleleft CG_1 = G$$

where each CG_i/CG_{i+1} is cyclic, so either $\mathbb{Z}$ or $\mathbb{Z}/n_i\mathbb{Z}$. The number of $\mathbb{Z}$ quotients in any polycyclic series for G is called the *Hirsch length* of G. From a polycyclic series we can form a generating set which supports a useful normal form for G. Make a choice of u_i in each CG_i so that u_iCG_{i+1} generates CG_i/CG_{i+1}. An inductive argument shows that the set $\{u_1, \dots, u_n\}$ generates G. We call such a choice a *Mal'cev basis* for G, and we filter it as $\mathrm{MB}_1 \sqcup \cdots \sqcup \mathrm{MB}_s$, with MB_j consisting of basis elements belonging to $G_j \smallsetminus G_{j+1}$. Now if $u_i \in \mathrm{MB}_j$, let τ_i be the smallest value such that $u_i^{\tau_i} \in \mathrm{MB}_{j+1}$, putting $\tau_i = \infty$ if no such power exists. Then the Mal'cev normal form in G is as follows: every element $g \in G$ has a unique expression as $g = u_1^{t_1} \cdots u_n^{t_n}$, with integer exponents and $0 \le t_i < \tau_i$ if $\tau_i < \infty$. Then the tuple of exponents $(t_1, \dots, t_n)$ gives a coordinate system on the group, called *Mal'cev coordinates*. We recall that $\mathrm{MB}_j \cup \cdots \cup \mathrm{MB}_s$ generates G_j for each j and that (by definition of s) the elements of MB_s are central.

We will construct a standard Mal'cev basis for free nilpotent groups $N_{s,m}$ as follows: let $\mathrm{MB}_1 = \{a_1, \dots, a_m\}$ be the basic generators, let $\mathrm{MB}_2 = \{b_{ij} := [a_i, a_j] : i < j\}$ be the basic commutators, and take each MB_j as a subset of $T_{j,m}$ consisting of some of the commutators from $[\mathrm{MB}_{j-1}, \mathrm{MB}_1]$. We note that $|\mathrm{MB}_2| = \binom{m}{2}$, and more generally the orders are given by the *necklace polynomials*

$$|\,\mathrm{MB}_j\,| = \frac{1}{j}\sum_{d|j}\mu(d)m^{j/d},$$

where μ is the Möbius function (see [17, Thm 11.2.2]).

For example, the Heisenberg group $H(\mathbb{Z}) = N_{2,2}$ has the lower central series $\{1\} \triangleleft \mathbb{Z} \triangleleft H(\mathbb{Z})$, so its Hirsch length is 3. $H(\mathbb{Z})$ admits the Mal'cev basis a, b, c (with $a = a_1$, $b = a_2$, and c equal to their commutator), which supports a normal form $g = a^A b^B c^C$. The Mal'cev coordinates of a group element are the triple $(A, B, C) \in \mathbb{Z}^3$.

3.1.3 Group theory and linear algebra lemmas

In the free group $F_m = \langle a_1, \ldots, a_m \rangle$, for any freely reduced $g \in F_m$, we define $A_i(g)$, called the *weight* of generator a_i in the word g, to be the exponent sum of a_i in g. Note that weights $A_1, \ldots, A_m$ are well defined in the same way for the free nilpotent group $N_{s,m}$ for any s. We will let ab be the abelianization map of a group, so that $\mathrm{ab}(F_m) \cong \mathrm{ab}(N_{s,m}) \cong \mathbb{Z}^m$. Under this isomorphism, we can identify $\mathrm{ab}(g)$ with the vector $\mathbf{A}(g) := (A_1(g), \ldots, A_m(g)) \in \mathbb{Z}^m$. If we have an automorphism ϕ on $N_{s,m}$, we write ϕ^{ab} for the induced map on $\mathbb{Z}^m$, which by construction satisfies $\mathrm{ab} \circ \phi = \phi^{\mathrm{ab}} \circ \mathrm{ab}$. Note that $\mathbf{A}(g)$ is also the MB_1 part of the Mal'cev coordinates for g, and we can similarly define a b-weight vector $\mathbf{B}(g)$ to be the MB_2 part, recording the exponents of the b_{ij} in the normal form.

To fix terminology: the *rank* of any finitely-generated group will be the minimum size of any generating set. Note this is different from the *dimension* of an abelian group, which we define by $\dim(\mathbb{Z}^d \times G_0) = d$ for any finite group G_0. (With this terminology, the Hirsch length of a nilpotent group G is the sum of the dimensions of its LCS quotients.)

In any finitely-generated group, we say an element is *primitive* if it belongs to some basis (i.e., a generating set of minimum size). For a vector $w = (w_1, \dots, w_m) \in \mathbb{Z}^m$, we will write $\gcd(w)$ to denote the gcd of the entries. So a vector $w \in \mathbb{Z}^m$ is primitive iff $\gcd(w) = 1$. In this case we will say that the tuple $(w_1, \dots, w_m)$ has the *relatively prime property* or is RP. As we will see below, an element $g \in N_{s,m}$ is primitive in that nilpotent group if and only if its abelianization is primitive in $\mathbb{Z}^m$, i.e., if $\mathbf{A}(g)$ is RP. In free groups, there *exists* a primitive element with the same abelianization as g iff $\mathbf{A}(g)$ is RP.

The latter follows from a classic theorem of Nielsen [27].

Theorem 3.1 (Nielsen primitivity theorem). *For every relatively prime pair of integers (i, j), there is a unique conjugacy class $[g]$ in the free group $F_2 = \langle a, b\rangle$ for which $A(g) = i$, $B(g) = j$, and g is primitive.*

Corollary 3.2 (Primitivity criterion in free groups). *There exists a primitive element $g \in F_m$ with $A_i(g) = w_i$ for $i = 1, \dots, m$ if and only if* $\gcd(w_1, \dots, w_m) = 1$.

Proof. Let $w = (w_1, \dots, w_m)$. If $\gcd(w) \neq 1$, then the image of any g with those weights would not be primitive in the abelianization $\mathbb{Z}^m$, so no such g is primitive in F_m.

For the other direction we use induction on m, with the base case $m = 2$ established by Nielsen. Suppose there exists a primitive element of F_{m-1} with given weights $w_1, \dots, w_{m-1}$. For $\delta = \gcd(w_1, \dots, w_{m-1})$, we have $\gcd(\delta, w_m) = 1$. Let $\overline{w} = (\frac{w_1}{\delta}, \dots, \frac{w_{m-1}}{\delta})$. By the inductive hypothesis, there exists an element $\overline{g} \in F_{m-1}$ such that the weights of $\overline{g}$ are $\overline{w}$, and $\overline{g}$ can be extended to a basis $\{\overline{g}, h_2, \dots, h_{m-1}\}$ of F_{m-1}. Consider the free group $\langle \overline{g}, a_m\rangle \cong F_2$. Since $\gcd(\delta, w_m) = 1$, there exist $\hat{g}, \hat{h}$ that generate this free group such that $\hat{g}$ has weights $A_{\overline{g}}(\hat{g}) = \delta$ and $A_m(\hat{g}) = w_m$ by Nielsen. Consequently, $A_i(\hat{g}) = w_i$.

Then $\langle \hat{g}, \hat{h}, h_2, \ldots, h_{m-1} \rangle = \langle \overline{g}, h_2, \ldots, h_{m-1}, a_m \rangle = F_m$, which shows that $\hat{g}$ is primitive, as desired. □

The criterion in free nilpotent groups easily follows from a powerful theorem due to Magnus [25, Lem 5.9].

Theorem 3.3 (Magnus lifting theorem). *If G is nilpotent and $S \subset G$ is any set of elements such that* $\mathrm{ab}(S)$ *generates* $\mathrm{ab}(G)$*, then S generates G.*

Note that this implies that if G is nilpotent of rank m, then $G/\langle\langle g \rangle\rangle$ has rank at least $m-1$, because we can drop at most one dimension in the abelianization.

Corollary 3.4 (Primitivity criterion in free nilpotent groups). *An element $g \in N_{s,m}$ is primitive if and only if $\mathbf{A}(g)$ is primitive in $\mathbb{Z}^m$.*

Now we establish a sequence of lemmas for working with rank and primitivity. Recall that a, b are the basic generators of the Heisenberg group $H(\mathbb{Z})$ and that $c = [a, b]$ is the central letter.

Lemma 3.5 (Heisenberg basis change). *For any integers i, j, there is an automorphism ϕ of $H(\mathbb{Z}) = N_{2,2}$ such that $\phi(a^i b^j c^k) = b^d c^m$, where $d = \gcd(i, j)$ and $m = \frac{ij}{2d}(d-1) + k$.*

In particular, if i, j are relatively prime, then there is an automorphism ϕ of $H(\mathbb{Z})$ such that $\phi(a^i b^j) = b$.

Proof. Suppose $ri + sj = d = \gcd(i, j)$ for integers r, s and consider $\hat{a} = a^s b^{-r}$, $\hat{b} = a^{i/d} b^{j/d}$. We compute

$$[a^s b^{-r}, a^{i/d} b^{j/d}] = [a^s, b^{j/d}] \cdot [b^{-r}, a^{i/d}] = c^{(ri+sj)/d} = c.$$

If we set $\hat{c} = c$, we have $[\hat{a}, \hat{b}] = \hat{c}$ and $[\hat{c}, \hat{a}] = [\hat{c}, \hat{b}] = 1$, so $\langle \hat{a}, \hat{b} \rangle$ presents a quotient of the Heisenberg group. We need to check that it is the full group. Consider $h = (\hat{a})^{-i/d}(\hat{b})^s$.

Writing h in terms of a, b, c, the a-weight of h is 0 and the b-weight is $(ri + sj)/d = 1$, so $h = bc^t$ for some t. But then $b = (\hat{a})^{-i/d}(\hat{b})^s(\hat{c})^{-t}$ and similarly $a = (\hat{a})^{j/d}(\hat{b})^r(\hat{c})^{-t'}$ for some t', so all of a, b, c can be expressed in terms of $\hat{a}, \hat{b}, \hat{c}$.

Finally,

$$(\hat{b})^d = (a^{i/d}b^{j/d})^d = a^i b^j c^{-\binom{d}{2}\frac{ij}{d^2}},$$

which gives the desired expression $a^i b^j c^k = (\hat{b})^d(\hat{c})^m$ from above. □

Proposition 3.6 (General basis change)**.** *Let $\delta = \gcd(A_1(g), \dots, A_m(g))$ for any $g \in H = N_{s,m}$. Then there is an automorphism ϕ of H such that $\phi(g) = a_m^\delta \cdot h$ for some $h \in H_2$.*

Proof. Let $w_i = A_i(g)$ for $i = 1, \dots, m$ and let $r_i = w_i/\delta$, so that $\gcd(r_1, \dots, r_m) = 1$. By Corollary 3.2, there exists a primitive element $x \in F_m$ with weights r_i. Let ϕ be a change of basis automorphism of F_m such that $\phi(x) = a_m$. This induces an automorphism of H, which we will also call ϕ.

By construction, x^δ and g have weight w. Since $\mathrm{ab}(x^\delta) = \mathrm{ab}(g) = w$, we must have $\phi^{\mathrm{ab}}(w) = \mathrm{ab}(\phi(x^\delta)) = \mathrm{ab}(\phi(g))$. Therefore $\phi(x^\delta)$ and $\phi(g)$ have the same weights.

Then $\mathrm{ab}(\phi(g)) = \mathrm{ab}(\phi(x^\delta)) = \mathrm{ab}(\phi(x)^\delta) = \mathrm{ab}(a_m^\delta)$, so $\phi(g)$ and a_m^δ only differ by commutators, i.e., $\phi(g) = a_m^\delta \cdot h$ for some $h \in H_2$. □

Remark 3.7. *Given an abelian group $G = \mathbb{Z}^m/\langle R\rangle$, the classification of finitely-generated abelian groups provides that there are non-negative integers $d_1, \dots, d_m$ with $d_m | d_{m-1} | \dots | d_1$ such that $G \cong \bigoplus_{i=1}^m \mathbb{Z}/d_i\mathbb{Z}$. If G has dimension q and rank r, then $d_1 = \dots = d_q = 0$, and $d_{r+1} = \dots = d_m = 1$, so that*

$$G \cong \mathbb{Z}^q \times (\mathbb{Z}/d_{q+1}\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}).$$

Now consider a projection map $f : \mathbb{Z}^m \to \mathbb{Z}^m/K \cong \bigoplus_{i=1}^m \mathbb{Z}/d_i\mathbb{Z}$. We can choose a basis $e_1, \dots, e_m$ of $\mathbb{Z}^m$ so that

$$K = \operatorname{span}\{d_1e_1, \dots, d_me_m\} \cong \bigoplus_{i=1}^m d_i\mathbb{Z}.$$

Then since every element in K is a linear combination of $\{d_1e_1, \dots, d_me_m\}$ and $d_m|d_{m-1}|\dots|d_1$, we have that d_m divides all the coordinates of all the elements in K. Also $d_me_m \in K$ with e_m being primitive.

Lemma 3.8 (Criterion for existence of primitive vector)**.** *Consider a set of r vectors in $\mathbb{Z}^m$, and let d be the gcd of the rm coordinate entries. Then there exists a vector in the span such that the gcd of its entries is d, and this is minimal among all vectors in the span.*

In particular, a set of r vectors in $\mathbb{Z}^m$ has a primitive vector in its span if and only if the gcd of the rm coordinate entries is 1.

Proof. With d as above, let K be the $\mathbb{Z}$-span of the vectors and let

$$\gamma := \inf_{w \in K} \gcd(w).$$

One direction is clear: every vector in the span has every coordinate divisible by d, so $\gamma \geq d$. On the other hand $d_me_m \in K$ and $\gcd(d_me_m) = d_m$ because e_m is primitive. But d_m is a common divisor of all rm coordinates, and d is the greatest one, so $d_m \leq d$ and thus $\gamma \leq d$. □

Lemma 3.9 (Killing a primitive element)**.** *Let $H = N_{s,m}$ and let K be a normal subgroup of H. If $\operatorname{rank}(H/K) < m$ then K contains a primitive element.*

Proof. Since $\operatorname{rank}(H/K) < m$, we also have $\operatorname{rank}(\operatorname{ab}(H/K)) < m$. Writing $\operatorname{ab}(H/K) \cong \bigoplus_{i=1}^{m} \mathbb{Z}/d_i\mathbb{Z}$ as above, we have $d_m = 1$. By the previous lemma there is a primitive element in the kernel of the projection $\operatorname{ab}(H) \to \operatorname{ab}(H/K)$, and any preimage in K is still primitive (see Cor 3.4). □

Lemma 3.10 (Linear algebra lemma). *Suppose $u_1, \dots, u_n \in \mathbb{Z}^m$ and suppose there exists a primitive vector v in their span. Then there exist $v_2, \dots, v_n$ such that $\operatorname{span}(v, v_2, \dots, v_n) = \operatorname{span}(u_1, \dots, u_n)$.*

Proof. Since $v \in \operatorname{span}(u_1, \dots, u_n)$, we can write $v = \alpha_1 u_1 + \dots + \alpha_n u_n$. Let $x \in \mathbb{Z}^n$ be the vector with coordinates α_i. Because $\gcd(v) = 1$, we have $\gcd(\alpha_i) = 1$, so x is primitive. Thus, we can complete x to a basis of $\mathbb{Z}^n$, say $\{x, x_2, \dots, x_n\}$. Then take $\begin{pmatrix} -v- \\ -v_2- \\ \vdots \\ -v_n- \end{pmatrix} = \begin{pmatrix} -x- \\ -x_2- \\ \vdots \\ -x_n- \end{pmatrix} \cdot \begin{pmatrix} -u_1- \\ -u_2- \\ \vdots \\ -u_n- \end{pmatrix}$. Since $\begin{pmatrix} -x- \\ -x_2- \\ \vdots \\ -x_n- \end{pmatrix} \in SL_n(\mathbb{Z})$, it represents a change of basis matrix, so we have $\operatorname{span}(v, v_2, \dots, v_n) = \operatorname{span}(u_1, \dots, u_n)$, as needed. □

Lemma 3.11 (String arithmetic). *Fix a free group $F = F_m$ on m generators and let R, S be arbitrary subsets, with normal closures $\langle\langle R \rangle\rangle, \langle\langle S \rangle\rangle$. Let $\phi : F \to F/\langle\langle R \rangle\rangle$ and $\psi : F \to F/\langle\langle S \rangle\rangle$ be the quotient homomorphisms. Then there exist canonical isomorphisms*

$$(F/\langle\langle R \rangle\rangle)\big/\langle\langle \phi(S) \rangle\rangle \cong F\big/\langle\langle R \cup S \rangle\rangle \cong (F/\langle\langle S \rangle\rangle)\big/\langle\langle \psi(R) \rangle\rangle$$

that are compatible with the underlying presentation (i.e., the projections from F commute with these isomorphisms).

Proof. We will abuse notation by writing strings from F and interpreting them in the various quotients we are considering. Then if $G = \langle F \mid T \rangle \cong F/\langle\langle T \rangle\rangle$ is a quotient of F

and U is a subset of F, we can write $\langle G \mid U \rangle$ to mean $F \big/ \langle\!\langle T \cup U \rangle\!\rangle$ and can equally well write $\langle F \mid T, U \rangle$. Then the isomorphisms we need just record the fact that

$$\langle\, F \mid R, S \,\rangle = \langle\, F/\langle\!\langle R \rangle\!\rangle \mid S \,\rangle = \langle\, F/\langle\!\langle S \rangle\!\rangle \mid R \,\rangle.$$

□

Because of this standard abuse of notation where we will variously interpret a string in $\{a_1, \dots, a_m\}^{\pm}$ as belonging to F_m, $N_{s,m}$, or some other quotient group, we will use the symbol $=_G$ to denote equality in the group G when trying to emphasize the appropriate ambient group.

3.2 Random walk and arithmetic uniformity

In this section we survey properties of the simple nearest-neighbor random walk (SRW) and the non-backtracking random walk (NBSRW) on the integer lattice $\mathbb{Z}^m$, then deduce consequences for the distribution of Mal'cev coordinates for random relators in free nilpotent groups. For the standard basis $\{e_i\}$ of $\mathbb{Z}^m$, SRW is defined by giving the steps $\pm e_i$ equal probability $1/2m$, and NBSRW is similarly defined but with the added condition that the step $\pm e_i$ cannot be immediately followed by the step $\mp e_i$ (that is, a step cannot undo the immediately preceding step; equivalently, the position after k steps cannot equal the position after $k+2$ steps). Then for a random string w_ℓ of ℓ letters from $\{a_1, \dots, a_m\}^{\pm}$, we have $w_\ell = \alpha_1 \alpha_2 \cdots \alpha_\ell$, where the α_i are i.i.d. random variables which equal each basic generator or its inverse with equal probability $1/2m$. The abelianization $X_\ell = \mathbf{A}(w_\ell)$ is a $\mathbb{Z}^m$-valued random variable corresponding to ℓ-step SRW. A random freely reduced string does not have an expression as a product of variables identically distributed under the same law, but if v_ℓ is such a string, its weight vector $Y_\ell = \mathbf{A}(v_\ell)$ is another $\mathbb{Z}^m$-valued random variable, this time corresponding to NBSRW.

It is well known that the distribution of endpoints for a simple random walk in $\mathbb{Z}^m$ converges to a multivariate Gaussian: if X_ℓ is again the random variable recording the endpoint after ℓ steps of simple random walk on $\mathbb{Z}^m$, and δ_t is the dilation in $\mathbb{R}^m$ sending $v \mapsto tv$, we have the central limit theorem

$$\delta_{\frac{1}{\sqrt{\ell}}} X_\ell \longrightarrow \mathcal{N}(\mathbf{0}, \tfrac{1}{m} I).$$

This convergence notation for a vector-valued random variable V_ℓ and a multivariate normal $\mathcal{N}(\mu, \Sigma)$ means that V_ℓ converges in distribution to $AW + \mu$, where the vector μ is the mean, $\Sigma = AA^T$ is the covariance matrix, and W is a vector-valued random variable with i.i.d. entries drawn from a standard (univariate) Gaussian distribution $\mathcal{N}(0,1)$. In other words, this central limit theorem tells us that the individual entries of X_ℓ are asymptotically independent, Gaussian random variables with mean zero and expected magnitude $\sqrt{\ell}/m$. This is a special case of a much more general result of Wehn for Lie groups and can be found for instance in [5, Thm 1.3]. Fitzner and Van der Hofstad derived a corresponding central limit theorem for NBSRW in [15]. Letting Y_ℓ be the $\mathbb{Z}^m$-valued random variable for ℓ-step NBSRW as before, they find that for $m \geq 2$,

$$\delta_{\frac{1}{\sqrt{\ell}}} Y_\ell \longrightarrow \mathcal{N}(\mathbf{0}, \tfrac{1}{m-1} I).$$

Note that the difference between the two statements records something intuitive: the non-backtracking walk still has mean zero, but the rule causes the expected size of the coordinates to be slightly higher than in the simple case; also, it blows up (as it should) in the case $m = 1$.

The setting of nilpotent groups is also well studied. To state the central limit theorem for free nilpotent groups, we take δ_t to be the similarity which scales each coordinate from MB_j by t^j, so that for instance in the Heisenberg group, $\delta_t(x, y, z) = (tx, ty, t^2 z)$.

Proposition 3.12 (Distribution of Mal'cev coordinates)**.** *Suppose* NB_ℓ *is an* $N_{s,m}$*-valued random variable chosen by non-backtracking simple random walk (NBSRW) on* $\{a_1, \ldots, a_m\}^\pm$ *for* ℓ *steps. Then the distribution on the Mal'cev coordinates is asymptotically normal:*

$$\delta_{\frac{1}{\sqrt{\ell}}} \mathrm{NB}_\ell \sim \mathcal{N}(\mathbf{0}, \Sigma).$$

For SRW, this is called a "simple corollary" of Wehn's theorem in [5, Thm 3.11]), where the only hypotheses are that the steps of the random walk are i.i.d. under a probability measure on $N_{s,m}$ that is centered, with finite second moment (in this case, the measure has finite support, so all moments are finite). Each Mal'cev coordinate is given by a polynomial formula in the a-weights of the step elements α_i (the polynomial for an MB_j coordinate has degree j), where the number of summands gets large as $\ell \to \infty$. Switching to NBSRW, it is still the case that NB_ℓ is a product of group elements whose a-weight vectors are independent and normally distributed, so their images under the same polynomials will be normally distributed as well, with only the covariance differing from the SRW case. We sketch a simple and self-contained argument for this in the $N_{2,2}$ non-backtracking case—that the third Mal'cev coordinate in $H(\mathbb{Z})$ is normally distributed—which we note is easily generalizable to the other $N_{s,m}$ with (only) considerable notational suffering. Without loss of generality, the sample path of the random walk is

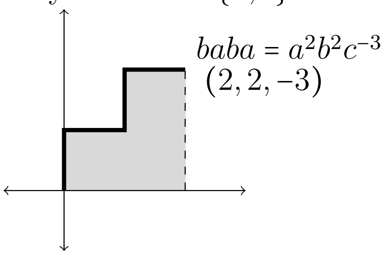
$$g = a^{i_1} b^{j_1} a^{i_2} b^{j_2} \ldots a^{i_r} b^{j_r}$$

for some integers i_s, j_t summing to ℓ or $\ell - 1$, with all but possibly i_1 and j_r nonzero. After a certain number of steps, suppose the last letter so far was a. Then the next letter is either a, b, or b^{-1} with equal probability, so there is a 1/3 chance of repeating the same letter and a 2/3 chance of switching. This means that the i_s and j_t are (asymptotically independent) run-lengths of heads for a biased coin (Bernoulli trial) which lands heads with probability 1/3. On the other hand, r is half the number of tails flipped by that coin in ℓ (or $\ell - 1$) trials. In Mal'cev normal form,

$$g = a^{\sum i_s} b^{\sum j_t} c^{\sum_{t<s} i_s j_t}.$$

Thus the exponent of c is obtained by adding products of run-lengths together $\binom{r}{2}$ times, and general central limit theorems ensure that adding many independent and identically distributed (i.i.d.) random variables together tends to a normal distribution.

Our distribution statement has a particularly nice formulation in this Heisenberg case, where the third Mal'cev coordinate records the *signed area* enclosed between the x-axis and the path traced out by a word in $\{a, b\}^{\pm}$.



Corollary 3.13 (Area interpretation for Heisenberg case)**.** *For the simple random walk on the plane, the signed area enclosed by the path is a normally distributed random variable.*

Next, we want to describe the effect of a group automorphism on the distribution of coordinates. Then we conclude this section by considering the distribution of coordinates in various $\mathbb{Z}/p\mathbb{Z}$.

Corollary 3.14 (Distributions induced by automorphisms). *If ϕ is an automorphism of $N_{s,m}$ and g is a random freely reduced word of length ℓ in $\{a_1, \dots, a_m\}^{\pm}$, then the Mal'cev coordinates of* $\mathrm{ab}(\phi(g))$ *are also normally distributed.*

Proof. The automorphism ϕ induces a change of basis on the copy of $\mathbb{Z}^m$ in the MB_1 coordinates, which is given by left-multiplication by a matrix $B \in SL_m(\mathbb{Z})$. Then $\phi_*(Y_\ell) \to \mathcal{N}(\mathbf{0}, B\Sigma B^T)$. □

Note that normality of the MB_j coordinates follows as well, as before: they are still described by sums of statistics coming from asymptotically independent Bernoulli trials, and only the coin bias has changed.

Relative primality of MB_1 coefficients turns out to be the key to studying the rank of quotient groups, so we will need some arithmetic lemmas.

Lemma 3.15 (Arithmetic uniformity). *Let $A_{i,\ell}$ be the $\mathbb{Z}$-valued random variable given by the a_i-weight of a random freely reduced word of length ℓ in $\{a_1, \dots, a_m\}^{\pm}$, for $1 \le i \le m$. Let $\hat{A}_{i,\ell}$ equal $A_{i,\ell}$ with probability $\frac{1}{2}$ and $A_{i,\ell-1}$ with probability $\frac{1}{2}$. Then for fixed $m \ge 2$, fixed i, and $\ell \to \infty$,*

$$\forall k, n, \qquad \Pr\Big(\hat{A}_{i,\ell} \equiv k \mod n\Big) = \frac{1}{n} + o(1).$$

Furthermore, the distributions are independent in different coordinates:

$$\Pr\Big(\hat{A}_{i_1,\ell} \equiv k_1, \cdots \hat{A}_{i_s,\ell} \equiv k_s \mod n\Big) = \frac{1}{n^s} + o(1) \quad \textit{for } i_j \textit{ distinct}, s \le m.$$

In other words, the $\mathbb{Z}/n\mathbb{Z}$-valued random variables induced by the coordinate projections from NBSRW on MB_1 approach independent uniform distributions.

Proof. First, consider SRW on $\mathbb{Z}^m$, which induces a lazy random walk (i.e., stays still with some probability, and moves forward or back with equal probabilities) on each coordinate. For odd n, the random walk is a Markov process on the finite graph given by the torus $(\mathbb{Z}/n\mathbb{Z})^m$, so $A_{i,\ell}$ approaches a uniform distribution (see [10, Ch 3C]), and the result follows for $\hat{A}_{i,\ell}$. In fact, in that case the error term decays exponentially fast in ℓ

$$\forall k, \forall n \leq \sqrt{\ell}, \qquad \left| \Pr\Big(A_{i,\ell} \equiv k \pmod{n} \Big) - \frac{1}{n} \right| \leq e^{-\pi^2 \ell / n^2}.$$

For $n = 2$ (and likewise for other even n) the construction of $\hat{A}$ corrects the parity bias, since $\hat{A}_{i,\ell}$ is now equally likely to have same parity as ℓ or the opposite parity. To make NBSRW into a Markov process, we must create a new state space where the states correspond to directed edges on the discrete torus, which encodes the one step of memory required to avoid backtracking. This new state space can itself be rendered as a homogeneous finite graph, and the result follows. Since the ith coordinate of the torus position corresponds to the $\hat{A}_{i,\ell}$ value, uniformity over the torus implies the independence and uniformity we need. □

Corollary 3.16 (Uniformity mod p)**.** *The abelianization of a random freely reduced word in F_m has entries that are asymptotically uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$ for each prime p, and the distribution mod p is independent of the distribution mod q for any distinct primes p, q.*

Proof. For independence, consider $n = pq$ in the previous lemma. □

Corollary 3.17 (Probability of primitivity)**.** *For a random freely reduced word in F_m, the probability that it is primitive in abelianization tends to $1/\zeta(m)$, where ζ is the Riemann zeta function. In particular, for $m = 2$, the probability is $6/\pi^2$.*

A heuristic argument for this corollary can be given by arithmetic uniformity. For a detailed proof, please see Lemma 3.42 in Section 3.7.

Remark 3.18 (Comparison of random models)**.** *As we have seen, abelianizations of Gromov random groups are computed as cokernels of random matrices M whose columns are given by non-backtracking simple random walk on $\mathbb{Z}^m$.*

Other models in the random abelian groups literature have somewhat different setup. Dunfield and Thurston [13] use a lazy random walk: ℓ letters are chosen uniformly from the $(2m+1)$ possibilities of $a_i^{\pm}$ and the identity letter, creating a word of length $\leq \ell$, whose abelianization becomes a column of M. Kravchenko–Mazur–Petrenko [23] and Wang–Stanley [41] use the standard "box" model: integer entries are drawn uniformly at random from $[-\ell, \ell]$, and asymptotics are calculated as $\ell \to \infty$. (This is the most classical way to randomize integers in number theory; see [18].)

However, all of the arguments in all of these settings rely on arithmetic uniformity of coordinates mod p to calculate probabilities of relative primality, which is why the Riemann zeta function comes up repeatedly in the calculations. Since we have also established arithmetic uniformity for our setting in Corollary 3.16, the results achieved in these other models will carry over to our groups directly.

3.3 Preliminary facts about random nilpotent groups via abelianization

In this section we make a few observations relevant to the model of random nilpotent groups we study below. In particular, there has been substantial work on quotients of free abelian groups $\mathbb{Z}^m$ by random lattices, so it is important to understand the relationship between a random nilpotent group and its abelianization. Below, and throughout the chapter, recall that probabilities are asymptotic as $\ell \to \infty$.

First, we record the simple observation that depth in the LCS is respected by homomorphisms.

Lemma 3.19. *Let $\phi : G \to H$ be a surjective group homomorphism. Then $\phi(G_k) = H_k$ where G_k, H_k are the level-k subgroups in the respective lower central series.*

Proof. Since ϕ is a homomorphism, depth-k commutators are mapped to depth-k commutators, i.e., $\phi(G_k) \subseteq H_k$. Let $h \in H_k$. Without loss of generality we can assume h is a single nested commutator $h = [w_1, \ldots, w_k]$. By surjectivity of ϕ we can choose lifts $\overline{w_1}, \ldots, \overline{w_k}$ of $w_1, \ldots, w_k$. We see $[\overline{w_1}, \ldots, \overline{w_k}] \in G_k$ and $\phi(G_k) \supseteq H_k$. □

To begin the consideration of ranks of random nilpotent groups, note that the Magnus lifting theorem (Theorem 3.3) tells us the rank of $N_{s,m}/\langle\langle R\rangle\rangle$ equals the rank of its abelianization $\mathbb{Z}^m/\langle R\rangle$, so we quickly deduce the probability of rank drop.

Proposition 3.20 (Rank drop)**.** *Let $G = N_{s,m}/\langle\langle g_1, \ldots, g_r\rangle\rangle$ be a random r-relator nilpotent group, then*

$$\Pr(\mathrm{rank}(G) < m) = \frac{1}{\zeta(rm)}.$$

Proof. This follows directly from considering the existence of a primitive element in $\langle \mathrm{ab}(R)\rangle$. By Lemma 3.8, this occurs if and only if the rm entries are relatively prime, and by arithmetic uniformity (Lemma 3.15), this is computed by the Riemann zeta function, as in Corollary 3.17. □

Next we observe that a nilpotent group is trivial if and only if its abelianization (i.e., the corresponding $\mathbb{Z}^m$ quotient) is trivial, and more generally it is finite if and only if the abelianization is finite. Equivalence of triviality follows directly from the Magnus lifting theorem (Theorem 3.3). For the other claim, suppose the abelianization is finite. Then powers of all the images of a_i are trivial in the abelianization, so in the nilpotent group G there are finite powers $a_i^{r_i}$ in the commutator subgroup G_2. A simple inductive argument shows that every element of G_j has a finite power in G_{j+1}; for example, consider $b_{ij} \in G_2$. Since $[a_i^{r_i}, a_j] = b_{ij}^{r_i}$ is a commutator of elements from G_2 and G_1, it must be in G_3, as claimed. But then we can see that there are only finitely many distinct elements in the group by considering the Mal'cev normal form

$$g = u_1^* u_2^* \cdots u_r^*$$

and noting that each exponent can take only finitely many values. Since the rank of a nilpotent group equals that of its abelianization (by Theorem 3.3 again), it is also true that a nilpotent group is cyclic if and only if its abelianization is cyclic.

We introduce the term *balanced* for groups presented with the number of relators equal to the number of generators, so that it applies to models of random groups $F_m/\langle\langle R\rangle\rangle$, random nilpotent groups $N_{s,m}/\langle\langle R\rangle\rangle$, or random abelian groups $\mathbb{Z}^m/\langle R\rangle$, where $|R| = m$, the rank of the seed group. We will correspondingly use the terms *nearly-balanced* for $|R| = m - 1$, and *underbalanced* or *overbalanced* in the cases $|R| < m - 1$ and $|R| > m$, respectively.

Then it is very easy to see that nearly-balanced (and thus underbalanced) groups are a.a.s. infinite, while balanced (and thus overbalanced) groups are a.a.s. finite because m random integer vectors are $\mathbb{R}$-linearly independent with probability one. However, it is also easy to see that if $|R|$ is held constant, no matter how large, then there is a nonzero probability that the group is nontrivial (because, for example, all the a-weights could be even).

To set up the statement of the next lemma, let $Z(m) := \zeta(2)\cdots\zeta(m)$ and

$$P(m) := \prod_{\text{primes } p} \left(1 + \frac{1/p - 1/p^m}{p-1}\right).$$

Recall from Remark 3.18 that we can quote the distribution results of [13],[23],[41] because of the common feature of arithmetic uniformity.

Lemma 3.21 (Cyclic quotients of abelian groups)**.** *The probability that the quotient of* $\mathbb{Z}^m$ *by* $m-1$ *random vectors is cyclic is* $1/Z(m)$*. With* m *random vectors, the probability is* $P(m)/Z(m)$*.*

These facts, particularly the first, can readily be derived "by hand," but can also be computed using Dunfield–Thurston [13] as follows: their generating functions give expressions for the probability that i random vectors with $\mathbb{Z}/p\mathbb{Z}$ entries generate a subgroup of rank j, and the product over primes of the probability that the $\mathbb{Z}/p\mathbb{Z}$ reduction has rank $\geq m-1$ produces the probability of a cyclic quotient over $\mathbb{Z}$.

The latter fact appears directly in Wang–Stanley [41] as Theorem 4.9(i). We note that corresponding facts for higher-rank quotients could also be derived from either of these two papers, but the expressions have successively less succinct forms.

Corollary 3.22 (Explicit probabilities for cyclic quotients)**.** *For balanced and nearly-balanced presentations, the probability that a random abelian group or a random nilpotent group is cyclic is a strictly decreasing function of* m *which converges as* $m \to \infty$*.*

In the balanced case, the limiting value is a well-known number-theoretic invariant. Values are estimated in the table below.

The convergence for both cases is proved in [41, Thm 4.9] as a corollary of the more general statement about the Smith normal form of a random not-necessarily-square matrix M, which is an expression $A = SMT$ for invertible S, T in which A has all zero entries except possibly its diagonal entries $a_{ii} = \alpha_i$. These α_i are then the abelian invariants for the quotient of $\mathbb{Z}^m$ by the column span of M (that is, they are the d_i from Remark 3.7 but with opposite indexing, $d_i = \alpha_{m+1-i}$). The rank of the quotient is the number of these that are not equal to 1.

The probabilities of cyclic groups among balanced and nearly-balanced quotients of free abelian groups and therefore also for random nilpotent groups are approximated below. Values in the table are truncated (not rounded) at four digits.

Pr(cyclic)	$m = 2$	$m = 3$	$m = 4$	$m = 10$	$m = 100$	$m = 1000$	$m \to \infty$
$\lvert R\rvert = m - 1$	.6079	.5057	.4672	.4361	.4357	.4357	.4357
$\lvert R\rvert = m$	.9239	.8842	.8651	.8469	.8469	.8469	.8469

Computing the probability of a trivial quotient with r relators is equivalent to the the probability that r random vectors generate $\mathbb{Z}^m$.

Lemma 3.23 (Explicit probability of trivial quotients)**.** *For $r > m$,*

$$\Pr\left(\mathbb{Z}^m / \langle v_1, \ldots, v_r\rangle = 0\right) = \frac{1}{\zeta(r-m+1)\cdots\zeta(r)}.$$

This is a rephrasing of [23, Cor 3.6] and [41, Thm 4.8].

Remark 3.24. *From the description of the Smith normal form, we get a symmetry in r and m, namely for all $1 \le k \le \min(r, m)$,*

$$\Pr\left(\operatorname{rank}\left(\mathbb{Z}^m / \langle v_1, \ldots, v_r\rangle\right) = m - k\right) = \Pr\left(\operatorname{rank}\left(\mathbb{Z}^r / \langle v_1, \ldots, v_m\rangle\right) = r - k\right)$$

just by the observation that the transpose of the normal form expression has the same invariants. For example, applying duality to Lemma 3.21 and reindexing, we immediately obtain, as in Lemma 3.23,

$$\Pr\left(\mathbb{Z}^m \big/ \langle v_1, \ldots, v_{m+1}\rangle = 0\right) = \frac{1}{Z(m+1)} = \frac{1}{\zeta(2)\cdots\zeta(m+1)}.$$

3.4 Quotients of the Heisenberg group

We will classify all $G := H(\mathbb{Z})/\langle\!\langle g \rangle\!\rangle$ for single relators g, up to isomorphism. As above, we write a, b for the generators of $H(\mathbb{Z})$, and $c = [a, b]$. With this notation, $H(\mathbb{Z})$ can be written as a semidirect product $\mathbb{Z}^2 \rtimes \mathbb{Z}$ via $\langle b, c\rangle \rtimes \langle a\rangle$ with the action of $\mathbb{Z}$ on $\mathbb{Z}^2$ given by $ba = abc^{-1}$, $ca = ac$.

Theorem 3.25 (Classification of one-relator Heisenberg quotients)**.** *Suppose $g = a^i b^j c^k \neq 1$. Let $d = \gcd(i, j)$, let $m = \frac{ij}{2d}(d-1) + k$ as in Lemma 3.5, and let $D = \gcd(d, m)$. Then*

$$G := H(\mathbb{Z}) \big/ \langle\!\langle g \rangle\!\rangle \cong \begin{cases} (\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}) \rtimes \mathbb{Z}, & \text{if } i = j = 0; \\ (\mathbb{Z}/\frac{d^2}{D}\mathbb{Z} \ \times \ \mathbb{Z}/D\mathbb{Z}) \rtimes \mathbb{Z}, & \text{else,} \end{cases}$$

with the convention that $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ and $\mathbb{Z}/1\mathbb{Z} = \{1\}$. In particular, G is abelian if and only if $g = c^{\pm 1}$ or $\gcd(i, j) = 1$; otherwise, it has step two. Furthermore, unless g is a power of c (the $i = j = 0$ case), the quotient group is virtually cyclic.

Note that this theorem is exact, not probabilistic.

Remark 3.26 (Baumslag–Solitar case)**.** *The* Baumslag–Solitar groups *are a famous class of groups given by the presentations $BS(p, q) = \langle a, b \mid ab^p a^{-1} = b^q\rangle$ for various p, q.*

For the Heisenberg quotients as described above, we will refer to $D = 1$ as the Baumslag–Solitar case, because in that case $sd - tm = 1$ has solutions in s, t, and one easily checks that the group is presented as

$$G = \langle a, b \mid [a,b] = b^{td}, \quad b^{d^2} = 1 \rangle \cong BS(1, 1+td) \big/ \langle\!\langle b^{d^2} \rangle\!\rangle,$$

a 1-relator quotient of a solvable Baumslag–Solitar group $BS(1,q)$.

Examples:

1. if $g = a$, then $G = \mathbb{Z}$.
2. if $g = c$, then $G = \mathbb{Z}^2$.
3. if $g = c^2$, then $G = (\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}$.
4. if $g = a^{20}b^{28}c^{16}$, we have $d = 4$, $m = 226$, and $D = 2$, so we get
$$G = \left(\mathbb{Z}^2 \big/ \langle \left(\begin{smallmatrix} 4 \\ 226 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 4 \end{smallmatrix}\right) \rangle \right) \rtimes \mathbb{Z} \cong \left(\mathbb{Z}^2 \big/ \langle \left(\begin{smallmatrix} 4 \\ 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 4 \end{smallmatrix}\right) \rangle \right) \rtimes \mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}.$$
5. if $g = a^2b^2c^2$, we have $d = 2$, $m = 3$, and $D = 1$. In this case, $b^4 =_G c^2 =_G 1$ and the quotient group is isomorphic to $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}$ with the action given by $aba^{-1} = b^3$. This is a two-step-nilpotent quotient of the Baumslag–Solitar group $BS(1,3)$ by introducing the relation $b^4 = 1$.

We see that the quotient group G collapses down to $\mathbb{Z}$ precisely if $\gcd(i,j) = 1$. Namely, $c =_G 1$ in that case, so we have a quotient of $\mathbb{Z}^2$ by a primitive vector.

Corollary 3.27. *For one-relator quotients of the Heisenberg group, $G = N_{2,2}/\langle\!\langle g \rangle\!\rangle$,*

$$\Pr(G \cong \mathbb{Z}) = \frac{6}{\pi^2} \approx 60.8\% \; ; \qquad \Pr(G \text{ step 2, rank 2}) = 1 - \frac{6}{\pi^2}.$$

Of course, if $g = c$, we have $\mathbb{Z}^2$, but this event occurs with probability zero. If $\gcd(i,j) \neq 1$, then G is two-step (thus non-abelian) and has torsion.

Proof of theorem. First, the $(i,j) = (0,0)$ case is very straightforward: then $g = c^k$ and the desired expression for G follows.

Below, we assume $(i,j) \neq (0,0)$, and by Lemma 3.5, without loss of generality, we will write $g = b^d c^m$.

Consider the normal closure of b, which is $\langle\!\langle b \rangle\!\rangle = \langle b, c\rangle$. This intersects trivially with $\langle a \rangle$, and $G = \langle\!\langle b \rangle\!\rangle \langle a \rangle$. Thus $G = \langle b, c\rangle \rtimes \langle a \rangle$.
Now in $H(\mathbb{Z})$, we compute $\langle\!\langle g \rangle\!\rangle = \langle b^d c^m, c^d \rangle \subset \langle b, c \rangle$. Thus

$$\langle b, c\rangle \cong \mathbb{Z}^2 \big/ \langle \left(\begin{smallmatrix} d \\ m \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) \rangle.$$

We have the semidirect product structure $G \cong \mathbb{Z}^2 \big/ \langle \left(\begin{smallmatrix} d \\ m \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) \rangle \rtimes \mathbb{Z}$, where the action sends $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ and fixes $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. Note that c has order d in G, and a simple calculation verifies that b has order d^2/D, where $D = \gcd(d,m)$. If we are willing to lose track of the action and just write the group up to isomorphism, then we can perform both row and column operations on $\left[\begin{smallmatrix} d & 0 \\ m & d \end{smallmatrix}\right]$ to get $\left[\begin{smallmatrix} d^2/D & 0 \\ 0 & D \end{smallmatrix}\right]$, which produces the desired expression. □

In fact, we can say something about quotients of $H(\mathbb{Z})$ with arbitrary numbers of relators. First let us define the *K-factor* $K(R)$ of a relator set $R = \{g_1, \ldots, g_r\}$, where relator g_1 has the Mal'cev coordinates (i_1, j_1, k_1), and similarly for $g_2, \ldots, g_r$. Let $M = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \\ j_1 & j_2 & \ldots & j_r \end{pmatrix}$ and suppose its nullity (the dimension of its kernel) is q. Then let W be a kernel matrix of M, i.e., an $r \times q$ matrix with rank q such that $MW = \mathbf{0}$. (Note that if R is a random relator set, then $q = r - 2$, since the rank of M is 2 with probability one.) Let $k = (k_1, \ldots, k_r)$ be the vector of c-coordinates of relators, so that $kW \in \mathbb{Z}^q$. Then $K(R) := \gcd(kW)$ is defined to be the gcd of those q integers.

Theorem 3.28 (Orders of Heisenberg quotients)**.** *Consider the group $G = H(\mathbb{Z})/\langle\!\langle g_1, \ldots, g_r \rangle\!\rangle$, where relator g_1 has the Mal'cev coordinates (i_1, j_1, k_1), and similarly for $g_2, \ldots, g_r$. Let $d = \gcd(i_1, j_1, \ldots, i_r, j_r)$; let Δ be the co-area of the lattice spanned by the $\binom{i_\alpha}{j_\alpha}$ in $\mathbb{Z}^2$; and let $K = K(R)$ be the K-factor defined above. Then c has order $\gamma = \gcd(d, K)$ in G and $|G| = \Delta \cdot \gamma$.*

Proof. Clearly Δ is the order of $\mathrm{ab}(G) = G/\langle c \rangle$. So to compute the order of G, we just need to show that the order of c in G is γ. Consider for which n we can have $c^n \in \langle\!\langle g_1, \ldots, g_r \rangle\!\rangle$, i.e.,

$$c^n = \prod_{\alpha=1}^{N} w_\alpha \; g_\alpha^{\epsilon_\alpha} \; w_\alpha^{-1}$$

for arbitrary words w_α and integers ϵ_α. First note that all commutators $[w, g_\alpha]$ are of this form, and that by letting $w = a$ or b, these commutators can equal c^{i_α} or c^{j_α} for any α, so n can be an arbitrary multiple of d.

Next, consider the expression in full generality and note that $\mathbf{A}(c^n) = \binom{0}{0}$. Conjugation preserves weights, so $\mathbf{A}(w_\alpha g_\alpha^{\epsilon_\alpha} w_\alpha^{-1}) = \mathbf{A}(g_\alpha^{\epsilon_\alpha}) = \epsilon_\alpha \mathbf{A}(g_\alpha) = \epsilon_\alpha \binom{i_\alpha}{j_\alpha}$. To get the two sides to be equal in abelianization, the ϵ_α must record a linear dependency in the $\binom{i_\alpha}{j_\alpha}$. Finally we compute

$$n = \sum_\alpha \epsilon_\alpha (x_\alpha j_\alpha - y_\alpha i_\alpha) + \sum_{\alpha<\beta} \epsilon_\alpha \epsilon_\beta i_\beta j_\alpha - \sum_\alpha i_\alpha j_\alpha \frac{\epsilon_\alpha(\epsilon_\alpha - 1)}{2} + \sum_\alpha \epsilon_\alpha k_\alpha,$$

where $\binom{x_\alpha}{y_\alpha} = \mathbf{A}(w_\alpha)$. We can observe that each of the first three terms is a multiple of d and the fourth term is an arbitrary integer multiple of K. (To see this, note that the column span of W is exactly the space of linear dependencies in the $\mathbf{A}(g_\alpha)$, so $\sum \epsilon_\alpha k_\alpha$

is a scalar product of the k vector with something in that column span, and is therefore a multiple of K.) Thus n can be any integer combination of d and K, as we needed to prove. □

3.5 Rank drop

First, we establish that adding a single relator to a (sufficiently complicated) free nilpotent group does not drop the nilpotency class; the rank drops by one if the relator is primitive in abelianization and it stays the same otherwise. Furthermore, a single relator never drops the step unless the starting rank was two. This is a nilpotent version of Magnus's famous *Freiheitssatz* (freeness theorem) for free groups [25, Thm 4.10].

Theorem 3.29 (Nilpotent *Freiheitssatz*)**.** *For any $g \in N_{s,m}$ with $s \geq 2, m \geq 3$, there is an injective homomorphism*

$$N_{s,m-1} \hookrightarrow N_{s,m}/\langle\!\langle g \rangle\!\rangle.$$

This is an isomorphism if and only if $\gcd(A_1(g), \ldots, A_m(g)) = 1$.

If $m = 2$ the result holds with $\mathbb{Z} \hookrightarrow N_{s,2}/\langle\!\langle g \rangle\!\rangle$.

Proof. Romanovskii's 1971 theorem [31, Thm 1] does most of this. In our language, the theorem says that if $A_m(g) \neq 0$, then $\langle a_1, \ldots, a_{m-1} \rangle$ is a copy of $N_{s,m-1}$. This establishes the needed injection except in the case $g \in [N_{s,m}, N_{s,m}]$, where $\mathbf{A}(g)$ is the zero vector. In the $m = 2$ case, any such $N_{s,2}/\langle\!\langle g \rangle\!\rangle$ has abelianization $\mathbb{Z}^2$, so the statement holds. For $m > 2$, one can apply an automorphism so that g is spelled with only commutators involving a_m. Even killing all such commutators does not drop the nilpotency class because $m > 2$ ensures that there are some Mal'cev generators spelled without a_m in each level. Thus in this case $\langle a_1, \ldots, a_{m-1} \rangle \cong N_{s,m-1}$ still embeds.

It is easy to see that if g is non-primitive in abelianization, then the rank of $\mathrm{ab}(N_{s,m}/\langle\langle g\rangle\rangle)$ is m, and so the quotient nilpotent group has rank m as well. However, the image of Romanovskii's map has rank $m-1$, so it is not a surjection.

On the other hand, suppose $\mathrm{ab}(g)$ is a primitive vector. Then the rank of the abelianized quotient is $m-1$, and by Magnus's theorem (Theorem 3.3) the rank of the nilpotent quotient is the same. The group $G = N_{s,m}/\langle\langle g\rangle\rangle$ is therefore realizable as a quotient of that copy of $N_{s,m-1}$. Since the lower central series of $N_{s,m-1}$ has all free abelian quotients, any proper quotient would have smaller Hirsch length, and this contradicts Romanovskii's injection. Thus relative primality implies that the injection is an isomorphism. □

Now we can use rank drop to analyze the probability of an abelian quotient for a free nilpotent group in the underbalanced, nearly balanced, and balanced cases (i.e., cases with the number of relators at most the rank).

Lemma 3.30 (Abelian implies rank drop for up to m relators)**.** *Let $G = N_{s,m}/\langle\langle R\rangle\rangle$, where $R = \{g_1,\dots,g_r\}$ is a set of $r \le m$ random relators. Suppose $s \ge 2$ and $m \ge 2$. Then*

$$\Pr(G \text{ abelian} \mid \operatorname{rank}(G) = m) = 0.$$

Proof. Suppose that $\operatorname{rank}(G) = m$ and G is abelian. We use the form of the classification of abelian groups (Remark 3.7) in which $G \cong \oplus_{i=1}^{m}\mathbb{Z}/d_i\mathbb{Z}$, where $d_m \mid \dots \mid d_1$ so that $d_1 = \dots = d_q = 0$ for $q = \dim(G)$, and we write $\langle\langle \mathrm{ab}(R)\rangle\rangle = \langle d_1e_1,\dots,d_me_m\rangle$ for a basis $\{e_i\}$ of $\mathbb{Z}^m$. Since $\operatorname{rank}(G) = m$, we can assume no $d_i = 1$. We can lift the basis $\{e_i\}$ of $\mathbb{Z}^m$ to a generating set $\{a_i\}$ of $N_{s,m}$ by Magnus (Theorem 3.3). Note that the exponent of each generator in each relator is a multiple of d_m.

Next we show that we cannot kill a commutator in G without dropping rank. Let $b_1 = [a_1, a_m]$. We claim that $b_1 \notin \langle\langle g_1, \dots, g_r \rangle\rangle$. To do so, we compute an arbitrary element

$$\prod_{\alpha}^{n} w_\alpha g_\alpha^{\epsilon_\alpha} w_\alpha^{-1} \in \langle\langle g_1, \dots, g_r \rangle\rangle.$$

Conjugation preserves weights, so $\mathbf{A}(w_\alpha g_{i_\alpha}^{\epsilon_\alpha} w_\alpha^{-1}) = \mathbf{A}(g_{i_\alpha}^{\epsilon_\alpha}) = \epsilon_\alpha \mathbf{A}(g_{i_\alpha})$. If the product is equal to b_1, then its a-weights are all zero. Now consider the b-weights. For the product, the b-weights are the combination of the b-weights of the g_α, modified by amounts created by commutation. However, since all the a-exponents of all the g_α are multiples of d_m, we get

$$\sum \epsilon_i \mathbf{A}(g_i) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \sum \epsilon_i \mathbf{B}(g_i) \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{d_m},$$

where each ϵ_i is the sum of the ϵ_α corresponding to g_i. The second expression ensures that the ϵ_i are not all zero, so the first equality is a linear dependence in the $\mathbf{A}(g_i)$, which has probability zero since $r \le m$. □

Theorem 3.31. *(Underbalanced quotients are not abelian) Let $G = N_{s,m}/\langle\langle R \rangle\rangle$, where $R = \{g_1, \dots, g_r\}$ is a set of $r \le m - 2$ random relators g_i. Then*

$$\Pr(G \text{ abelian}) = 0.$$

Proof. Suppose that G is abelian, and consider elements of G as vectors in $\mathbb{Z}^m$ via the abelianization map on $N_{s,m}$; in this way we get vectors $v_1 = \mathbf{A}(g_1), \dots, v_r = \mathbf{A}(g_r)$. From the previous result we may assume $\operatorname{rank}(G) < m$. By Lemma 3.8, we can find a primitive vector w as a linear combination of the v_i. Then we apply the linear algebra lemma (Lemma 3.10) to extend w appropriately so that $\operatorname{span}(v_1, \dots, v_r) = \operatorname{span}(w, w_2, \dots, w_r)$. We can find a series of elementary row operations (switching, multiplication by -1, or addition) to get $(w, w_2, \dots, w_r)$ from $(v_1, \dots, v_r)$, and we lift these operations to elementary Nielsen transformations (switching, inverse, or multiplication, respectively) in $N_{s,m}$ to get $(g', g_2', \dots, g_r')$ from $(g_1, \dots, g_r)$. Note that Nielsen transformations on a set of group elements preserve the subgroup they generate, so also preserve normal closure. This lets us define $R' = \{g', g_2', \dots, g_r'\}$ with $\langle\!\langle R' \rangle\!\rangle = \langle\!\langle R \rangle\!\rangle$. Since g' has a weight vector w whose coordinates are relatively prime, the Freiheitssatz (Theorem 3.29) ensures that $N_{s,m}/\langle\!\langle g' \rangle\!\rangle \cong N_{s,m-1}$. Thus we have $G = N_{s,m-1}/\langle\!\langle g_2', \dots, g_r' \rangle\!\rangle$.

If $r \leq m - 2$, then iterating this argument $r - 1$ times gives $G \cong N_{s,m-r+1}/\langle\!\langle g_r \rangle\!\rangle$ for some new g_r, and $m - r + 1 \geq 3$. Then we can apply Theorem 3.29 to conclude that this quotient is not abelian, because its nilpotency class is $s > 1$. □

Proposition 3.32 (Cyclic quotients)**.** *If $|R| = m - 1$ or $|R| = m$, then abelian implies cyclic:*

$$\Pr(G \text{ cyclic} \mid G \text{ abelian}) = 1.$$

Proof. Running the proof as above, we iterate the reduction $m - 2$ times to obtain $G \cong N_{s,2}/\langle\!\langle g \rangle\!\rangle$ or $N_{s,2}/\langle\!\langle g, g' \rangle\!\rangle$.

If g (or any element of $\langle\!\langle g, g' \rangle\!\rangle$) is primitive, then G is isomorphic to $\mathbb{Z}$ or a quotient of $\mathbb{Z}$, i.e., G is cyclic.

Otherwise, note that $N := N_{s,2}$ has the Heisenberg group as a quotient ($H(\mathbb{Z}) = N_1/N_3$). If G is abelian, then the corresponding quotient of $H(\mathbb{Z})$ is abelian. In the non-primitive case, this can only occur if $c \in \langle\!\langle g, g' \rangle\!\rangle$, which (as in the proof of Lemma 3.30) implies $\mathbf{A}(g) = (0, 0)$ (or a linear dependency between $\mathbf{A}(g)$ and $\mathbf{A}(g')$). But by Corollary 3.14, the changes of basis do not affect the probability of linear dependency, so this has probability zero. □

Corollary 3.33. *For nearly-balanced and balanced models, the probability that a random* *nilpotent group is abelian equals the probability that it is cyclic.*

We reprise the table from Section 3.3, recalling that values are truncated at four digits.

Pr(abelian)	$m = 2$	$m = 3$	$m = 4$	$m = 10$	$m = 100$	$m = 1000$	$m \to \infty$
$\lvert R\rvert = m - 1$	.6079	.5057	.4672	.4361	.4357	.4357	.4357
$\lvert R\rvert = m$	.9239	.8842	.8651	.8469	.8469	.8469	.8469

Corollary 3.34 (Abelian one-relator)**.** *For any step $s \geq 2$,*

$$\Pr(N_{s,m}/\langle\langle g\rangle\rangle \text{ is abelian}) = \begin{cases} 6/\pi^2, & m = 2 \\ 0, & m \geq 3. \end{cases}$$

Note that these last two statements agree for $m = 2$, $|R| = m - 1 = 1$.

3.6 Trivializing and perfecting random groups

In this final section, we first find the threshold for collapse of a random nilpotent group, using the abelianization. Then we will prove a statement lifting facts about random nilpotent groups to facts about the LCS of classical random groups, deducing that *random groups are perfect* with exactly the same threshold again.

Recall that $T_{j,m} = \left\{\left[a_{i_1}, \ldots, a_{i_j}\right] \mid 1 \leq i_1, \ldots, i_j \leq m\right\}$ contains the basic nested commutators with j arguments. In this section we fix m and write F for the free group, so we can write F_i for the groups in its lower central series. Similarly we write N for $N_{s,m}$ (when s is understood), and T_j for $T_{j,m}$. Note that $\langle\langle T_j\rangle\rangle = F_j$, so $N = F/F_{s+1}$.

For a random relator set $R \subset F$, we write $\Gamma = F/\langle\langle R\rangle\rangle$, $G = N/\langle\langle R\rangle\rangle$, and $H = \mathbb{Z}^m/\langle R\rangle = \mathrm{ab}(\Gamma) = \mathrm{ab}(G)$, using the abuse of notation from Lemma 3.11 and treating R as a set of strings from F to be identified with its image in N or $\mathbb{Z}^m$. In all cases, R is chosen uniformly from freely reduced words of length ℓ or $\ell - 1$ in F.

Here we give an incomplete treatment of the threshold theorem. We also include a complete (but a lot more technical) proof in Section 3.7.

First we need a result describing the divisibility properties of the determinants of matrices whose columns record the coordinates of random relators.

Lemma 3.35 (Arithmetic distribution of determinants)**.** *For a fixed rank $m \geq 1$ and prime p, let M be an $m \times m$ random matrix whose entries are independently uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$ and let $\Delta = \det M$. Then*

$$\Pr(\Delta \equiv 0 \mod p) = 1 - \left[\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)\cdots\left(1 - \frac{1}{p^m}\right)\right],$$

and the remaining probability is uniformly distributed over the nonzero residues.

Proof. The number of nonsingular matrices with $\mathbb{F}_q$ entries is

$$\left|GL_m(\mathbb{F}_q)\right| = \left(q^m - 1\right)\left(q^m - q\right)\cdots\left(q^m - q^{m-1}\right)$$

out of q^{m^2} total matrices, where q is any prime power [30]. This establishes the probability that $p \mid \Delta$. On the other hand, it is a classical fact due to Gauss that every prime modulus has a primitive root, or a generator for its multiplicative group of nonzero elements. Suppose α is a primitive root mod p. If x is the random variable that is uniformly distributed in $\mathbb{Z}/p\mathbb{Z}$, then αx is as well. For any $m \times m$ matrix A, let $f(A)$ be the matrix whose entries are identical to A but $(f(A))_{1j} = \alpha a_{1j}$ for the first-row entries. Then $\det(f^k(A)) \equiv \alpha^k \Delta$. If $\Delta \not\equiv 0$, then this takes all nonzero values modulo p for $k = 0, 1, \ldots, m-1$. But since all of the matrix entries are distributed by the same law for each random matrix $f^k(M)$, it follows that Δ gives equal probability to each nonzero value mod p. □

The following theorem tells us that in sharp contrast to Gromov random groups, where the number of relators required to trivialize the group is exponential in ℓ, even the slowest-growing unbounded functions, like $\log\log\log\ell$ or an inverse Ackermann function, suffice to collapse random abelian groups and random nilpotent groups.

Theorem 3.36 (Collapsing abelian quotients). *For random abelian groups $H = \mathbb{Z}^m/\langle R\rangle$ with $|R|$ random relators, if $|R| \to \infty$ as a function of ℓ, then $H = \{0\}$ with probability one (a.a.s.). If $|R|$ is bounded as a function of ℓ, then there is a positive probability of a nontrivial quotient, both for each ℓ and asymptotically.*

Proof. For a relator g, its image in $\mathbb{Z}^m$ is the random vector $\mathbf{A}(g)$, which converges in distribution to a multivariate normal, as described in Section 3.2. Furthermore, the image of this vector in projection to $\mathbb{Z}/p\mathbb{Z}$ has entries independently and uniformly distributed. We will consider adding vectors to this collection R until they span $\mathbb{Z}^m$, which suffices to get $H = \{0\}$.

Choose m vectors $v_1, \dots v_m$ in $\mathbb{Z}^m$ at random. These vectors are a.a.s. $\mathbb{R}$-linearly independent, because their distribution is normal and linear dependence is a codimension-one condition. Therefore they span a sublattice $L_1 \subset \mathbb{Z}^m$. The covolume of L_1 (i.e., the volume of the fundamental domain) is $\Delta_1 = \det(v_1, \dots, v_m)$. As we add more vectors, we refine the lattice. Note that $\Delta_1 = 1$ if and only if $L_1 = \mathbb{Z}^m$. Similarly define L_k to be spanned by $v_{(k-1)m+1}, \dots, v_{km}$ for $k = 2, 3, \dots$, and define Δ_k to be the corresponding covolumes.

Note that for two lattices L, L', the covolume of the lattice $L \cup L'$ is always a common divisor of the respective covolumes Δ, Δ'. Therefore, the lattice $L_1 \cup \cdots \cup L_k$ has covolume $\leq \gcd(\Delta_1, \ldots, \Delta_k)$. Here, the Δ_k are identically and independently distributed with the probabilities described in the previous result (Lemma 3.35), and divisibility by different primes is independent, and therefore the probability of having $\gcd(\Delta_1, \ldots, \Delta_k) = 1$ is

$$\prod_{\text{primes } p} 1 - \left[1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) \cdots \left(1 - \frac{1}{p^m}\right)\right]^k,$$

which goes to 1 as $k \to \infty$. (To see this, note that first applying a logarithm, then exchanging the sum and the limit, gives an absolutely convergent sequence.)

On the other hand, it is immediate that for any finite $|R|$ there is a small but nonzero chance that all entries are even, say, which would produce a nontrivial quotient group. □

Of course this also follows immediately from the statement in Lemma 3.23, because

$$\Pr(\operatorname{span}\{v_1, \ldots, v_r\} = \mathbb{Z}^m) = \frac{1}{\zeta(r - m + 1) \cdots \zeta(r)} \longrightarrow 1$$

for any fixed m as $r \to \infty$, but the above argument is appealingly self-contained.

We immediately get corresponding statements for random nilpotent groups and standard random groups. Recall that a group Γ is called *perfect* if $\Gamma = [\Gamma, \Gamma]$; equivalently, if $\mathrm{ab}(\Gamma) = \Gamma / [\Gamma, \Gamma] = \{0\}$.

Corollary 3.37 (Threshold for collapsing random nilpotent groups)**.** *A random nilpotent group $G = N_{s,m} / \langle\langle R \rangle\rangle$ is a.a.s. trivial precisely in those models for which $|R| \to \infty$ as a function of ℓ.*

Corollary 3.38 (Random groups are perfect)**.** *Random groups $\Gamma = F_m / \langle\langle R \rangle\rangle$ are a.a.s. perfect precisely in those models for which $|R| \to \infty$ as a function of ℓ.*

Proof. $\mathbb{Z}^m/\langle R\rangle = \{0\} \iff \mathrm{ab}(\Gamma) = \{0\} \iff \mathrm{ab}(G) = \{0\} \iff G = \{1\}$, with the last equivalence from Theorem 3.3. □

We have established that the collapse to triviality of a random nilpotent group G corresponds to the immediate stabilization of the lower central series of the corresponding standard random group: $\Gamma_1 = \Gamma_2 = \dots$ In fact, we can be somewhat more detailed about the relationship between G and the LCS of Γ.

Theorem 3.39 (Lifting to random groups)**.** *$\Gamma = F_m/\langle\langle R\rangle\rangle$ and $G = N_{s,m}/\langle\langle R\rangle\rangle$ are related by the isomorphism $\Gamma/\Gamma_{s+1} \cong G$. Furthermore, the first s of the successive LCS quotients of Γ are the same as those in the LCS of G, i.e.,*

$$\Gamma_i/\Gamma_{i+1} \cong G_i/G_{i+1} \qquad \text{for } 1 \le i \le s.$$

Proof. Since homomorphisms respect LCS depth (Lemma 3.19), the quotient map $\phi : F \to \Gamma$ gives $\phi(F_j) = \Gamma_j$ for all j. We have

$$\Gamma/\Gamma_{s+1} \cong F/\langle\langle R, F_{s+1}\rangle\rangle \cong N/\langle\langle R\rangle\rangle = G$$

by Lemma 3.11 (string arithmetic).

From the quotient map $\psi : \Gamma \to G$, we get $\Gamma_i/\Gamma_{s+1} = \psi(\Gamma_i) = G_i$. Thus

$$G_i\Big/G_{i+1} \cong \Gamma_i/\Gamma_{s+1}\Big/\Gamma_{i+1}/\Gamma_{s+1} \cong \Gamma_i\Big/\Gamma_{i+1}. \quad \square$$

Corollary 3.40 (Step drop implies LCS stabilization)**.** *For $G = N_{s,m}/\langle\langle R\rangle\rangle$, if* $\mathrm{step}(G) = k < s = \mathrm{step}(N_{s,m})$*, then the LCS of the random group Γ stabilizes: $\Gamma_{k+1} = \Gamma_{k+2} = \dots$.*

Proof. This follows directly from the previous result, since $\mathrm{step}(G) = k$ implies that $G_{k+1} = G_{k+2} = 1$, which means $G_{k+1}/G_{k+2} = 1$. Since $k+1 \le s$, we conclude that $\Gamma_{k+1}/\Gamma_{k+2} =$

1. Thus $\Gamma_{k+2} = \Gamma_{k+1}$, and it follows by the definition of LCS that these also equal Γ_i for all $i \geq k+1$. □

Thus, in particular, when a random nilpotent group (with $m \geq 2$) is abelian but not trivial, the corresponding standard random group has its lower central series stabilize after one proper step:

$$\cdots\Gamma_4 = \Gamma_3 = \Gamma_2 \triangleleft \Gamma_1 = \Gamma$$

For instance, with balanced quotients of F_2 this happens about 92% of the time.

In future work, we hope to further study the distribution of steps for random nilpotent groups.

3.7 Detailed proof of Corollary 3.17 and Theorem 3.36

In this section we give a detailed (but technical) proof of Corollary 3.17 and Theorem 3.36. Here we state them again:

Corollary 3.17 (Probability of primitivity)**.** *For a random freely reduced word in F_m, the probability that it is primitive in abelianization tends to $1/\zeta(m)$, where ζ is the Riemann zeta function. In particular, for $m = 2$, the probability is $6/\pi^2$.*

Theorem 3.36 (Collapsing abelian quotients)**.** *For random abelian groups $H = \mathbb{Z}^m/\langle R\rangle$ with $|R|$ random relators, if $|R| \to \infty$ as a function of ℓ, then $H = \{0\}$ with probability one (a.a.s.). If $|R|$ is bounded as a function of ℓ, then there is a positive probability of a nontrivial quotient, both for each ℓ and asymptotically.*

Recall that we have: Y_ℓ is $\mathbb{Z}^m$-valued NBSRW. Let R_ℓ be the random walk on $\mathbb{Z}$ given by projecting Y_ℓ to a single coordinate. Let M_ℓ be $m \times m$ matrix-valued random variable whose columns are Y_ℓ, and let $\Delta = \Delta_\ell$ be its determinant, a $\mathbb{Z}$-valued random variable. Let $M_{k,\ell}$ be the $k \times k$ matrix-valued random variable whose columns are given by projections of Y_ℓ to the first k coordinates; that is, it's the upper left-hand $k \times k$ minor of M_ℓ, so that $R_\ell = M_{1,\ell}$.

If E_ℓ is an event that depends on a parameter ℓ, we use the symbol $\mathbb{P}(E_\ell)$ for the probability for fixed ℓ and write $\overline{\mathbb{P}}(E_\ell) := \lim_{\ell \to \infty} \mathbb{P}(E_\ell)$ for the asymptotic probability. If E is an event with respect to a matrix-valued random variable, we use the notation $\mathbb{P}'(E)$ to denote the conditional probability of E given that no matrix entries are zero.

Note that for any $\epsilon > 0$ and for large enough ℓ, we have $\overline{\mathbb{P}}(R_\ell < \ell^{1/2+\epsilon}) = 1$. Indeed, the expectation for $|R_\ell|$ is $\sqrt{\frac{\ell}{m-1}}$ by [15].

We will analyze primes by their size relative to ℓ. Define

$$\mathcal{P}_1 := \{p \le \log\log \ell\} \qquad \mathcal{P}_2 := \{\log\log \ell \le p \le \ell^{\frac{1}{2}-\epsilon}\}$$
$$\mathcal{P}_3 := \{\ell^{\frac{1}{2}-\epsilon} \le p \le \ell^{m+1}\} \qquad \mathcal{P}_4 := \{p \ge \ell^{m+1}\}.$$

Lemma 3.41 (Divisibility of coordinate projections)**.** *For every $m, n \ge 2$ and $\ell \gg 1$, there is a conditional probability bound given by*

$$\mathbb{P}(R_\ell \equiv 0 \mod n \mid R_\ell \ne 0) < 1/n.$$

Proof. This follows from the bell-curve shape of the distribution. □

Now Corollary 3.17 follows easily from the following lemma:

Lemma 3.42. *Let δ be the greatest common divisor of the entries of Y_ℓ. Then*

$$\overline{\mathbb{P}}(\delta > 1) = 1 - \frac{1}{\zeta(m)}.$$

Proof. We have

$$\begin{aligned}\mathbb{P}(p|\delta \text{ for some } p \in \mathcal{P}_1) < \mathbb{P}(\delta > 1) < \mathbb{P}'(p|\delta \text{ for some } p \in \mathcal{P}_1)\\ + \mathbb{P}'(p|\delta \text{ for some } p > \log\log \ell)\\ + \mathbb{P}(\text{some entry is zero})\end{aligned}$$

Now $\mathbb{P}(p|\delta \text{ for some } p \in \mathcal{P}_1) \to 1 - \frac{1}{\zeta(m)}$ by arithmetic uniformity and independence (Lemma 3.15 and Corollary 3.16). By Lemma 3.41,

$$\mathbb{P}'(p|\delta \text{ for some } p > \log\log \ell) < \sum_{p \notin \mathcal{P}_1} \frac{1}{p^m} \to 0,$$

where we have convergence because the sum is the tail of a converging sequence. Lastly, $\mathbb{P}(\text{some entry is zero}) \to 0$ and the lemma follows. □

Lemma 3.43 (Values of coordinate projections)**.** *There is a constant c_m such that for any $\alpha \in \mathbb{Z}$ and any $\epsilon > 0$,*

$$\mathbb{P}(R_\ell = \alpha) + \mathbb{P}(R_\ell > \ell^{\frac{1}{2}+\epsilon}) < \frac{c_m}{\sqrt{\ell}} \text{ for } \ell \gg 1.$$

Proof. Bounding $\mathbb{P}(R_\ell = \alpha)$ is achieved by straightforward Stirling approximation, and the second term decays exponentially. □

Lemma 3.44 (Divisibility of determinants by large primes)**.** *Fix $\epsilon > 0$. Then for sufficiently large ℓ and any large prime p (i.e., $p \geq \ell^{\frac{1}{2}+\epsilon}$), we have*

$$\mathbb{P}'(\det M_{k,\ell} \equiv 0 \mod p) < \frac{(m-1)c_m}{\sqrt{\ell}} + \frac{1}{p},$$

where $\mathbb{P}'$ denotes conditional probability given that the matrix entries are nonzero.

Proof. For fixed m, we induct on k. When $k = 1$, the statement follows from Lemma 3.41.

For $k > 1$, we introduce the equivalence relation $A \sim B \iff a_{ij} = b_{ij}$ for all $(i,j) \neq (k,k)$; that is, we declare two $k \times k$ matrices equivalent if they agree in all entries except possibly the bottom right. Then there is a constant C_M for each matrix M such that

$$\det A = a_{kk} \det N + C_M \qquad \forall A \in [M],$$

where N is the upper left-hand $(k-1) \times (k-1)$ minor. Now if $p \nmid \det N$, then solving for a_{kk} gives $(\det A - C_M)(\det N)^{-1} \bmod p$. For $\ell \gg 1$, the choice of p ensures that $|a_{kk}| < p/2$ with high probability; but there is only one matrix $A \in [M]$ with $-p/2 < a_{kk} < p/2$ satisfying the needed congruence. By Lemma 3.43, the probability that a matrix in $[M]$ takes a particular value or that the entry falls outside those bounds is at most $\frac{c_m}{\sqrt{\ell}}$. Finally, the induction hypothesis provides that the probability of $p | \det N$ is less than $(m-2)\frac{c_m}{\sqrt{\ell}} + \frac{1}{p}$. We get the needed bound from the expansion $\mathbb{P}'(E) = \mathbb{P}'(A) \cdot \mathbb{P}'(E|A) + \mathbb{P}'(A^c) \cdot \mathbb{P}'(E|A^c) \leq \mathbb{P}'(A) \cdot 1 + 1 \cdot \mathbb{P}'(E|A^c)$, namely

$$\mathbb{P}'(p|\det M_{k,\ell}) = \left(\frac{(m-2)c_m}{\sqrt{\ell}} + \frac{1}{p} \right) \cdot 1 + 1 \cdot \left(\frac{c_m}{\sqrt{\ell}} \right).$$

□

Lemma 3.45 (Divisibility of determinants by medium primes)**.** *For sufficiently large ℓ and any medium prime p (i.e., $\ell^{1/2-\epsilon} \leq p \leq \ell^{1/2+\epsilon}$), we have*

$$\mathbb{P}'(\det M_{k,\ell} \equiv 0 \mod p) < \frac{2(m-1)c_m}{\ell^{\frac{1}{2}-2\epsilon}} + \frac{1}{p},$$

where $\mathbb{P}'$ denotes conditional probability given that the matrix entries are nonzero.

Proof. We induct on m. Then in each equivalence class $[M]$, we have $\det A = \det N \cdot a_{nn} + C_M$ as before. For large enough ℓ, we may assume all the entries are less than $\ell^{1/2+\epsilon}$. Now if $p \nmid \det N$, then solving for a_{kk} gives $(\det A - C_M)(\det N)^{-1} \bmod p$, so at most $1/p$ of the a_{kk} values in $\mathbb{Z}$ give a possible solution. Thus there are at most $2\ell^{1/2+\epsilon}/p$ matrices $A \in [M]$ with determinant divisible by p in this case, and this has a conditional probability at most $\frac{2\ell^{1/2+\epsilon}}{p}\frac{c}{\sqrt{\ell}} < \frac{c}{\ell^{1/2-2\epsilon}}$ (given that the matrix falls in the equivalence class).

Finally, the induction hypothesis says that the probability that $\det N$ is divisible by p is $< (m-2)\frac{c}{\ell^{1/2-2\epsilon}} + \frac{1}{p}$. Thus, the lemma follows by induction. □

These two lemmas together gives us that there is some c'_m such that for any $p \in \mathcal{P}_3$

$$\mathbb{P}'(p \mid \Delta_i) < c'_m l^{2\epsilon - \frac{1}{2}} < c'_m p^{\frac{4\epsilon-1}{2m+2}}$$

Lemma 3.46 (Divisibility of determinants by small primes)**.** *For a fixed $p \in \mathcal{P}_1$,*

$$\mathbb{P}(p \mid d_\ell) = \left[1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)\cdots\left(1 - \frac{1}{p^m}\right)\right]^k + O(e^{-\ell})$$

Proof. The number of nonsingular matrices with $\mathbb{F}_p$ entries is

$$\left|GL_m(\mathbb{F}_p)\right| = (p^m - 1)(p^m - p)\cdots\left(p^m - p^{m-1}\right)$$

out of p^{m^2} total matrices [30]. Thus the lemma follows from the fact that each entry approaches a uniform distribution with the error term decays exponentially fast in ℓ. □

Lemma 3.47 (Nonsingularity)**.** $\overline{\mathbb{P}}(\Delta = 0) = 0$.

Proof. Determinant zero is a codimension one condition. □

Now let's define a $\mathbb{Z}$-valued random variable $d_\ell := \gcd(\Delta_1, \ldots, \Delta_k)$ for a fixed k.

Lemma 3.48 (Common divisors of random determinants)**.** *Fix m and $k > 4m + 4$.*

$$\overline{\mathbb{P}}(d_\ell = 1) = \prod_{primes\ p} 1 - \left[1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)\cdots\left(1 - \frac{1}{p^m}\right)\right]^k.$$

Proof. We'll break down the probability by the sizes of possible prime divisors relative to ℓ. Fix $\epsilon > 0$ sufficiently small that $\frac{4m+4}{1-4\epsilon} \le k$ to partition the primes $\mathcal{P}$ into the size ranges $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, and $\mathcal{P}_4$. Let $P_m(p) := 1 - \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)\cdots\left(1 - \frac{1}{p^m}\right)$, as in the statement of the lemma, and note that

$$P_m(p) = \frac{1}{p} + \frac{-1}{p^2} + \frac{0}{p^3} + \cdots + \frac{(-1)^m}{p^{\binom{m+1}{2}}},$$

with appropriate integer numerators.

For one bound, we have $d_\ell > 1$ iff there exists some prime p such that $p \mid \Delta_1, \dots, \Delta_k$, where the Δ_i are i.i.d. random variables. For each ℓ we have

$$\mathbb{P}(p \mid d_\ell \text{ for some } p \in \mathcal{P}_1) = 1 - \mathbb{P}(p \nmid d_\ell \text{ for every } p < \log\log\ell)$$

$$= 1 - \prod_{\mathcal{P}_1}\left(1 - [P_m(p)]^k\right) + O(e^{-\ell}) \longrightarrow 1 - \prod_{\mathcal{P}}\left(1 - [P_m(p)]^k\right),$$

where the product expression is valid because $\prod_{p<\log\log\ell} p < \sqrt{\ell}$, which means that the events of divisibility by the primes in the class are asymptotically independent, with exponentially small error term. This shows that $\overline{\mathbb{P}}(d_\ell = 1) < \prod_{\text{primes } p}\left(1 - [P_m(p)]^k\right)$.

Next,

$$\mathbb{P}(p \mid d_\ell \text{ for some } p \in \mathcal{P}_2) < \sum_{\mathcal{P}_2}\mathbb{P}(p|d_\ell) = \sum_{\mathcal{P}_2}\left(P_m(p) + O(e^{-\ell})\right)^k$$

$$= \sum_{\mathcal{P}_2}\left(\frac{1}{p} + \frac{-1}{p^2} + \frac{0}{p^3} + \cdots + \frac{(-1)^m}{p^{\binom{m+1}{2}}} + O(e^{-\ell})\right)^k = \sum_{\mathcal{P}_2}\left(\frac{1}{p^k} + \cdots + \frac{(-1)^{mk}}{p^{k\binom{m+1}{2}}} + O(e^{-\ell})\right) \longrightarrow 0,$$

where the $P_m(p)$ term appears because $p < \ell^{\frac{1}{2}-\epsilon}$ means we can apply Lemma 3.46. To justify the convergence to zero, note that each individual $\sum_{\mathcal{P}_2} \frac{a}{p^b}$ has $b \ge k$, and so is part of the tail of a convergent p-series; all other terms are $\ell^{\frac{1}{2}-\epsilon}\frac{a}{(\log\log\ell)^b}O(e^{-\ell})$ (obtained by using $\ell^{\frac{1}{2}-\epsilon}$ as an upper bound for the number of terms in the sum), and these do not contribute.

Now observe

$$\mathbb{P}(d_\ell > 1) < \left(\sum_{j=1}^{4} \mathbb{P}'(p|d_\ell \text{ for some } p \in \mathcal{P}_j) \right) + \mathbb{P}(\text{some entry is zero}).$$

We now compute the case of $\mathcal{P}_3 = \{\ell^{\frac{1}{2}-\epsilon} \leq p \leq \ell^{m+1}\}$.

$$\mathbb{P}'(p \mid d_\ell \text{ for some } p \in \mathcal{P}_3) \leq \sum_{\mathcal{P}_3} \mathbb{P}'(p \mid d_\ell) = \sum_{\mathcal{P}_3} \left(\mathbb{P}'(p \mid \Delta_i)^k \right) < \sum_{\mathcal{P}_3} c'_m \cdot p^{\frac{4\epsilon-1}{2m+2}k}.$$

Since the sum over all primes of $p^{-k/2}$ converges, this certainly converges to zero as $\ell \to \infty$.

In the range $p > \ell^{m+1}$, since all coordinates of the random walk vector are $\leq \ell$, we have $|\Delta| \leq m!\ell^m < \ell^{m+1}$ for $\ell \gg 1$. Since $\Delta = 0$ is an asymptotically negligible event (Lemma 3.47), we have $\mathbb{P}'(p|d_\ell \text{ for some } p > \ell^{m+1}) \longrightarrow 0$. Finally, the probability of a zero entry also goes to zero (Lemma 3.43), which completes the proof. □

If we take k to be a function of ℓ such that $k \to \infty$, then $\overline{\mathbb{P}}(d_\ell = 1) = 1$. This proves Theorem 3.36.

Chapter 4

Describing Groups

4.1 Introduction

One important aspect of computable structure theory is the study of the computability-theoretic complexity of structures. Historically, there are many natural questions of this flavor even outside the realm of logic. For example, the word problem for groups asks: for a given finitely-generated group, is there an algorithm that can determine if two words are the same in the group? It was shown in [29] that there is such an algorithm if and only if the group is computable in the sense of computability theory.

In this work, we will study the computability-theoretic complexity of groups. Among many different notions of complexities of a structure, we look at the quantifier complexity of a computable Scott sentence and the complexity of the index set.

4.1.1 Background in recursive structure theory

Instead of just using the first-order language, we will work in $\mathcal{L}_{\omega_1,\omega}$. This is the language where we allow countable disjunctions and countable conjunctions in addition to the usual first-order language. A classic theorem of Scott shows that this gives all the expressive power one needs for countable structures.

Theorem 4.1 (Scott, [32])**.** *Let L be a countable language, and $\mathcal{A}$ be a countable structure in L. Then there is a sentence in $\mathcal{L}_{\omega_1,\omega}$ whose countable models are exactly the isomorphic copies of $\mathcal{A}$. Such a sentence is called a* Scott sentence *for $\mathcal{A}$.*

To work in a computability setting, this is not good enough, because we also want the sentence to be computable in the following way:

Definition 4.2. *We say a set is* computably enumerable *(*c.e.*, or* recursively enumerable*,* r.e.*) if there is an algorithm that enumerates the elements of the set.*

We say a sentence (or formula) in $\mathcal{L}_{\omega_1,\omega}$ is computable *if all the infinite conjunctions and disjunctions in it are over c.e. sets. Similarly, we define a* computable Scott sentence *to be a Scott sentence which is computable.*

All the $\mathcal{L}_{\omega_1,\omega}$ sentences and formulas we mention in this chapter will be computable, so we will say Scott sentence instead of computable Scott sentence.

We say a structure is *computable* if its atomic diagram is computable. We also identify a structure with its atomic diagram. However, the effective Scott theorem is not true, that is, not all computable structures have a computable Scott sentence.

We say an $\mathcal{L}_{\omega_1,\omega}$ formula is Σ_0 or Π_0 if it is finitary (i.e. no infinite disjunction or conjunction) and quantifier free. For $\alpha > 0$, a Σ_α formula is a countable disjunction of formulas of the form $\exists x \phi$ where ϕ is Π_β for some $\beta < \alpha$. Similarly, a Π_α formula is a countable conjunction of formulas of the form $\forall x \phi$ where ϕ is Σ_β for some $\beta < \alpha$. We say a formula is d-Σ_α if it is a conjunction of a Σ_α formula and a Π_α formula. The complexity of Scott sentences of groups will be one of the main topics throughout this chapter.

Another complexity notion we will study is the following:

Definition 4.3. *For a structure $\mathcal{A}$, the* index set *$I(\mathcal{A})$ is the set of all indices e such that ϕ_e gives the atomic diagram of a structure $\mathcal{B}$ with $\mathcal{B} \cong \mathcal{A}$.*

There is a connection between the two complexity notions that we study:

Proposition 4.4. *For a complexity class Γ, if we have a computable Γ Scott sentence for a structure $\mathcal{A}$, then the index set $I(\mathcal{A})$ is in Γ.*

This proposition and many examples lead to the following thesis:

> For a given computable structure $\mathcal{A}$, to calculate the precise complexity of $I(\mathcal{A})$, we need a good description of $\mathcal{A}$, and once we have an "optimal" description, the complexity of $I(\mathcal{A})$ will match that of the description.

In this chapter, we focus on the case where the above-mentioned structures are groups. The thesis is shown to be false in [21], where they found a subgroup of $\mathbb{Q}$ with index set being d-Σ_2 (shorthand of d-Σ_2^0) which cannot have a computable d-Σ_2 Scott sentence. However, in the case of finitely-generated groups, the thesis is still open, and the groups we considered give further evidence for the thesis in this case. For more background in computable structure theory, we refer the reader to [1].

4.1.2 Groups

We fix the signature of groups to be $\{\cdot,^{-1},1\}$. Throughout the chapter, we will often identify elements (words) in the free group $F_k = F(x_1,\dots,x_k)$ with functions from $G^k \to G$, by substituting x_i by the corresponding elements from G, and do the group multiplication in G. Here we restate the relation between word problem and computability of the group:

Theorem 4.5 ([29]). *A finitely-generated group is computable if and only if it has solvable word problem.*

In this chapter, all the groups we consider will be computable.

4.1.3 History

Scott sentences and index sets for many classes of groups have been studied, for example, reduced abelian p-groups [7], free groups [8], finitely-generated abelian groups, the infinite dihedral group D_∞, and torsion-free abelian groups of rank 1 [22]. We will not list all the results, but will mention many of them as needed.

4.1.4 Overview of results

For the reader's convenience, we summarize the main results of each section:

- (Section 2) Every polycyclic group (including the nilpotent groups) has a computable d-Σ_2 Scott sentence, and the index set of a finitely-generated non-co-Hopfian nilpotent group is m-complete d-Σ_2.

- (Section 3) Certain finitely-generated solvable groups, including $(\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}$, $\mathbb{Z} \wr \mathbb{Z}$, and the solvable Baumslag–Solitar groups $BS(1, n)$, have computable d-Σ_2 Scott sentences and their index sets are m-complete d-Σ_2.

- (Section 4) The infinitely-generated free nilpotent group has a computable Π_3 Scott sentence and its index set is m-complete Π_3.

- (Section 5) We give an example of a subgroup of $\mathbb{Q}$ whose index set is m-complete Σ_3, achieving an upper bound of such groups given in [22].

- (Section 6) We give another example of a subgroup of $\mathbb{Q}$ which has both computable Σ_3 and computable Π_3 pseudo-Scott sentences, but has no computable d-Σ_2 pseudo-Scott sentence, contrasting a result in the Borel hierarchy of $\mathrm{Mod}(\mathcal{L})$.

4.2 Finitely-generated nilpotent and polycyclic groups

In this section, we will focus on finitely-generated groups, especially nilpotent and polycyclic groups. A priori, even if a structure is computable, it might not have a computable Scott sentence. However, the following theorem says that a computable finitely-generated group always has a computable Scott sentence.

Theorem 4.6 (Knight, Saraph, [22]). *Every computable finitely-generated group has a computable Σ_3 Scott sentence.*

If we think of nilpotent and polycyclic groups as classes of "tame" groups, then the abelian groups are the "tamest" groups. Using the fundamental theorem of finitely-generated abelian groups, which says that every finitely-generated abelian group is a direct sum of cyclic groups, one can obtain the following theorem saying that the previous computable Scott sentences are not optimal in the case of abelian groups:

Theorem 4.7 (Knight, Saraph, [22]). *Let G be an infinite finitely-generated abelian group. Then G has a computable d-Σ_2 Scott sentence. Furthermore, $I(G)$ is m-complete d-Σ_2.*

This theorem, together with some other results in [22], leads to the question: Does every finitely-generated group have a computable d-Σ_2 Scott sentence? Generalizing the previous theorem, we show that this is true for polycyclic groups, and also prove completeness for certain classes of groups. We start by giving the definition for several group-theoretic notions that are used in the discussion.

Definition 4.8. *For two subgroups N, M of G, we write $[N, M]$ to be the subgroup of G generated by all commutators $[n, m]$ with $n \in N$ and $m \in M$.*

For a group G, we inductively define $G_1 = G$ and $G_{k+1} = [G_k, G]$. We call G_k the k-th term in the lower central series. *A group is called* nilpotent *if G_{k+1} is the trivial group for some k, and the smallest such k is called the* nilpotency class *of the group. Note that G is abelian if its nilpotency class equals 1.*

We also inductively define $Z_0(G) = 1$ and $Z_{k+1}(G) = \{x \in G \mid \forall y \in G, [x, y] \in Z_i(G)\}$. We call $Z_k(G)$ the k-th term in the upper central series. *It is well-known that a group G is nilpotent if and only $Z_k(G) = G$ for some k. In this case, the smallest such k is equal to to the nilpotency class of the group.*

We define the free nilpotent group *of rank m and class p by $N_{p,m} = F(m)/F(m)_{p+1}$, where $F(m)$ is the free group of m generators.*

Definition 4.9. *For a group G, we inductively define $G^{(0)} = G$ and $G^{(k+1)} = [G^{(k)}, G^{(k)}]$. We call $G^{(k)}$ the k-th term in the* derived series. *In the case when $k = 1$, this is the* derived subgroup *$G' = G^{(1)}$ of G. A group is called* solvable *if $G^{(k)} = 1$ for some k, and the smallest such k is called the* derived length *of the group. Note that G is abelian if its derived length equals 1.*

Definition 4.10. *A polycyclic group is a solvable group in which every subgroup is finitely-generated.*

By definition, every polycyclic group is solvable. It is well known that every finitely-generated nilpotent group is polycyclic. It is also known that all polycylic groups have solvable word problem, and thus are computable. By contrast, an example of a finitely-presented solvable but non-computable group is given in [20].

We start by giving a sentence saying a tuple generates a subgroup isomorphic to a given finitely-generated computable group G. We first fix a presentation $\langle \overline{a} \mid R \rangle$ of G, where R is normally closed. The solvability of the word problem of G then says R is computable. Throughout this chapter, we will write $\langle \overline{x} \rangle \cong G$ to be shorthand for

$$\bigwedge_{w(\overline{a}) \in R} w(\overline{x}) = 1 \wedge \bigwedge_{w(\overline{a}) \notin R} w(\overline{x}) \neq 1.$$

Since R is computable, the sentence is also computable, and we see it is Π_1. And since $\overline{x}$ satisfies all the relations of $\overline{a}$ and nothing more, this sentence implies $\langle \overline{x} \rangle \cong \langle \overline{a} \rangle = G$. However, this actually says more – this sentence requires that these two groups are generated in the same way. Thus, for instance, if a_1 is a central element in G, then so is x_1. This will be a useful observation later. This also implies that the choice of presentation is relevant. In most of our discussion, the choice will be implicit, which is usually the standard presentation (i.e. the one given in the definition.)

The following is a very useful lemma for finding a computable Scott sentence for finitely-generated groups. We will use this lemma for both polycyclic and solvable groups.

Lemma 4.11 (Generating Set Lemma). *In a computable group G, if there is a non-empty computable Σ_2 formula $\phi(\overline{x})$ such that every $\overline{x} \in G$ satisfying ϕ is a generating tuple of the group, then G has a computable d-Σ_2 Scott sentence.*

Proof. Consider the Scott sentence which is the conjunction of the following:

1. $\forall \overline{x} \left[\phi(\overline{x}) \rightarrow \forall y \bigvee_{w} w(\overline{x}) = y \right]$

2. $\exists \overline{x}\,[\phi(\overline{x}) \wedge \langle \overline{x} \rangle \cong G]$

In (1), w ranges over all words in $\overline{x}$.

Note that (1) is Π_2 and (2) is Σ_2, thus the conjunction is d-Σ_2. To see this is a Scott sentence, pick a group H satisfying the sentence. Then pick a tuple $\overline{x} \in H$ that satisfies the second conjunct. The first conjunct then says H is generated by $\overline{x}$, thus is isomorphic to G. □

We now are ready to state and prove our theorem about polycyclic groups, which generalizes the result in [22] about infinite finitely-generated abelian groups.

Theorem 4.12. *Every polycyclic group G has a computable d-Σ_2 Scott sentence.*

Proof. We will prove the claim that there is a d-Σ_1 formula $\phi(\overline{x})$ such that every $\overline{x} \in G$ satisfying ϕ is a generating set of the group. We induct on the derived length of G.

When the derived length is 1, i.e. G is abelian, the statement of the theorem was proved in [22], but for the inductive hypothesis, we need to find ϕ for G. For simplicity, we think of G additively in this case. By the fundamental theorem of abelian groups, suppose $G \cong \mathbb{Z}^n \oplus T$, where T is the torsion part of G, and $|T| = k$. Let $\chi(\overline{y})$ be the (finitary) sentence saying the k-tuple $\overline{y}$ satisfies the atomic diagram of T. Then we consider $\phi(\overline{x}, \overline{y})$ to be

$$\chi(\overline{y}) \wedge (\bigwedge_{m>1} mx \neq 1) \wedge (\bigwedge_{\det(M)\neq\pm1} \forall \overline{z} \bigwedge_{\langle i_j \rangle \in k^n} M\overline{z} \neq \overline{x} + \langle y_{i_j} \rangle).$$

Here, we use two tuples $\overline{x}$ and $\overline{y}$ for clarity, but one can concatenate them into just one tuple $\overline{x}$.

The first conjunct says that $\overline{y}$ is exactly the k torsion elements in the group. The second conjunct says $\overline{x}$ is torsion-free. In the third conjunct, we are thinking $\overline{z}$, $\overline{x}$, and $\langle y_{i_j} \rangle$ as row vectors, and M ranges over all $n \times n$ matrices with entries in $\mathbb{Z}$ and determinant not equal to ±1. Thus $\bigwedge_{\langle i_j \rangle \in k^n} M\overline{z} \neq \overline{x} + \langle y_{i_j} \rangle$ is really saying $M\overline{z} \neq \overline{x}$ modulo T. So, working modulo T and again thinking of the x_i's as row vectors in $\mathbb{Z} \cong G/T$, the third conjunct forces $\overline{x}$, as an $n \times n$ matrix, to have determinant ±1. Thus, $\overline{x}$ is a basis of G modulo T, and so every $\overline{x}, \overline{y}$ satisfying ϕ will generate the group G. Finally, we see that the sentence is Π_1, thus proving the induction base.

Now we prove the induction step. Assume the claim is true for all polycyclic groups with derived length less than that of G. In particular, the derived subgroup G' has a computable d-Σ_1 formula $\phi_{G'}$ as described in the claim. In G, G' is defined by the computable Σ_1 formula

$$G'(x) \equiv \exists \overline{s} \bigvee_{w \in (F_{|\overline{s}|})'} x = w(\overline{s}).$$

Thus, we may relativize ϕ by replacing $\exists \overline{x} \theta(\overline{x})$ by $\exists \overline{x}(G'(\overline{x}) \wedge \theta(\overline{x}))$, $\forall \overline{x} \theta(\overline{x})$ by $\forall \overline{x}(G'(\overline{x}) \to \theta(\overline{x}))$, and adding one more conjunct $\bigwedge_i G'(x_i)$. This does not increase the complexity of the sentences. Furthermore, every element of G satisfying the relativized version $\tilde{\phi}_{G'}$ of $\phi_{G'}$ generates G' in G. As in the base case, suppose $G/G' \cong \mathbb{Z}^n \oplus T$, where T is the torsion part, and let $\chi(\overline{y})$ to be the atomic diagram of T. We consider $\phi(\overline{x}, \overline{y}, \overline{z})$ to be the conjunction of the following:

1. $(\bigwedge_{m>1} mx \mathrel{\hat{\neq}} 1) \wedge (\bigwedge_{\det(M) \neq \pm 1} \forall \overline{z} \bigwedge_{\langle i_j \rangle \in k^n} M\overline{z} \mathrel{\hat{\neq}} \overline{x} + \langle y_{i_j} \rangle)$
2. $\hat{\chi}(\overline{y})$
3. $\tilde{\phi}_{G'}(\overline{z})$

Notice that in (1) we still think of G/G' additively for clarity, while we should really think of it multiplicatively since G is no longer abelian. This is very similar to the sentence in the base case, but everything is relativized. We write $a \hat{=} b$ to denote that $\exists g(G'(g) \wedge a = bg)$, i.e. a and b are equal in the quotient group, and this is Σ_1. And we write $a \hat{\neq} b$ to denote the negation of $a \hat{=} b$, which is Π_1. So, the complexity of (1) is still Π_1. For $\hat{\chi}(\overline{y})$, again we replace all the $=$ and $\neq$ in χ by the relativized versions $\hat{=}$ and $\hat{\neq}$, hence making it d-Σ_1. The relativization doesn't increase the complexity of $\phi_{G'}$, thus the whole conjunct is d-Σ_1.

Now (2) says $\overline{y}$ is T in G/G', (1) says $\overline{x}$ generates $\mathbb{Z}^n$ in G/G', and (3) says $\overline{z}$ generates G' in G. Thus, $\overline{x}, \overline{y}$, and $\overline{z}$ together generate G, hence proving the claim. The theorem now follows from the Generating Set Lemma (Lemma 4.11). □

We now turn our attention to index sets. We give some results on the completeness of index sets of nilpotent groups, but we need a group-theoretic lemma and a definition first.

Proposition 4.13 (Finitely-generated nilpotent group lemma)**.** *Every finitely-generated infinite nilpotent group has infinite center. In particular the center is isomorphic to $\mathbb{Z} \times A$ for some abelian group A.*

Proof. We induct on the nilpotency class. The statement is obvious when the nilpotency class is 1.

Suppose N is a finitely-generated nilpotent group with finite center. It suffices to show that N is finite. Let the order of the center $Z(N)$ be k. Then $Z(N)^k = 1$. Let the upper central series of N be $1 = Z_0(N) \lhd Z_1(N) \lhd Z_2(N) \lhd \cdots \lhd Z_p(N) = N$. For $g \in Z_2(N)$ and $h \in N$, one has $[g, h] \in Z(N)$. Thus, using the identity $[xy, z] = [y, z]^x [x, z]$, we have $[g^k, h] = [g, h]^k = 1$, and so $g^k \in Z(N)$, i.e., $Z_2(N)/Z(N)$ has exponent dividing k.

Now consider $M = N/Z(N)$. We have $Z(M) = Z_2(N)/Z(N)$, thus has exponent dividing k. Since N is finitely-generated and nilpotent, so is M, and so is $Z(M)$. Hence $Z(M)$ is finite. But the nilpotency class of M is less than that of N, so by the induction hypothesis, M is finite. Then $|N| = |M| \cdot |Z(N)|$ is also finite. □

Definition 4.14. *A group is* co-Hopfian *if it does not contain an isomorphic proper subgroup.*

Consider G to be a finitely-generated non-co-Hopfian group. Then let $\phi : G \to G$ be an injective endomorphism from G onto one of its proper isomorphic subgroups. Then we can form the direct system $G \xrightarrow{\phi} G \xrightarrow{\phi} G \xrightarrow{\phi} \cdots$, and write the direct limit as $\hat{G}$. Since every finite subset of $\hat{G}$ is contained in some finite stage, $\hat{G}$ is not finitely-generated, thus is not isomorphic to G. This observation will be used later.

We're now ready to prove the completeness result:

Theorem 4.15. *The index set of a finitely-generated nilpotent group is Π_2-hard. Furthermore, the index set of a non-co-Hopfian finitely-generated nilpotent group N is d-Σ_2-complete.*

Proof. We start by proving the second statement. Fix ϕ to be an injective endomorphism of N onto one of its proper isomorphic subgroups. Then we apply the construction above to obtain $\hat{N}$.

For a d-Σ_2 set S, we write $S = S_1 \setminus S_2$, where $S_1 \supseteq S_2$ are both Σ_2 sets, and we let $S_{1,s}$ and $S_{2,s}$ be uniformly computable sequences of sets such that $n \in S_i$ if and only if for all but finitely many s, $n \in S_{i,s}$. Then we construct

$$G_n \cong \begin{cases} \hat{N}, & n \notin S_1 \\ N, & n \in S_1 \smallsetminus S_2 \\ N \times \mathbb{Z}, & n \in S_1 \cap S_2. \end{cases}$$

To build the diagram of G_n, at stage s, we build a finite part of G_n and a partial isomorphism to one of these three groups based on whether $n \notin S_{1,s}$, $n \in S_{1,s} \smallsetminus S_{2,s}$, or $n \in S_{1,s} \cap S_{2,s}$. It is clear how to build the partial isomorphisms, since all the groups are computable, so we only need to explain how we can change between these groups when $S_{1,s}$ and $S_{2,s}$ change.

To change from N to $\hat{N}$, we apply ϕ. Note that at every finite stage, the resulting group will still be isomorphic to N, but in the limit, it will be $\hat{N}$ if and only if we apply ϕ infinitely often, i.e., $n \notin S_1$, as desired.

To change from N to $N \times \mathbb{Z}$, we simply create a new element a that has infinite order and commutes with everything else. To change from $N \times \mathbb{Z}$ to N, we choose an element b of infinite order in $Z(N)$ by the finitely-generated nilpotent group lemma (Lemma 4.13). We collapse the new element a by equating it with a big enough power of b. (Indeed, there is an elementary extension G of N with an element g of infinite order such that $N \times \langle g \rangle \cong N \times \mathbb{Z}$. Thus $N \subseteq N \times \langle g \rangle \subseteq G$, and hence $(N, \overline{h}) \leq_1 (N \times \mathbb{Z}, \overline{h})$ for every finite tuple $\overline{h} \in N$.) Again, this will result in the limiting group being N if we collapse b infinitely often, i.e. $n \notin S_2$, and $N \times \mathbb{Z}$ if we collapse b only finitely often, i.e. $n \in S_2$.

The second statement follows from doing only the Π_2 part of the above argument, i.e. constructing

$$G_n \cong \begin{cases} N, & n \notin S_2 \\ N \times \mathbb{Z}, & n \in S_2. \end{cases}$$

□

Note that here we do not have a completeness result for the class of co-Hopfian finitely-generated nilpotent groups. For a discussion about this ad-hoc class of groups, we refer the readers to [4]. However, "most" finitely-generated nilpotent groups are non-co-Hopfian, including the finitely-generated free nilpotent groups, and we have the following:

Corollary 4.16. *The index set of a finitely-generated free nilpotent group is d-Σ_2-complete.*

Note. *Using the nilpotent residual property (Lemma 4.28), we can show the d-Σ_2 completeness result for free nilpotent groups within the class of free nilpotent groups, provided that the number of generators is more than the step of the group. For the definition and more discussion on the complexity within a class of groups, we refer the reader to [8].*

To close this section, we state a proposition about co-Hopfian and non-co-Hopfian groups.

Proposition 4.17. *The index set of a computable finitely-generated non-co-Hopfian group is Σ_2-hard. On the other hand, a computable finitely-generated co-Hopfian group G has a computable d-Σ_2 Scott sentence.*

Proof. The first statement is proved by running the Σ_2 part of the argument in Theorem 4.15.

For the second statement, consider the computable Π_1 formula $\phi(\overline{x}) \equiv \langle \overline{x} \rangle \cong G$. This is a non-empty formula, and since G is co-Hopfian, every realization of ϕ in G generates G. Thus by the Generating Set Lemma (Lemma 4.11), G has a computable d-Σ_2 Scott sentence. □

4.3 Some examples of finitely-generated solvable groups

In this section, we continue to look at the bigger, but still somewhat tame, class of finitely-generated solvable groups. Note that even though the class of solvable groups is closed under subgroups, the class of finitely-generated solvable groups is not. This leads to an inherent difficulty when dealing with solvable groups, namely a group could possibly contain a higher-complexity subgroup. For example, the lamplighter group, which we shall define later and prove to have a computable d-Σ_2 Scott sentence, contains a subgroup isomorphic to $\mathbb{Z}^\omega$, whose index set is m-complete Π_3.

We start this section with the definition of the (regular, restricted) wreath product, which is a technique often used in group theory to construct counterexamples:

Definition 4.18. *For two groups G and H, we define the* wreath product $G \wr H$ *of G by H to be the semidirect product $B \rtimes H$, where the* base group B *is the direct sum of $|H|$ copies of G indexed by H, and the action of H on B is by shifting the coordinates by left multiplication.*

One important example of a finitely-generated solvable group is the lamplighter group. It is usually defined as the wreath product $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$, but we will be looking at two generalizations of it, $(\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}$ and $\mathbb{Z} \wr \mathbb{Z}$.

Theorem 4.19. *The* lamplighter groups $L_d = (\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}$ *each have computable d-Σ_2 Scott sentences. Furthermore, their index sets are m-complete d-Σ_2.*

Proof. To find the Scott sentence, we will use the Generating Set Lemma (Lemma 4.11). Consider the formula

$$\phi(a,t) \equiv (\langle a,t\rangle \cong L_d) \wedge (\forall s \bigwedge_{i>1} a^t \neq a^{(s^i)}) \wedge (\forall b \bigwedge_{\overline{k}} \prod_i (b^{k_i})^{t^i} \neq a).$$

In the second conjunct, s ranges over the group elements. In the second infinite conjunction, $\overline{k}$ ranges over all sequences in $\mathbb{Z}$ indexed by $\mathbb{Z}$ and has only finitely many, but at least two, nonzero entries. We first observe that the standard generator satisfies this formula, so ϕ does not define the empty set.

Now let (a,t) be a tuple satisfying ϕ. The first conjunct implies that a is in the base group, and t is not in the base group. The second conjunct says that if we think of t as an element of the semidirect product $L_d \cong (\mathbb{Z}/d\mathbb{Z})^{\mathbb{Z}} \rtimes \mathbb{Z}$, then the $\mathbb{Z}$-coordinate of t is ± 1. The third coordinate then says that a does not have more than one nonzero entries, and hence (by the first conjunct) the only nonzero entry must be co-prime to d. Thus, a generates a copy of $\mathbb{Z}/d\mathbb{Z}$. Using conjugation by t to generate the other copies of $\mathbb{Z}/d\mathbb{Z}$, we see a together with t generate the whole group. So by the Generating Set Lemma (Lemma 4.11), L_d has a computable d-Σ_2 Scott sentence.

To show completeness of the index set, fix ϕ to be an injective endomorphism of L_d onto one of its proper isomorphic subgroups, say mapping the standard generators (a,t) to (a,t^2). Let $\hat{L}_d$ be the direct limit of $L_d \xrightarrow{\phi} L_d \xrightarrow{\phi} L_d \xrightarrow{\phi} \cdots$.

For a d-Σ_2 set S, we write $S = S_1 \setminus S_2$, where $S_1 \supseteq S_2$ are both Σ_2 sets, and we let $S_{1,s}$ and $S_{2,s}$ be uniformly computable sequences of sets such that $n \in S_i$ if and only if for all but finitely many s, $n \in S_{i,s}$. Then we construct

$$G_n \cong \begin{cases} \hat{L}_d, & n \notin S_1 \\ L_d, & n \in S_1 \setminus S_2 \\ (\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}^2, & n \in S_1 \cap S_2. \end{cases}$$

As in the nilpotent case (Theorem 4.15), we build a partial isomorphism of one of these groups in stages. To change between L_d and $\hat{L}_d$ is the same as before, we apply ϕ whenever $n \notin S_{1,m}$, and keep building L_d otherwise.

To change from L_d to $(\mathbb{Z}/d\mathbb{Z})\wr\mathbb{Z}^2$, we create a new element s to be the other generator of $\mathbb{Z}^2$, and equate it with a big enough power of t to change back. (Again, there is an elementary extension G of L_d with an element g of infinite order such that $\langle L_d, g\rangle \cong (\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}^2$. Thus $L_d \subseteq \langle L_d, g\rangle \subseteq G$, and hence $(L_d, \overline{h}) \leq_1 ((\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}^2, \overline{h})$ for every finite tuple $\overline{h} \in N$.) This will result in the limiting group being L_d if we collapse s infinitely often, i.e. $n \notin S_2$, and $(\mathbb{Z}/d\mathbb{Z}) \wr \mathbb{Z}^2$ otherwise. □

Theorem 4.20. *Let $L = \mathbb{Z} \wr \mathbb{Z}$. Then L has a computable d-Σ_2 Scott sentence, and $I(L)$ is m-complete d-Σ_2.*

Sketch of proof. The proof is essentially the same as above. The Π_1 formula will be

$$\phi(a,t) \equiv (\langle a,t\rangle \cong L) \wedge (\forall s \bigwedge_{i>1} a^t \neq a^{(s^i)}) \wedge (\forall b \bigwedge_{\overline{l},\overline{k}} \prod_i (b^{k_i})^{t^{l_i}} \neq a).$$

The only difference is that we will also allow $\overline{k}$ to have only one nonzero entry which is not ±1, in addition to $\overline{k}$'s which have at least two nonzero entries. This is to rule out the case where a is a power of the standard generator.

For completeness, we will construct

$$G_n \cong \begin{cases} \hat{L}, & n \notin S_1 \\ L, & n \in S_1 \setminus S_2 \\ \mathbb{Z} \wr \mathbb{Z}^2, & n \in S_1 \cap S_2. \end{cases}$$

□

Remark 4.21. *In fact, this theorem can be generalized to $\mathbb{Z}^n \wr \mathbb{Z}^m$. However, we will omit the proof in the interest of space. We have to add into $\phi(\overline{a}, \overline{t})$ extra conjuncts to make sure that $\overline{a}$ generates a copy of $\mathbb{Z}^n$ and $\overline{t}$ generates $\mathbb{Z}^m$ modulo the base group, and the extra conjuncts are similar to what we did in the polycyclic case (Theorem 4.12). In proving completeness, we use the direct limit and $\mathbb{Z}^n \wr \mathbb{Z}^{(m+1)}$ as the alternate structures.*

We now look at another class of groups, the Baumslag–Solitar groups, which are very closely related to the lamplighter groups. Indeed, in [37], it was shown that $BS(1,n)$ converges to $\mathbb{Z} \wr \mathbb{Z}$ as $n \to \infty$. We shall see great similarity in the arguments used for these groups also.

Definition 4.22. *The* Baumslag–Solitar groups $BS(m,n)$ *are two-generator one-relator groups given by the presentation:*

$$BS(m,n) = \langle\, a, b \mid ba^m b^{-1} = a^n \,\rangle$$

Note that $BS(m,n) \cong BS(n,m)$.

Theorem 4.23. *$BS(m,n)$ is solvable if and only if $|m| = 1$ or $|n| = 1$, in which case it is also not polycyclic and its derived length is 2.*

Theorem 4.24. *For each n, the solvable Baumslag–Solitar group $BS(1,n)$ has a computable d-Σ_2 Scott sentence. Furthermore, its index set is m-complete d-Σ_2 for every n.*

Proof. $BS(1,n)$ has the semidirect product structure $B \rtimes \mathbb{Z}$ where $B = \mathbb{Z}[\frac{1}{n}, \frac{1}{n^2}, \dots] = \{\dfrac{x}{y} : y|n^k \text{ for some } k\}$, and the action of $1 \in \mathbb{Z}$ on B is by multiplication by n. Again we are abusing notation by writing $BS(1,n)$ multiplicatively but B additively.

For finding the Scott sentence, we consider the formula

$$\phi(a,t) \equiv (\langle a,t\rangle \cong BS(1,n)) \wedge (\forall b \bigwedge_{\gcd(i,n)=1} b^i \neq a).$$

This is not empty because the standard generators $(1,0)$, $(0,1) \in B \rtimes \mathbb{Z}$ satisfy it.

For a tuple (a,t) satisfying ϕ, the first conjunct guarantees that a is in the base group and t, as an element of the original Baumslag–Solitar group $BS(1,n) = B \rtimes \mathbb{Z}$, has the $\mathbb{Z}$ coordinate being 1 in the semidirect product, because of the inclusion of the formula $tat^{-1} = a^d$. The second conjunct guarantees that the B coordinate of a is $\frac{x}{y}$ for some x and y both dividing some power of n. Thus appropriately conjugating a by t, we see $\frac{1}{y'} \in \langle a,t\rangle$ for some y', thus $1 \in \langle a,t\rangle$, and hence a and t generate the whole group. By the Generating Set Lemma (Lemma 4.11), we obtain a computable d-Σ_2 Scott sentence for $BS(1,n)$.

To show completeness, we first observe $BS(1,n)$ is not co-Hopfian. Indeed, let p be a prime not dividing n, then consider the endomorphism sending a to a^p and fixing b. This is injective but not surjective because, for instance, it misses the element 1 in B.

Thus, we construct

$$G_n \cong \begin{cases} \widehat{BS(1,n)}, & n \notin S_1 \\ BS(1,n), & n \in S_1 \setminus S_2 \\ (B^{\mathbb{Z}}) \rtimes (\mathbb{Z}^2), & n \in S_1 \cap S_2, \end{cases}$$

where in $(B^{\mathbb{Z}}) \rtimes (\mathbb{Z}^2)$, $B^{\mathbb{Z}}$ is the direct sum of countably many copies of B, indexed by $\mathbb{Z}$, and the action of the first coordinate of $\mathbb{Z}^2$ is by multiplying by n (to each coordinate), and the action of the second coordinate is by shifting the copies of B. The same argument as above will show this construction gives d-Σ_2 completeness of $I(BS(1,n))$. □

4.4 Infinitely-generated free nilpotent groups

We will now turn our attention to infinitely-generated groups. In this section, we start with a natural continuation of Section 2, showing that the infinitely-generated free nilpotent groups $N_{p,\infty}$ have a computable Π_3 Scott sentence, and their index sets are m-complete Π_3. We start by stating the following result for $p = 1$:

Theorem 4.25 ([7])**.** *The infinitely-generated free abelian group $\mathbb{Z}^\omega$ has a computable Π_3 Scott sentence. Furthermore, $I(\mathbb{Z}^\omega)$ is m-complete Π_3.*

To find a computable Scott sentence for the infinitely-generated free nilpotent group, we give a lemma analogous to the Generating Set Lemma (Lemma 4.11).

Lemma 4.26 (Infinite Generating Set Lemma)**.** *Suppose $G \cong \langle a_1, a_2, \dots \mid R \rangle$, where R is a normal subgroup of F_ω. Let R_i be $R \cap F_{a_1,\dots,a_i} \subset F_\omega$. If there are $\langle \gamma_k \rangle_{k\in\omega}$ such that*

1. *$\gamma_k(\overline{x})$ implies $\langle \overline{x} \rangle \cong \langle a_1, a_2, \dots, a_k \mid R_k \rangle$ modulo the theory of groups.*

2. *$G \models \exists x_1 \; \gamma_1(x_1)$.*

3. *$G \models \bigwedge_k (\forall x_1, \dots, x_k [\gamma_k(x_1, \dots, x_k) \to \forall y \bigvee_{l \geq k+1} \exists x_{k+1}, \dots, x_l \; \gamma_l(x_1, \dots, x_l) \wedge z \in \langle x_1, \dots, x_l \rangle])$ (“Every $\gamma_k(\overline{x})$ can be ‘extended’ ”. In a countable group, this implies $\overline{x}$ can be extended to a basis.)*

Then ϕ, the conjunction of the group axioms and the sentences (2) and (3), is a Scott sentence of G.

Proof. By assumption, G models ϕ. Let H be a countable group modeling ϕ. We first choose x_1 by (2). Note that (3) allows us to extend any $\overline{x}$ satisfying γ_k to generate any element in the group H. Thus, we enumerate H, and iteratively extend $\overline{x}$ to generate the whole group H. If we consider the relations that hold on the infinite limiting sequence $\overline{x}$, the relation on $x_1, \dots, x_k$ is exactly R_k by (1), thus the group $H = \langle \overline{x} \rangle \cong \langle \overline{a} \mid R \rangle = G$. □

Corollary 4.27. *$N_{p,\infty}$ has a computable Π_3 Scott sentence.*

Proof. Let $\gamma_k(\overline{y}) \equiv (\langle \overline{y} \rangle \cong N_{p,k}) \wedge (\forall \overline{z} \bigwedge_{\det(M) \neq \pm 1} M\overline{z} \mathrel{\hat{\neq}} \overline{y})$, where in the second conjunct the inequality is relativized (as in the polycyclic case, Theorem 4.12) to the abelianization H/H' and we are abusing notation and thinking of the abelianization additively. So for $M\overline{z}$ we mean matrix multiplication, thinking of each z_i as a row vector.

To show the γ_k's satisfy the extendibility condition, fix $\overline{x}$ satisfying γ_k. Working in the abelianization, after truncating the columns in which $\overline{x}$ has no nonzero entries , we write $\overline{x}$ in its Smith normal form, i.e. find invertible $k \times k$ and $n \times n$ matrices S and T such that $S\overline{x}T$ has all but the (i,i)-th entries being zero. The second conjunct of γ_k guarantees that all the (i,i)-th entries are actually 1. Thus, $\overline{x}$ can be extended to a basis of $\mathbb{Z}^\infty = \mathrm{ab}(N_{p,\infty})$. By a theorem of Magnus ([25, Lemma 5.9]), this implies that $\overline{x}$ can be extended to a basis of $N_{p,\infty}$, thus satisfying the extendibility condition.

The γ_k's are Π_1, and a direct counting shows that the Scott sentence we obtain from the previous lemma is Π_3. □

For completeness of the index set of $N_{p,\infty}$, we generalize the technique from the abelian case, but we will need the following group-theoretic lemma.

Lemma 4.28 (Nilpotent residual property)**.** *For $n, m \geq p$, $N_{p,n}$ is fully residually-$N_{p,m}$. I.e., for every finite subset $S \subset N_{p,n}$, there exists a homomorphism $\phi : N_{p,n} \to N_{p,m}$ such that ϕ is injective on S.*

Proof. Baumslag, Myasnikov, and Remeslennikov in [3] showed that any group universally equivalent to (i.e., having the same first-order universal theory as) a free nilpotent group $N_{p,m}$ is fully residually-$N_{p,m}$. Timoshenko in [38] showed that $N_{p,n}$ and $N_{p,m}$ are universally equivalent for $n, m \geq p$. Combining these two results, we prove the desired lemma. □

Corollary 4.29. *$I(N_{p,\infty})$ is m-complete Π_3 for every p.*

Proof. Recall that COF, the index set of all cofinite c.e. sets, is m-complete Σ_3. We will reduce the complement of COF to $I(N_{p,\infty})$.

We construct G_n uniformly in n. We first fix an infinite set of generators $a_0, a_1, \ldots$ and p distinguished generators $b_0, b_1, \ldots, b_p$ distinct from the a_i's, and we start the construction by constructing $\bar{b}$. At a finite stage, if we see some natural number k being enumerated into W_n, we collapse a_k by taking the subgroup $N_{p,m} \subset N_{p,\infty}$ generated by all the generators that have been mentioned so far. Having the $\bar{b}$ means $m > p$, so by the nilpotent residual property (Lemma 4.28), we can embed what we have constructed so far into $N_{p,m-1}$ with the same generators except a_k.

Thus, in the limit, if $n \in \mathrm{COF}$, then we will collapse all but finitely many a_i's, hence the limiting group will be a finitely-generated (free) nilpotent group not isomorphic to $N_{p,\infty}$; and if $n \notin \mathrm{COF}$, we will still have infinitely many of the a_i's, and the limiting group will be isomorphic to $N_{p,\infty}$. This shows $I(N_{p,\infty})$ is m-complete Π_3. □

Remark 4.30. *In the corollary, one actually can prove that $I(N_{p,\infty})$ is m-complete Π_3 within the class of free nilpotent groups. The interested reader can compare this to the same result for infinitely-generated free abelian groups in [7].*

4.5 A subgroup of $\mathbb{Q}$

In this section, we will look at a special subgroup of $\mathbb{Q}$. Knight and Saraph [22, §3] considered subgroups of $\mathbb{Q}$, distinguishing between cases by looking at the following invariants.

Definition 4.31. *We write P for the set of primes. Let G be a computable subgroup of $\mathbb{Q}$. Without loss of generality, we will assume $1 \in G$; otherwise, we can take a subgroup of $\mathbb{Q}$ isomorphic to G containing 1. We define:*

1. $P^0(G) = \{p \in P : G \vDash p \nmid 1\}$
2. $P^{fin}(G) = \{p \in P : G \vDash p|1$ *and* $p^k \nmid 1$ *for some* $k\}$
3. $P^\infty(G) = \{p \in P : G \vDash p^k|1$ *for all* $k\}$

Remark 4.32. 1. *Define $P^k(G) = \{p \in P : G \vDash p^k|1$ and $p^{k+1} \nmid 1\}$. Then two subgroups G, H of $\mathbb{Q}$ are isomorphic if and only if $P^k(G) =^* P^k(H)$ for every k, with equalities holding on cofinitely many of k, and $P^\infty(G) = P^\infty(H)$. $S =^* T$ means S and T only differ by finitely many elements.*

2. *Since G is computable, P^0 is Π_1, $P^{\mathit{fin}} \cup P^\infty$ is Σ_1, P^{fin} is Σ_2, and P^∞ is Π_2.*

Dividing the subgroups of $\mathbb{Q}$ into cases by these invariants, Knight and Saraph determined the upper and lower bound of complexities of Scott sentences and the index sets in some cases. The case we consider here is when P^0 is infinite, P^{fin} is finite (and thus, without loss of generality, empty), and P^∞ is infinite. This is case 5 in [22], and they have the following results:

Theorem 4.33 ([22]). *Let G be a computable subgroup of $\mathbb{Q}$ with $|P^0| = \infty$, $P^{\mathit{fin}} = \varnothing$, and $|P^\infty| = \infty$. Then*

1. *G has a computable Σ_3 Scott sentence.*

2. *$I(G)$ is d-Σ_2-hard.*

3. *If P^∞ is low, then $I(G)$ is d-Σ_2.*

4. *If P^∞ is not high$_2$, then $I(G)$ is not m-complete Σ_3.*

It was not known that if there is a subgroup of $\mathbb{Q}$ as in the theorem that has m-complete Σ_3 index set, thus achieving the upper bound in (1). In Proposition 4.35, we shall give such an example.

Also, the following theorem shows that such a group does not have a computable d-Σ_2 Scott sentence unless P^0 is computable.

Theorem 4.34 ([21]). *Let G be a computable subgroup of $\mathbb{Q}$ with $|P^0| = \infty$, $P^{\mathit{fin}} = \varnothing$, and $|P^\infty| = \infty$, and suppose P^∞ is not computable. Then G does not have a computable d-Σ_2 Scott sentence.*

Thus, when P^∞ is low but not computable, this gives a negative answer to the conjecture that the complexity of the index set should equal to the complexity an optimal Scott sentence. Continuing in this direction, we give an example of a subgroup in this case where the two complexities do equal each other, and are both Σ_3.

Proposition 4.35. *Let K be the halting set. Let $G \subseteq \mathbb{Q}$ be a subgroup such that $1 \in G$, $P^\infty(G) = \{p_n \in P \mid n \in K\}$, and $P^{fin}(G) = \varnothing$. Then $I(G)$ is m-complete Σ_3.*

Proof. Fix n. We construct G_n so that $G_n \cong G$ if and only if $n \in \mathrm{COF}$.

For every s, we can recursively find the index $k_s = e$ of a program such that

$$\phi_e(e) = \begin{cases} \downarrow, & \text{if } \phi_n(s)\downarrow \\ \uparrow, & \text{if } \phi_n(s)\uparrow . \end{cases}$$

Now we construct G_n by making $p_{k_s}|1$ for every k_s. We also make p_i divide every element if we see $i \in K$.

Now we verify $G_n \cong G$ if and only if $n \in \mathrm{COF}$. We first observe that $P^\infty(G_n) = \{p_i \mid i \in K\}$. It's also clear from construction that $P^{\mathrm{fin}}(G_n) = \{p_{k_s} \mid k_s \notin K\}$. But $k_s \in K$ if and only if $\phi_n(s)\downarrow$, thus $P^{\mathrm{fin}}(G) = \{p_{k_s} \mid \phi_n(s)\uparrow\}$.

Now, $P^\infty(G_n) = \{p_i \mid i \in K\} = P^\infty(G)$. Thus $G_n \cong G$ iff $P^{\mathrm{fin}}(G_n) =^* P^{\mathrm{fin}}(G) = \varnothing$ iff $P^{\mathrm{fin}}(G_n) = \{p_{k_s} \mid \phi_n(s)\uparrow\}$ is finite iff $n \in \mathrm{COF}$. □

Remark 4.36. *Note that this argument works for any $X \equiv_m K$. It is natural to then ask that whether we can find a Turing-degree based characterization of when the index set will be m-complete Σ_3. In the next section, we will show this cannot be found.*

4.6 Complexity hierarchy of pseudo-Scott sentences

In this section, we continue looking at subgroups of $\mathbb{Q}$ as above. We first give the definition of a pseudo-Scott sentence, which, just like a Scott sentence, identifies a structure, but only among the computable structures. Note that every computable Scott sentence is a pseudo-Scott sentence.

Definition 4.37. *A* pseudo-Scott sentence *for a structure $\mathcal{A}$ is a sentence in $\mathcal{L}_{\omega_1,\omega}$ whose computable models are exactly the computable isomorphic copies of $\mathcal{A}$.*

Similar to the case of computable Scott sentences, a pseudo-Scott sentence of a structure yields a bound on the complexity of the index set of the structure.

We shall give an example of a group which has a computable Σ_3 pseudo-Scott sentence and a computable Π_3 pseudo-Scott sentence, but no computable d-Σ_2 pseudo-Scott sentence. This is related to a question about the effective Borel hierarchy in $\mathrm{Mod}(\mathcal{L})$.

Consider the complexity hierarchy of (computable pseudo-)Scott sentences. Since $\alpha \smallsetminus (\beta \smallsetminus \gamma) = (\alpha \wedge \neg\beta) \vee (\alpha \wedge \gamma)$, we see that the hierarchy collapses in the sense that the complexity classes k-Σ_n are all the same for $k \geq 2$.

One open question is whether the complexity classes Δ_{n+1} and d-Σ_n are the same or not for regular, computable, and pseudo-Scott sentences. The complexity hierarchy of Scott sentences (computable Scott sentences, respectively) is related to the boldface (effective, respectively) Borel hierarchy on the space $\mathrm{Mod}(\mathcal{L})$, see [40] and [39]. In [26], it was shown that $\boldsymbol{\Delta}_{n+1}$ and d-$\boldsymbol{\Sigma}_n$ are the same in the boldface case, i.e. if a structure has a Σ_{n+1} Scott sentence and a Π_{n+1} Scott sentence, then it also has a d-Σ_n Scott sentence. This gives a positive answer to the question for Scott sentences. However, we will prove that this is not true in the complexity hierarchy of computable pseudo-Scott sentences by giving a subgroup $G \subset \mathbb{Q}$ which has a computable Σ_3 pseudo-Scott sentence and a computable Π_3 pseudo-Scott sentence, but no computable d-Σ_2 pseudo-Scott sentence. This gives a negative answer to the question for pseudo-Scott sentences. The question of whether Δ_{n+1} and d-Σ_n are the same in the effective case (the complexity hierarchy of computable Scott sentence) remains open.

We start by strengthening a result in [21]. The first part of the proof where we construct the theory T is unchanged.

Lemma 4.38. *Fix a non-computable c.e. set X, and let $G \subset \mathbb{Q}$ be a subgroup such that $1 \in G$, $P^\infty(G) = \{p_i \mid i \in X\}$, and $P^{fin}(G) = \varnothing$. Then G does not have a computable d-Σ_2 pseudo-Scott sentence.*

Proof. Suppose G has a computable d-Σ_2 pseudo-Scott sentence $\phi \wedge \psi$, where ϕ is computable Π_2 and ψ is computable Σ_2. Let α be a computable Π_2 sentence characterizing the torsion-free abelian groups A of rank 1 such that $P^\infty(A) \subseteq X$. By [21, Lemma 2.3], $\alpha \vdash \phi$, thus we can replace ϕ by α in the pseudo-Scott sentence.

Also, again by [21], we can assume ψ has the form $\exists x\ \chi(x)$ where x is a singleton and $\chi(x)$ is a c.e. conjunction of finitary Π_1 formulas.

Now, we consider an elementary first-order theory T, in the extension of the language $\mathcal{L}$ by an extra constant symbol c, where T is generated by the following sentences:

1. axioms of torsion-free abelian groups,
2. $\forall x \exists y\ py = x$ for each $p \in X$,
3. $\rho_i(c)$ for every finitary Π_1 conjunct $\rho_i(x)$ of the Π_1 sentence $\chi(x)$.

Now we show that [21, Lemma 2.4] is still true:

Claim 4.39. *For every $i \notin X$, there is some k such that $T \vdash p_i^k \nmid c$.*

Proof of claim. Suppose this is not true. There is $n \notin X$ such that $T \cup \{p_n^k | c \ : k \geq 1\}$ is consistent. Take a model H of $T \cup \{p_n^k | c : k \geq 1\}$, and let $C \subset H$ be the subgroup consisting of rational multiples of c.

Let $K \subset \mathbb{Q}$ be the computable group with $1 \in K$, $P^{\infty}(K) = \{p_i \mid i \in X\} \cup \{p_n\}$, and $P^{\text{fin}}(K) = \varnothing$. Then K is isomorphic to a subgroup of C. By interpreting the constant symbol c in K as the preimage of $c \in C$, K is a substructure of H. Thus all the finitary Π_1 statements $\rho_i(c)$ are also true in K.

So, K is a torsion-free rank 1 abelian group satisfying T, thus $K \vDash \phi \wedge \psi$. Since K is computable, it is isomorphic to G, but $P^{\infty}(G) \neq P^{\infty}(K)$, a contradiction. □

Now we have a computable theory T such that for every $i \notin X$, there is some k such that $T \vdash p_i^k \nmid c$. Therefore, the complement of X is c.e., and this contradicts the assumption that X is non-computable c.e. □

We also need the following lemma:

Lemma 4.40. *There exists a c.e. set $X \subseteq \omega$ with $X \equiv_T 0'$ satisfying the following: There is a uniformly c.e. sequence S_n so that if $W_n \supset X$, $W_n \neq^* X$, then S_n is an infinite c.e. subset of $W_n \smallsetminus X$.*

Proof. Write $I_i = [\frac{i(i+1)}{2}, \frac{(i+1)(i+2)}{2})$. Note that the interval $|I_i|$ has length $i+1$. Consider the following requirements:

- R_i: $X \cap I_i \neq \varnothing$ if and only if $i \in 0'$
- Q_k: build an infinite c.e. $S_k \subset W_k \smallsetminus X$ if $W_k \supset X$ and $W_k \neq^* X$

If at some stage R_i sees $i \in 0'$, then it puts some element of I_i that is not yet blocked by higher priority Q_k's into X.

Q_k will attempt to put n into S_k whenever $n \in W_k \setminus X$ at stage s. Suppose $n \in I_i$. If $i < k$, then Q_k does nothing. If $i > k$, then Q_k puts n into S_k, and blocks R_i from enumerating n into X, but Q_k will also block itself from enumerating other elements of I_i into S_k.

Note that for each R_i, at most i elements of I_i will be blocked, because for each I_i, every higher priority Q_k will block at most one element. Thus R_i can always satisfy the requirement.

Also, if $W_k \supset X$ and $W_k \neq^* X$, then Q_k will eventually enumerate infinitely many numbers into S_k, since after enumerating finitely many of them, there are only finitely many things blocked by Q_k itself and finitely many higher priority R_i's. Lastly, S_k will be disjoint from X because whenever n is enumerated into S_k, the R_i's will be blocked from enumerating it into X. □

Theorem 4.41. *There exists a group with both computable Σ_3 and computable Π_3 pseudo-Scott sentences (i.e. Δ_3), but no computable d-Σ_2 pseudo-Scott sentence.*

Proof. Choose X as in the previous lemma. Consider the subgroup $G \subset \mathbb{Q}$ with $P^{\text{fin}}(G) = \varnothing$ and $P^{\infty}(G) = X$. By [21], G has a computable Σ_3 (pseudo-)Scott sentence. By Lemma 4.38, G does not have a computable d-Σ_2 pseudo-Scott sentence.

Let ϕ be the conjunction of $\bigwedge\limits_{S_k} \exists g \bigwedge\limits_{p \in S_k} p \nmid g$, "$G$ is a subgroup of Q", and "$P^{\infty}(G) \supseteq X$".

Say $H \vDash \phi$ is a computable group. Then $P^{\infty}(H) \cup P^{\text{fin}}(H)$ is c.e., so let n be such that $W_n = P^{\infty}(H) \cup P^{\text{fin}}(H)$. Note that $W_n \supset X$. If $H \ncong G$, then $W_n \neq^* X$. Now consider $S_n \subset Y \setminus X$, and the corresponding conjunct in ϕ which says $\exists g \bigwedge\limits_{p \in S_Y} p \nmid g$. But every element in H is divisible by all but finitely many elements from W_n, and S_n is an infinite subset of W_n, so H cannot model this existential sentence, a contradiction. Thus ϕ is a computable Π_3 pseudo-Scott sentence of G_X. □

Remark 4.42. *Note that in the first countable conjunction, the set of indices of S_Y for $Y \supset X$ and $Y \neq^* X$ is not c.e. However, the set of indices of S_Y for all $Y \subset \omega$ is c.e., even computable, by construction, and G_X still models ϕ for this bigger conjunction.*

Note that the two groups in Proposition 4.35 and Theorem 4.41 both have $P^{\text{fin}} = \varnothing$ and $P^\infty \equiv_T 0'$. However, one of them has index set being m-complete Σ_3, while the other has index set being Δ_3. This tells us that we cannot hope to give a Turing-degree based characterization of which combinations of P^0, P^{fin}, and P^∞ give m-complete Σ_3 index sets and which do not.

Chapter 5

Addendum: Normal Closures in Nilpotent Groups

We include in this addendum a lemma, which was proved when the author was studying random nilpotent groups, but ended up not being used there.

Magnus proved that two elements a and b of a free group have the same normal closure if and only if a is conjugate to b or b^{-1} [24, Chapter II, Proposition 5.8]. In [14], Endimioni gave an analog of Magnus' theorem for a nilpotent metabelian group. Here, we give a generalization of Endimioni's result for any nilpotent group.

First we fix some notations. We will write the commutator as $[x,y] = xyx^{-1}y^{-1}$, conjugates as $x^y = yxy^{-1}$, and thus we have the identity $[xy,z] = [y,z]^x[x,z]$. For a group G, we write $G_1 = G$ and $G_{k+1} = [G_k, G]$, and call $G_1 \supseteq G_2 \supseteq \dots$ the *lower central series* of G.

For a subset S of a group G, we write $\langle S\rangle$ to be the subgroup generated by S in G, and $\langle\langle S\rangle\rangle$ to be the normal subgroup generated by S in G. For an element $g \in G$, we define *[g,G]* $= \langle\{[g,x] | x \in G\}\rangle$. Note that $[g,G]$ is normal by the identity $[g,h]^k = [g,k]^{-1}[g,kh]$.

Lemma 5.1. *Let $g \in G$. If $h \in [g,G]$, then there exists an $\ell \in [h,G]$ such that $\ell h \in [gh,G]$.*

Proof. Since $h \in [g, G]$, we can write $h = \prod_i [g, x_i]^{\epsilon_i}$, where $x_i \in G$, and $\epsilon_i = \pm 1$. Let $\ell = (\prod_i [gh, x_i]^{\epsilon_i})h^{-1}$, so we have $\ell h \in [gh, G]$. Now we compute (modulo $[h, G]$):

$$\ell = (\prod_i [gh, x_i]^{\epsilon_i})h^{-1} = (\prod_i ([h, x_i]^g [g, x_i])^{\epsilon_i})h^{-1} = (\prod_i [g, x_i]^{\epsilon_i})h^{-1} = 1$$

Thus, $\ell \in [h, G]$. □

Lemma 5.2. *Let g, k be two elements of a nilpotent group N of class r. If $k^{-1}g \in [g, G]$, then $\langle\langle g \rangle\rangle = \langle\langle k \rangle\rangle$.*

Proof. First, we have $k^{-1} = k^{-1}g \cdot g^{-1} \in \langle\langle g \rangle\rangle$, so $\langle\langle g \rangle\rangle \supseteq \langle\langle k^{-1} \rangle\rangle = \langle\langle k \rangle\rangle$. We then need to show $\langle\langle k \rangle\rangle \supseteq \langle\langle g \rangle\rangle$.

Let $n \leq r + 1$ be the largest number such that $k^{-1}g \in N_n$. We induct on n.

When $n = r + 1$, $g = k$ and thus $\langle\langle g \rangle\rangle = \langle\langle k \rangle\rangle$.

For $n \leq r$, using the previous lemma with $h = g^{-1}k \in [g, G]$, we obtain an $\ell \in [h, G]$ such that $\ell h \in [gh, G] = [k, G] \subseteq \langle\langle k \rangle\rangle$. Now $\langle\langle k \rangle\rangle = \langle\langle gh \rangle\rangle \supseteq \langle\langle (gh)(\ell h)^{-1} \rangle\rangle = \langle\langle g\ell^{-1} \rangle\rangle$. Write $k' = g\ell^{-1}$, we have $(k')^{-1}g = \ell \in [h, G] \subset \langle\langle h \rangle\rangle \subseteq [g, G]$, and $(k')^{-1}g = \ell \in [h, G] \subseteq N_{n+1}$. Thus by induction, $\langle\langle g\ell^{-1} \rangle\rangle = \langle\langle k' \rangle\rangle = \langle\langle g \rangle\rangle$. It follows that $\langle\langle k \rangle\rangle \supseteq \langle\langle g\ell^{-1} \rangle\rangle = \langle\langle g \rangle\rangle$, which completes the proof. □

Theorem 5.3. *Let g, k be elements of a nilpotent group N. Then the following are equivalent:*

1. $\langle\langle g \rangle\rangle = \langle\langle k \rangle\rangle$

2. *There is an integer μ such that $k^{-\mu}g \in [g, G]$ where μ is coprime to the order of k if k is of finite order, and $\mu = \pm 1$ otherwise.*

Proof. Suppose that $\langle\!\langle g\rangle\!\rangle = \langle\!\langle k\rangle\!\rangle$. Then $[g, G] = [\langle\!\langle g\rangle\!\rangle, G] = [\langle\!\langle k\rangle\!\rangle, G] = [k, G]$. Since $\langle\!\langle g\rangle\!\rangle/[g, G]$ and $\langle\!\langle h\rangle\!\rangle/[g, G]$ are both cyclic, we have $g = k^{\mu}$ and $k = g^{\lambda}$ mod $[g, G]$ for some integers μ and λ. In particular, we have $k^{-\mu}g \in [g, G]$. We also have $k^{\mu\lambda-1} \in [g, G]$. So by [14, Lemma 3.2], $k^{(\mu\lambda-1)^m} = 1$ for some m. Thus μ is coprime to the order of k if k is of finite order, and $\mu = \pm 1$ otherwise.

Now suppose that $k^{-\mu}g \in [g, G]$ with μ being either coprime to the order of k and k is of finite order, or ± 1. In any case, we can find an integer s such that $k^{\mu s} = k^{-1}$, and hence $\langle\!\langle k^{\mu}\rangle\!\rangle = \langle\!\langle k^{-1}\rangle\!\rangle$. Now by applying the previous lemma with $k' = k^{\mu}$, we have $\langle\!\langle g\rangle\!\rangle = \langle\!\langle k^{\mu}\rangle\!\rangle = \langle\!\langle k\rangle\!\rangle$, and the theorem follows. □

Bibliography

[1] C. J. Ash and J. Knight, *Computable structures and the hyperarithmetical hierarchy*, vol. 144 of Studies in Logic and the Foundations of Mathematics, North-Holland Publishing Co., Amsterdam, 2000.

[2] B. Baumslag, *Residually free groups*, Proc. London Math. Soc. (3), 17 (1967), pp. 402–418.

[3] G. Baumslag, A. Myasnikov, and V. Remeslennikov, *Algebraic geometry over groups. I. Algebraic sets and ideal theory*, J. Algebra, 219 (1999), pp. 16–79.

[4] I. Belegradek, *On co-Hopfian nilpotent groups*, Bull. London Math. Soc., 35 (2003), pp. 805–811.

[5] E. Breuillard, *Random walks on lie groups*. `http://www.math.u-psud.fr/~breuilla/part0gb.pdf`.

[6] M. R. Bridson and A. Haefliger, *Metric spaces of non-positive curvature*, vol. 319 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 1999.

[7] W. Calvert, V. S. Harizanov, J. F. Knight, and S. Miller, *Index sets of computable models*, Algebra Logika, 45 (2006), pp. 538–574, 631–632.

[8] J. Carson, V. Harizanov, J. Knight, K. Lange, C. McCoy, A. Morozov, S. Quinn, C. Safranski, and J. Wallbaum, *Describing free groups*, Trans. Amer. Math. Soc., 364 (2012), pp. 5715–5728.

[9] P.-A. Cherix and G. Schaeffer, *An asymptotic Freiheitssatz for finitely generated groups*, Enseign. Math. (2), 44 (1998), pp. 9–22.

[10] P. Diaconis, *Group representations in probability and statistics*, Institute of Mathematical Statistics Lecture Notes—Monograph Series, 11, Institute of Mathematical Statistics, Hayward, CA, 1988.

[11] Drutu and Kapovich, *Lectures on geometric group theory.* Preprint.

[12] M. Duchin, K. Jankiewicz, S. Kilmer, S. Lelièvre, J. Mackay, and A. Sánchez, *A sharper threshold for random groups at density one-half*, Groups, Geometry, and Dynamics. to appear.

[13] N. M. Dunfield and W. P. Thurston, *Finite covers of random 3-manifolds*, Invent. Math., 166 (2006), pp. 457–521.

[14] G. Endimioni, *Elements with the same normal closure in a metabelian group*, Q. J. Math., 58 (2007), pp. 23–29.

[15] R. Fitzner and R. van der Hofstad, *Non-backtracking random walk*, J. Stat. Phys., 150 (2013), pp. 264–284.

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

[17] M. Hall, Jr., *The theory of groups*, Chelsea Publishing Co., New York, 1976. Reprinting of the 1968 edition.

[18] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, sixth ed., 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[19] O. Kharlampovich and A. Myasnikov, *Elementary theory of free non-abelian groups*, J. Algebra, 302 (2006), pp. 451–552.

[20] O. G. Kharlampovich, *A finitely presented solvable group with unsolvable word problem*, Izv. Akad. Nauk SSSR Ser. Mat., 45 (1981), pp. 852–873, 928.

[21] J. F. Knight and C. McCoy, *Index sets and Scott sentences*, Arch. Math. Logic, 53 (2014), pp. 519–524.

[22] J. F. Knight and V. Saraph, *Scott sentences for certain groups.*

[23] R. V. Kravchenko, M. Mazur, and B. V. Petrenko, *On the smallest number of generators and the probability of generating an algebra*, Algebra Number Theory, 6 (2012), pp. 243–291.

[24] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin, 1977. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89.

[25] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*, Dover Publications Inc., Mineola, NY, second ed., 2004. Presentations of groups in terms of generators and relations.

[26] D. E. Miller, *The invariant π^0_α separation principle*, Trans. Amer. Math. Soc., 242 (1978), pp. 185–204.

[27] J. Nielsen, *Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden*, Math. Ann., 78 (1917), pp. 385–397.

[28] Y. Ollivier, *A January 2005 invitation to random groups*, vol. 10 of Ensaios Matemáticos [Mathematical Surveys], Sociedade Brasileira de Matemática, Rio de Janeiro, 2005.

[29] M. O. Rabin, *Computable algebra, general theory and theory of computable fields.*, Trans. Amer. Math. Soc., 95 (1960), pp. 341–360.

[30] D. J. S. Robinson, *A course in the theory of groups*, vol. 80 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 1996.

[31] N. Romanovskii, *A freedom theorem for groups with one defining relation in the varieties of solvable and nilpotent groups on given lengths*, Math. USSR-Sb., 18 (1972), pp. 93–99. (English translation.).

[32] D. Scott, *Logic with denumerably long formulas and finite strings of quantifiers*, in Theory of Models (Proc. 1963 Internat. Sympos. Berkeley), North-Holland, Amsterdam, 1965, pp. 329–341.

[33] Z. Sela, *Diophantine geometry over groups. I. Makanin-Razborov diagrams*, Publ. Math. Inst. Hautes Études Sci., (2001), pp. 31–105.

[34] Z. Sela, *Diophantine geometry over groups. VI. The elementary theory of a free group*, Geom. Funct. Anal., 16 (2006), pp. 707–730.

[35] ——, *Diophantine geometry over groups VIII: Stability*, Ann. of Math. (2), 177 (2013), pp. 787–868.

[36] C. C. Sims, *Computation with finitely presented groups*, vol. 48 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1994.

[37] Y. Stalder, *Convergence of Baumslag-Solitar groups*, Bull. Belg. Math. Soc. Simon Stevin, 13 (2006), pp. 221–233.

[38] E. I. Timoshenko, *On universally equivalent solvable groups*, Algebra Log., 39 (2000), pp. 227–240, 245.

[39] M. Vanden Boom, *The effective Borel hierarchy*, Fund. Math., 195 (2007), pp. 269–289.

[40] R. Vaught, *Invariant sets in topology and logic*, Fund. Math., 82 (1974/75), pp. 269–294. Collection of articles dedicated to Andrzej Mostowski on his sixtieth birthday, VII.

[41] Y. Wang and R. P. Stanley, *The smith normal form distribution of a random integer matrix*. `http://front.math.ucdavis.edu/1506.00160`.

[42] M. M. Wood, *Random integral matrices and the Cohen Lenstra Heuristics*. `http://front.math.ucdavis.edu/1504.04391`.