RANDOM NILPOTENT GROUPS I

MATTHEW CORDES, MOON DUCHIN, YEN DUONG, MENG-CHE HO,
AND ANDREW P. SÁNCHEZ

Abstract. We study random nilpotent groups in the well-established style of random groups, by choosing relators uniformly among freely reduced words of (nearly) equal length and letting the length tend to infinity. Whereas random groups $\Gamma = F_m/\langle\langle R\rangle\rangle$ are quotients of a free group by such a random set of relators, *random nilpotent groups* are formed as corresponding quotients $G = N_{s,m}/\langle\langle R\rangle\rangle$ of a free nilpotent group.

We establish results about the distribution of ranks for random nilpotent groups, and about the distribution of group orders for some finite-order cases. We also study the probabilities of obtaining an abelian or a cyclic group. For example, for balanced presentations (number of relators equal to number of generators), the probability that a random nilpotent group is abelian can be calculated for each rank m, and approaches 84.69...% as $m \to \infty$. Further, up to probability, abelian implies cyclic in this setting.

We find the precise vanishing threshold for random nilpotent groups—the analog of the famous density one-half theorem for random groups—by studying the abelianization. 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. Finally, we describe how to lift results about random nilpotent groups to obtain more general information about the lower central series of standard random groups.

1. Introduction and background

1.1. **Random groups.** The background idea for the paper 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 stating that for $d > 1/2$, 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. (In the rest of this paper, we will choose our relators from those of length ℓ and $\ell - 1$ with probability $\frac{1}{2}$ and $\frac{1}{2}$ in order to avoid the parity issue.)

That is, the threshold for trivializing a free group is to choose roughly the *square root* of the available number of relators, a number that grows exponentially in relator length. Because the threshold for vanishing coincides with the threshold for hyperbolicity, this means one never sees other kinds of groups, for example abelian groups, in this model. To be precise, all finitely-generated groups are quotients of F_m, but probability of getting any nontrivial, non-hyperbolic group is zero. (Furthermore the recent paper [4] shows that this 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. In this paper we begin a study of random nilpotent groups by adding random relators to the free nilpotent groups $N_{s,m}$ of step s and rank m; all nilpotent groups occur as quotients of these. Then we can try to characterize 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 paper are summarized as follows:

- 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. (§3)
- Using a Freiheitssatz for nilpotent groups, we study the consequences of rank drop, and conclude that abelian groups occur with probability zero for $|R| \le m - 2$, though 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. (§4)
- We prove 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. (§5)

Finally, an appendix records experimental data gathered in Sage for random quotients of the Heisenberg group, showing in particular the variety of non-isomorphic groups visible in this model of random nilpotent groups and indicating some of their group-theoretic properties.

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. 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 [11, Ch 9], [3, Ch 10-12].

In the free group F_m of rank m, let

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

be the set of all nested commutators with j arguments. 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 a s-step nilpotent group G is a sequence of subgroups inductively defined by $G_{k+1} = [G_k, G]$ which form a subnormal series

$$\{1\} = G_{s+1} \lhd \ldots \lhd G_3 \lhd G_2 \lhd G_1 = G.$$

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

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

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 $\{u_1, \ldots, u_n\}$ 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 $t_i \le \tau_i$ for all i. Then the tuple of exponents $(t_1, \ldots, t_n)$ 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 $\mathrm{MB}_1 = \{a_1, \ldots, a_m\}$ 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.

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 $(A, B, C) \in \mathbb{Z}^3$.

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 $w = (w_1, \ldots, w_m) \in \mathbb{Z}^m$, 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 $(w_1, \ldots, w_m)$ 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.

Theorem 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 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 $\overline{w} = (\frac{w_1}{\delta},\cdots,\frac{w_{m-1}}{\delta})$. 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 $\langle \hat{g}, \hat{h}, h_2, \cdots, h_{m-1}\rangle = \langle \overline{g}, h_2,\dots,h_{m-1}, a_m\rangle = F_m$, which shows that $\hat{g}$ is primitive, as desired. □

The criterion in free nilpotent groups easily follows from a powerful theorem due to Magnus.

Theorem 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 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 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 $a = (\hat{a})^{-j/d}(\hat{b})^r(\hat{c})^{-t}$, 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 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 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 7. Given an abelian group $G = \mathbb{Z}^m/\langle\langle R \rangle\rangle$, 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

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

Consider the 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

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

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 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 such, so $d_m \leq d$ and thus $\gamma \leq d$. □

Lemma 9 (Killing a primitive element)**.** Let $H = N_{s,m}$ and let K be a normal subgroup of H. If $\mathrm{rank}(H/K) < m$ then K contains a primitive element.

Proof. Since $\mathrm{rank}(H/K) < m$, we also have $\mathrm{rank}(\mathrm{ab}(H/K)) < m$. Writing $\mathrm{ab}(H/K) \cong \bigoplus_{i=1}^m \mathbb{Z}/d_i\mathbb{Z}$ as above, we have $d_m = 1$. By the previous lemma there is a primitive element in the kernel of the projection $\mathrm{ab}(H) \to \mathrm{ab}(H/K)$, and any preimage in K is still primitive (see Cor 4). □

Lemma 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 $\mathrm{span}(v, v_2, \dots, v_n) = \mathrm{span}(u_1, \dots, u_n)$.

Proof. Since $v \in \mathrm{span}(u_1, \dots, u_n)$, we can write $v = \alpha_1u_1 + \dots + \alpha_nu_n$. 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 $\operatorname{span}(v, v_2, \cdots, v_n) = \operatorname{span}(u_1, \cdots, u_n)$, as needed. □

Lemma 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

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

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.

1.4. **Probability lemmas.** 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 can't undo the immediately previous 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 [1, Thm 1.3]. Fitzner and van der Hofstad derived a corresponding central limit theorem for NBSRW in [6]. 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 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 [1, 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

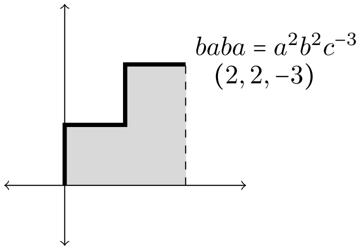
$$g = a^{i_1} b^{j_1} a^{i_2} b^{j_2} \ldots a^{i_r} b^{j_r}$$

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 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 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 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:

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

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 [2, Ch 3C]), and the result follows for $\hat{A}_{i,\ell}$. In fact, in that case the error term decays exponentially fast in ℓ:

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

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 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 $n = pq$. □

Corollary 17 (Probability of primitivity)**.** For a random freely reduced word in F_m, the probability that it is primitive in abelianization tends to $1/\zeta(m)$. In particular, for $m = 2$, the probability is $6/\pi^2$.

Proof. Using arithmetic uniformity, one derives a probability expression that agrees with $1/\zeta(m)$ by Euler's product formula for the zeta function; see [7]. □

Acknowledgments. This work was initiated in the Random Groups Research Cluster held at Tufts University in Summer 2014, supported by NSF CAREER award DMS-1255442. The coauthors had many stimulating and useful conversations in the course of the work, including with Phil Matchett-Wood, Nathan Dunfield, Dylan Thurston, Ilya Kapovich, Anschel Schaffer-Cohen, and Larry Guth. Special thanks to Keith Conrad for the clever suggestion for calculating $\hat{P}$ in §2 and to Hannah Alpert for several insightful observations.

2. 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.

First, it is a simple observation that depth in the LCS is respected by homomorphisms.

Lemma 18. 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 $\phi(G_k) \supseteq H_k$. □

The Magnus lifting theorem tells us the rank of $N_{s,m}/\langle\langle R\rangle\rangle$ equals the rank of its abelianization, so we quickly deduce the probability of rank drop.

Proposition 19 (Rank drop)**.** For a random r-relator nilpotent group $G = N_{s,m}/\langle\langle g_1, \ldots, g_r\rangle\rangle$,

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

Proof. This follows directly from considering the existence of a primitive element in $\langle\!\langle \mathrm{ab}(R) \rangle\!\rangle$. By Lemma 8, this occurs if and only if the rm entries are relatively prime, and by arithmetic uniformity (Lemma 15), this is computed by the zeta function, as in Corollary 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. 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

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

and noting that each exponent can take only finitely many values. Since the rank of a nilpotent group equals that of its abelianization (by Magnus 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 $\mathbb{Z}^m/\langle\!\langle R \rangle\!\rangle$, 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 $|R| < m-1$ and $|R| > m$ cases, 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, 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, in particular, all the a-weights could be even).

Random abelian groups are relatively well-studied, for instance in the important paper of Dunfield–Thurston testing the virtual Haken conjecture through random models [5, §3.14].

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

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

Lemma 20 (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 the generating functions derived by Dunfield–Thurston. (Corresponding facts for higher-rank quotients could also be derived from Dunfield–Thurston, but would be much more painful to compute by hand.)

Corollary 21 (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 can be explicitly bounded for each m. In the nearly-balanced case, the probability converges to .4357... as $m \to \infty$, while in the balanced case, the probability converges to at most .8469....

Proof. First we define $\hat{P} = \prod_p \left(1 + \frac{1/p}{p-1}\right)$ and note that $P(m)$ is a monotone increasing function in m, bounded above by $\hat{P}$, so it converges to some $P(\infty)$. We will compute the value of $\hat{P}$ precisely. First note that ${}^{(x^6-1)}/_{(x^3-1)(x+1)} = 1 - x + x^2$. From this, we have

$$1 + \frac{x^2}{1-x} = \frac{1-x+x^2}{1-x} = \frac{{}^{(x^6-1)}/_{(x^3-1)(x+1)}}{1-x} = \frac{1-x^6}{(1-x^3)(1-x^2)}.$$

Now putting in $x = 1/p$, we get

$$1 + \frac{1/p}{p-1} = \frac{1 - \frac{1}{p^6}}{(1 - \frac{1}{p^3})(1 - \frac{1}{p^2})}.$$

Recall that Euler's product formula for the zeta function is

$$\zeta(k) = \prod_{\text{primes } p} \frac{1}{1 - \frac{1}{p^k}},$$

we finally take the infinite product over primes and conclude that $\hat{P} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.943596436...$ On the other hand, it is well known that the product of zeta values converges, and we can define $\hat{Z} = \prod_{k=2}^{\infty} \zeta(k) = 2.294856591...$, so that $1/\hat{Z} = .4357....$

Finally, we have

$$\frac{P(m)}{Z(m)} \to \frac{P(\infty)}{\hat{Z}} \le \frac{\hat{P}}{\hat{Z}} = .8469...$$

$\square$

The probabilities of cyclic groups for balanced and nearly-balanced quotients of free abelian groups and therefore also for random nilpotent groups are approximated below.

Pr(cyclic)	$m = 2$	$m = 3$	$m = 4$	$m = 10$	$m = 100$	$m = 1000$	lower bound $\forall m$
$\lvert R \rvert = m - 1$	.607	.505	.467	.436	.4357	.4357	.4357
$\lvert R \rvert = m$	.9237	.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 $\mathbb{Z}^m$. In the recent paper [8], the authors show that

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

for a different model of random vectors, where entries are chosen uniformly from $[-n, n]$ and $n \to \infty$. However, the argument only uses mod p uniformity of coordinates, which we have also established for our setting in Corollary 16.

3. 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 22 (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 5, and let $D = \gcd(d,m)$. Then

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

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.

Note that this theorem is exact, not probabilistic.

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 $d = 4$, $m = 226$, $D = 2$, so we get

$$G = \left(\mathbb{Z}^2\big/_{\langle \binom{4}{226}, \binom{0}{4} \rangle}\right) \rtimes \mathbb{Z} \cong \left(\mathbb{Z}^2\big/_{\langle \binom{4}{2}, \binom{0}{4} \rangle}\right) \rtimes \mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}.$$

(5) if $g = a^2b^2c^2$, we have $d = 2$, $m = 3$, $D = 1$. 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.

We will refer to $D = 1$ as the *Baumslag-Solitar case*, because that is precisely the condition under which $b^d c$ is in the normal closure of $b^d c^m$, which means the group is presented as

$$G = \langle a, b \mid aba^{-1} = b^{d+1}, b^{d^2} = 1 \rangle,$$

a 1-relator quotient of the Baumslag-Solitar group $BS(1, d+1) = \langle a, b \mid aba^{-1} = b^{d+1} \rangle$.

Corollary 23. 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 Proposition 6, 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 $\langle\!\langle g \rangle\!\rangle = \langle b^d c^m, c^d \rangle \subset \langle b, c \rangle$. So in G, c has order d. A simple calculation verifies that b has order d^2/D in G, where $D = \gcd(d,m)$. Thus

$$\langle b, c \rangle \cong \mathbb{Z}^2\big/_{\langle \binom{d}{m}, \binom{0}{d} \rangle} \cong \left(\mathbb{Z}/\tfrac{d^2}{D}\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}\right)\big/_{\langle \binom{d}{m} \rangle}.$$

So, we have $G \cong \mathbb{Z}^2\big/_{\langle \binom{d}{m}, \binom{0}{d} \rangle} \rtimes \mathbb{Z}$, where the action sends $\binom{1}{0} \mapsto \binom{1}{1}$ and fixes $\binom{0}{1}$. If we are willing to lose track of the action and just write the group up to isomorphism, this simplifies to $G \cong (\mathbb{Z}/\frac{d^2}{D}\mathbb{Z} \ \times \ \mathbb{Z}/D\mathbb{Z}) \rtimes \mathbb{Z}$, as desired. □

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 $R = \{g_1, \dots, g_r\}$, where relator g_1 has the Mal'cev coordinates (i_1, j_1, k_1), and similarly for $g_2, \dots, g_r$. Let $M = \begin{pmatrix} i_1 & i_2 & \dots & i_r \\ j_1 & j_2 & \dots & j_r \end{pmatrix}$ 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 $k = (k_1, \dots, k_r)$ 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 24 (Orders of Heisenberg quotients)**.** Consider the group $G = H(\mathbb{Z})/\langle\langle g_1, \dots, g_r \rangle\rangle$, where relator g_1 has the Mal'cev coordinates (i_1, j_1, k_1), and similarly for $g_2, \dots, g_r$. Let $d = \gcd(i_1, j_1, \dots, i_r, j_r)$; 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 $c^n \in \langle\langle g_1, \dots, g_r \rangle\rangle$, 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. □

We will include experimental data about the distribution of random Heisenberg quotients in the appendix.

4. 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.

Theorem 25 (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 $\gcd(A_1(g), \dots, A_m(g)) = 1$.

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

Proof. Romanovskii's 1971 theorem [10, Thm 1] does most of this. In our language, he says that if $A_m(g) \neq 0$, then $\langle a_1, \dots, a_{m-1}\rangle$ 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 $\langle a_1, \dots, a_{m-1}\rangle \cong N_{s,m-1}$ 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. Furthermore, after a change of basis g can be written as $a_m^{\delta} h$ for some h in the commutator subgroup (Prop 6). So by taking enough commutators with a_1, we can see that there is torsion in the quotient group, which means that Romanovskii's injection is not an isomorphism.

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) 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 26 (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 $r \leq m$ random relators. Suppose $s \geq 2$ and $m \geq 2$. 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 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 $d_1 = \cdots = d_q = 0$ for $q = \dim(G)$, and we write $\langle\!\langle \mathrm{ab}(R)\rangle\!\rangle = \langle d_1 e_1, \dots, d_m e_m\rangle$ 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). 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 $b_1 \notin \langle\!\langle g_1, \dots, g_k\rangle\!\rangle$. To do so, we compute an arbitrary element

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

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 $r \leq m$. □

Theorem 27. (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. Then from the previous result we may assume $\operatorname{rank}(G) < m$ and therefore $\operatorname{rank}(\operatorname{ab}(G)) < m$. By Lemma 8, we can find a primitive vector w as a linear combination of the r vectors $\mathbf{A}(g_j)$. Consider a copy of the rank-r free group $F_r = F(\bar{a}_1, \dots, \bar{a}_r)$. We know there is a primitive element u of this free group with weights given w by the criterion for primitivity in free groups (Corollary 2). Replace each $\bar{a}_i$ in u by g_i to get a new word in $N_{s,m}$, which we call g'. Note that $\gcd(A_1(g'), \dots, A_m(g')) = \gcd(w) = 1$, so we can apply the linear algebra lemma (Lemma 10) and extend g' appropriately so that $\operatorname{span}(g', g'_2 \dots, g'_r) = \operatorname{span}(g_1, \dots, g_k)$. 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 relatively prime weights, the Freiheitssatz (Thm 25) 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 $r \le m-2$, then iterating this argument $r-1$ times gives $G \cong N_{s,m-k+1}/\langle\langle g_r\rangle\rangle$ for some new g_r, and $m-r+1 \ge 3$. Then we can apply Theorem 25 to conclude that this quotient is not abelian, because its nilpotency class is $s > 1$. □

Proposition 28 (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 26) implies $\mathbf{A}(g) = (0,0)$ (or a linear dependency between $\mathbf{A}(g)$ and $\mathbf{A}(g')$). But by Corollary 14, the changes of basis do not affect the probability of linear dependency, so this has probability zero. □

Corollary 29. 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 §2.

Pr(abelian)	$m=2$	$m=3$	$m=4$	$m=10$	$m=100$	$m=1000$	lower bound $\forall m$
$\lvert R\rvert = m-1$	.607	.505	.467	.436	.4357	.4357	.4357
$\lvert R\rvert = m$	.9237	.8842	.8651	.8469	.8469	.8469	.8469

Corollary 30 (Abelian one-relator)**.** For any step $s \ge 2$,

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

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

5. 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 group to facts about the LCS of classical random groups, deducing that *random groups are perfect* with exactly the same threshold again.

Recall that $T_{j,m} = \left\{ \left[a_{i_1}, \ldots, a_{i_j} \right] : 1 \le i_1, \ldots, i_j \le m \right\}$ 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 $H = \mathbb{Z}^m/\langle\!\langle R \rangle\!\rangle = \mathrm{ab}(\Gamma) = \mathrm{ab}(G)$, using the abuse of notation from Lemma 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.

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

Lemma 31 (Arithmetic distribution of determinants)**.** For a fixed rank $m \ge 1$ 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

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

out of q^{m^2} total matrices, where q is any prime power [9]. 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. □

Theorem 32 (Collapsing abelian quotients)**.** For random abelian groups $H = \mathbb{Z}^m/\langle\!\langle R \rangle\!\rangle$ with $|R|$ random relators, if $|R| \to \infty$ as a function of ℓ, then $H = \{0\}$ with probability one. If $|R|$ is bounded as a function of ℓ, then there is a positive probability of a nontrivial quotient.

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 §1.4. 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 $v_1, \ldots v_m$ 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 $\Delta_1 = \det(v_1, \ldots, v_m)$. 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 $L_1 \cup \dots \cup L_k$ has covolume $\le \gcd(\Delta_1, \dots, \Delta_k)$. Here, the Δ_k are identically and independently distributed with the probabilities described in the previous result (Lemma 31), and divisibility by different primes is independent, and therefore the probability of having $\gcd(\Delta_1, \dots, \Delta_k) = 1$ is

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

which goes to 1 as $k \to \infty$.

On the other hand, it is easy to see 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. □

Alternately, going through the theorem from KMP [8] and its modification for non-backtracking random walk vectors described in §2, we can simply observe that

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

for any fixed m as $r \to \infty$.

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 $\operatorname{ab}(\Gamma) = \Gamma/[\Gamma, \Gamma] = \{0\}$.

Corollary 33 (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 34 (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. $\mathbb{Z}^m/\langle\langle R \rangle\rangle = \{0\} \iff \operatorname{ab}(\Gamma) = \{0\} \iff \operatorname{ab}(G) = \{0\} \iff G = \{1\}$, with the last equivalence from Theorem 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 35 (Lifting to random groups)**.** *For $\Gamma = F_m/\langle\langle R \rangle\rangle$ and $G = N_{s,m}/\langle\langle R \rangle\rangle$, they 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 18), 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 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 36 (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 $i \ge k+1$. □

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

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

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.

6. Appendix: Experiments

6.1. **Multi-relator Heisenberg quotients.** The following table records the outcomes of 10,000 trials (1000 trials for each of the ten rows) with relators of length 999 and 1000. The shaded columns show infinite groups.

	$\lvert G\rvert = 1$	G cyclic nontrivial		G abelian noncyclic		G nonabelian		largest finite order
	(trivial)	(rk 1)		(rk 2 step 1)		(rk 2 step 2)		
$\lvert R\rvert = 1$	0	604	0	0	0	396	0	—
2	1	1	917	0	0	0	81	11178
3	514	0	467	0	9	0	10	717
4	766	0	228	0	2	0	4	104
5	884	0	116	0	0	0	0	7
6	945	0	55	0	0	0	0	4
7	979	0	21	0	0	0	0	3
8	981	0	19	0	0	0	0	3
9	995	0	5	0	0	0	0	2
10	997	0	3	0	0	0	0	2

Note that the triviality column comports closely with Kravchenko–Mazur–Petrenko's probability calculation described in §2:

$$\Pr(\operatorname{span}\{v_1,\dots,v_r\} = \mathbb{Z}^2) = \frac{1}{\zeta(r-1)\cdot\zeta(r)},$$

which predicts $0, 0, 506, 769, 891, 948, 975, 988, 994$, and 997 trivial quotients.

6.2. **Finite nonabelian quotients of balanced presentations.** Because underbalanced ($\lvert R\rvert \le m-2$) and nearly-balanced ($\lvert R\rvert = m-1$) presentations necessarily produce infinite groups, while the overbalanced case ($\lvert R\rvert \ge m+1$) often collapses the group, balanced presentations are a good source for finite nonabelian quotients, as one sees in the table above. Consider balanced quotients of $H(\mathbb{Z})$ for which the random relators have Mal'cev coordinates (i_1, j_1, k_1) and (i_2, j_2, k_2). Letting $\Delta = \lvert i_1 j_2 - i_2 j_1\rvert$, the group is finite if and only if $\Delta > 0$, in which case the order of the abelianization is Δ. Letting $d = \gcd(i_1, j_1, i_2, j_2)$, we recall that $d = 1$ implies a cyclic quotient, so the finite nonabelian case requires $\Delta > 0$ and $d > 1$. Having $\Delta > 0$ implies that there are no nontrivial linear dependencies between $\binom{i_1}{j_1}$ and $\binom{i_2}{j_2}$, so $K(R) = 0$ (as in Theorem 24), making the order of c in the quotient group equal to d; since $\lvert\langle c\rangle\rvert = d$, the quotient is nonabelian iff $d > 1$. Finally $\lvert G\rvert = \Delta \cdot d$, and we further note that $d^2 \mid \Delta$, so d^3 divides the order of the group. This means that the smallest possible orders of nonabelian quotients are $8, 16, 24, 27, 32, 40, 48, 54, \dots$

With small-order groups, one can easily classify by isomorphism type, asking for instance how many of the order-eight nonabelian groups are isomorphic to the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ and how many to the dihedral group D_4. However, since the expected magnitude of each of the entries in $\binom{i_1}{j_1}$ and $\binom{i_2}{j_2}$ is $\sqrt{\ell}$, the value of Δ and hence the expected size of these quotient groups is growing fast with ℓ. Therefore to illustrate the distribution of random nilpotent groups that are small-order nonabelian, we consider $n = 10,000$ trials with $\ell = 9$ or 10. In this sample, 562 of the quotients were finite nonabelian.

order	8	16	24	27	32	40	48	54	56	64	72	80	81	88	96	125	216
frequency	130	138	65	41	45	32	35	24	9	18	9	3	6	1	2	2	2

Of the 130 groups in this sample of order eight, 33 were isomorphic to Q, and the other 97 to D_4.

6.3. **One-relator Heisenberg quotients.** Finally, we use Lemma 5 and Theorem 22 to study the diversity of random infinite groups appearing in the one-relator case. Given a random relator whose Mal'cev coordinates are (i, j, k), we first change variables as in the Lemma to obtain coordinates $(0, d, m)$, where $d = \gcd(i, j)$ and $m = \frac{ij}{2d}(d-1) + k$. In this presentation, as noted in the proof of the Theorem, $\operatorname{ord}(c) = d$ and $\operatorname{ord}(b) = d^2/D$, while a has infinite order. Thus every word involving a has infinite order; on the other hand, b and c commute and so any word in those letters alone has order at most d^2/D (note that this is divisible by d because $D = \gcd(d, m)$). Extracting information that is independent of presentation, we conclude that the order of the center is d and the largest order of a torsion element is d^2/D.

We ran $n = 20,000$ trials with $\ell = 999$ or 1000 and plotted the frequency of each $(d^2/D, d)$ pair (Figure 1). Besides the groups that are pictured, there were also four occurrences of $(i, j) = (0, 0)$ in the sample, with k values $55, 187, 230, 580$, that are not pictured. Because groups with distinct $(d^2/D, d)$ pairs must be non-isomorphic, our sample contains at least 202 distinct groups (up to isomorphism).

Recall from the discussion on page 12 that groups with $D = 1$ are quotients of $BS(1, d+1)$, which we call Baumslag-Solitar type. But $D = \gcd(d, m)$, and from the expression $m = \frac{ij}{2d}(d-1) + k$ we can note that $2d \mid ij$ if either i or j is even, in which case $\gcd(d, m) = \gcd(i, j, k)$. (If both are odd, the situation splits into cases depending on the 2-adic valuations.) This suggests heuristically that non-cyclic groups of Baumslag-Solitar type should occur with probability $\frac{1}{\zeta(3)} - \frac{1}{\zeta(2)} = .22398\ldots$ The precise frequency of groups of this type in the sample was 4404, or 22.02%.

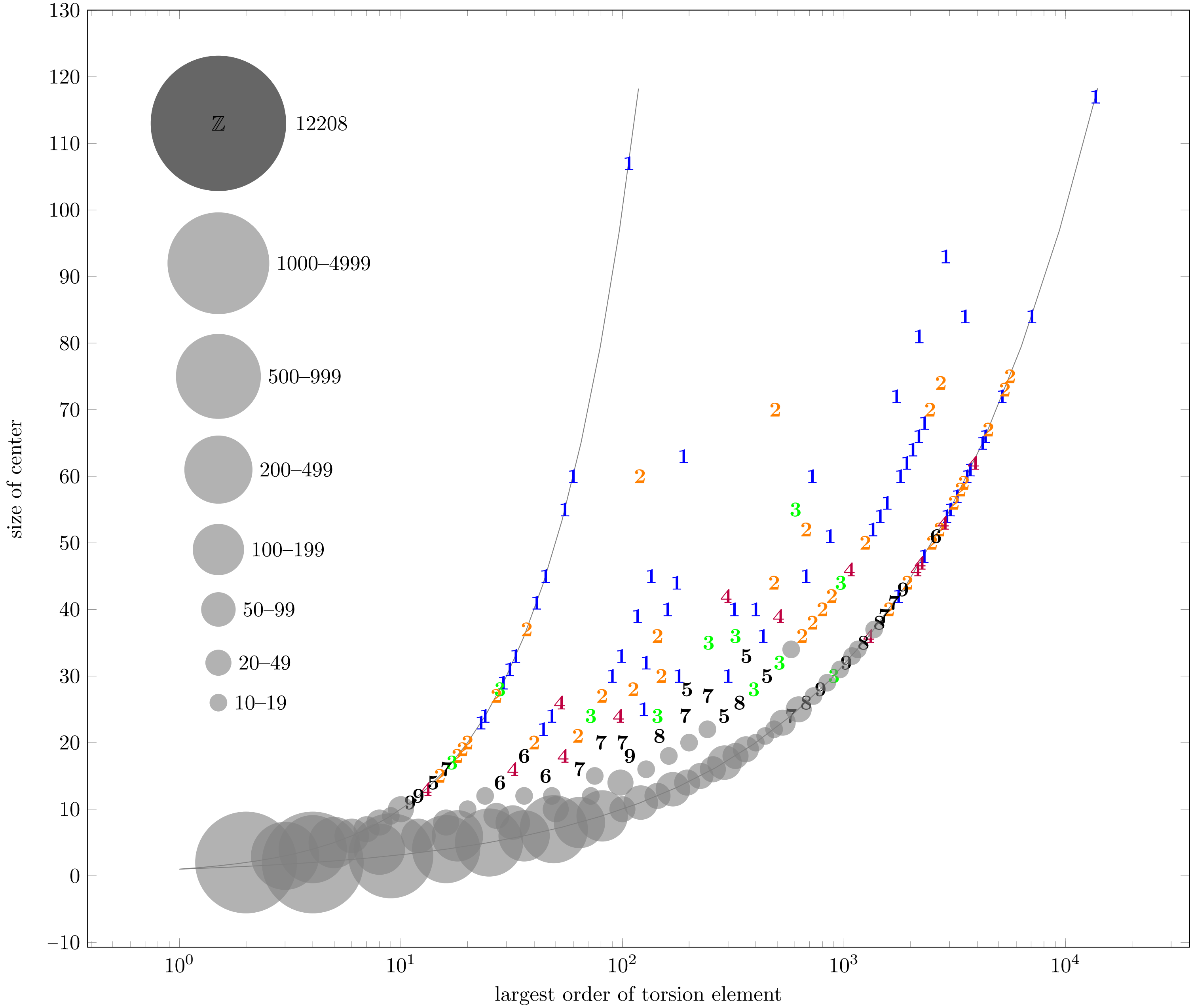


FIGURE 1. A semilog plot of $(d^2/D, d)$ in 20,000 random 1-relator quotients of the Heisenberg group with relator length 999 or 1000, showing a variety of non-isomorphic groups. Displayed digits represent the number of occurrences of a particular $(d^2/D, d)$ pair below 10, and variously sized disks indicate frequencies of ten and higher. Since $D \mid d$, all possibilities lie between the curves (d, d) and (d^2, d). Of these random groups, 61% are isomorphic to $\mathbb{Z}$ and an additional 22% are of Baumslag-Solitar type ($D = 1$), and thus lie along the lower curve (d^2, d).

References

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

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

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

[4] 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.

[5] N. Dunfield and W. Thurston, *Finite covers of random 3-manifolds.* Invent. Math. 166 (2006), no. 3, 457–521.

[6] R. Fitzner and R. van der Hofstad, *Non-backtracking random walk.* Journal of Statistical Physics 150(2): 264-284, (2013).

[7] Hardy and Wright, *An introduction to the theory of numbers.* Sixth edition. Oxford University Press, 2008.

[8] R. Kravchenko, M. Mazur, and B. Petrenko, *On the smallest number of generators and the probability of generating an algebra.* Algebra Number Theory 6 (2012), no. 2, 243–291.

[9] Derek J.S. Robinson, A course in the theory of groups, 2nd ed., Springer-Verlag, 1996.

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

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