Random groups are not left-orderable

Damian Orlef

Abstract

We prove that random groups in Gromov density model at any density \( d \) are with overwhelming probability either non-left-orderable or trivial. It implies the lack of left-orderability for \( d < \frac{1}{2} \).

1 Introduction

We work in the density model for random groups introduced by Gromov.

Definition 1.1 [3, Section 9.B], [6, Definition 7]. Let \( F_n \) be the free group on \( n \geq 2 \) generators \( a_1, \ldots, a_n \). For any integer \( L \) let \( R_L \subset F_n \) be the set of reduced words of length \( L \) in these generators.

Let \( d \in (0,1) \). A random set of relators at density \( d \), at length \( L \) is a \( \lfloor (2n - 1)^d L \rfloor \)-tuple of elements of \( R_L \), picked independently and uniformly at random from all elements of \( R_L \).

A random group at density \( d \), at length \( L \) is the group \( G \) presented by \( \langle S \mid R \rangle \), where \( S = \{a_1, \ldots, a_n\} \) and \( R \) is a random set of relators at density \( d \), at length \( L \).

Let \( I \subset \mathbb{N}_+ \) be infinite. We say that a property of \( R \), or of \( G \), occurs with \( I \)-overwhelming probability (shortly, w. I-o.p.) at density \( d \) if its probability of occurrence tends to 1 as \( L \to \infty \), for \( L \in I \) and fixed \( d \). We omit writing “I-” if \( I = \mathbb{N}_+ \).

Relators in \( R_L \) are not assumed to be cyclically reduced.

Basic properties of the model were proved by Gromov in the following phase transition theorem.

Theorem 1.2 [3, Section 9.B], [5, Theorem 2]. A random group is with overwhelming probability

- trivial or \( \mathbb{Z}/2\mathbb{Z} \) at density \( d > \frac{1}{2} \),
- infinite, hyperbolic and torsion-free at density \( d < \frac{1}{2} \).

Random groups can be treated as a model of typical finitely-presented groups. They are thus possibly useful as testing grounds for various conjectures. For torsion-free groups, still open is the following, attributed to I.Kaplansky.

Conjecture 1.3. Let \( K \) be a field and \( G \) a group. The group algebra \( K[G] \) contains no zero divisors if and only if \( G \) is torsion-free.

As random groups are torsion-free for \( d < \frac{1}{2} \), it would be interesting to settle Conjecture 1.3 at least for them.

Conjecture 1.3 can be easily seen to hold for groups that can be left-ordered.

Definition 1.4. A group \( G \) is said to be left-ordered by \( \leq \) if \( \leq \) is a total order on \( G \) which is left-invariant: for all \( g_1, g_2, h \in G \) the condition \( g_1 \leq g_2 \) implies \( hg_1 \leq hg_2 \).
In this paper, however, we show that we cannot use this approach for random groups, because random groups below the critical density \( d = \frac{1}{2} \) are not left-orderable. More precisely, we prove the following.

**Theorem 1.5.** Let \( d \in (0, 1) \). A random group in Gromov density model at density \( d \) is with overwhelming probability either trivial or non-left-orderable.

As free groups are left-orderable (see [1, Theorem 2.3.1]), this result may be regarded as an alternative way of proving that random groups are not free of rank \( \geq 1 \) at any density.

The main idea of the proof is to use the order to explicitly construct a high-density set \( P \) containing only words representing strictly positive (in the sense of order) elements of the given random group \( G = \langle S | R \rangle \). It happens that for fixed \( d \), the density of \( P \) exceeds \((1 - d)\) for \( n \) sufficiently large. By a well-known fact it thus contains w.o.p. a word \( w \) from the set \( R \) of relators, leading to a contradiction of corresponding element \( w \in G \) being both positive and trivial. Finally, we use the approach of [2] to increase the number of generators we work with to obtain the result for all \( n \geq 2 \).

The whole proof is phrased in the language of b-automata and associated groups, introduced in [2] and follows a very similar framework.

Section 2 deals with basic properties of left-ordered groups. In Section 3 we introduce basic properties of b-automata and its languages and use them to give a proof of Theorem 1.5 for \( n \) sufficiently large. In Section 4 we use the concept of associated groups to generalise it to all \( n \geq 2 \). In Section 5 we reprove a well-known generalisation of the fact that a random set of relators at density \( d \) intersects w.o.p. any fixed set of relators of density \( d' \), such that \( d + d' > 1 \). The more general statement is that their intersection is roughly of density \( d + d' - 1 \), if \( d < \frac{1}{2} \) (cf. [3, Section 9.A]). We prove it by a pretty straightforward application of the Central Limit Theorem. The assumption on \( d \) comes from the fact that we define “a random set at density \( d' \) to be a tuple with possible repetitions. If we, however, have \( d < \frac{1}{2} \), then there are w.o.p. no such repetitions and the counting is easier.

**Acknowledgements**

Yago Antolin-Pichel, in private communication, suggested the key property of the left-ordered groups used in the proof, Lemma 2.4. Piotr Przytycki suggested the topic of this paper, encouraged and advised the author. I would like to thank both of them.

## 2 Left orders

Let \( G \) be a group left-ordered by \( \leq \). Symbols \(<\) and \(>\) are the usual shorthands. By \( e \) we denote the neutral element of \( G \). The following remarks are easily obtained from Definition 1.4.

**Remark 2.1.** Any non-empty product of elements strictly greater than \( e \) is itself strictly greater than \( e \).

**Remark 2.2.** For every \( g \in G \setminus \{ e \} \) one can choose a sign \( \varepsilon \in \{-1, 1\} \), such that \( g^\varepsilon > e \).

Those two imply quickly the following.

**Corollary 2.3.** \( G \) is torsion-free.

**Proof.** Take any \( g \in G \setminus \{ e \} \). By Remark 2.2, we can choose \( \varepsilon \in \{-1, 1\} \) such that \( g^\varepsilon > e \). Remark 2.1 implies now that for every \( n \geq 1 \) we have \( g^{n\varepsilon} > e \), so \( g \) is not a torsion element. \( \square \)
Moreover, by combining Remarks 2.1 and 2.2, we obtain Lemma 2.4, which will be used in a moment to construct high-density sets of words representing non-trivial elements. It was suggested by Yago Antonin-Pichel.

**Lemma 2.4.** For every choice of non-trivial \(g_1, \ldots, g_n \in G\) there exists a sequence of signs \(\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}\) for which every non-empty product (possibly with repetitions) of elements of form \(g_i^{\varepsilon_i}\) is non-trivial.

**Proof.** Choose \((\varepsilon_i)_{i=1}^n\) for which \(g_i^{\varepsilon_i} > e\) for \(i = 1, \ldots, n\). \(\square\)

Lemma 2.4 is in fact equivalent to \(G\) being left-orderable, but we will only need the implication we proved (see [1, Theorem 7.1.1]).

### 3 Random groups with large number of generators

We begin by reproducing terminology and useful observations of [2, Section 2]. By \(S\) we denote a finite set, called the *alphabet*. We define \(S^{-1}\) to be the set of formal inverses to elements of \(S\), and denote \(S^\pm = S \cup S^{-1}\). Elements of \(S^\pm\) are called *letters*. By *word* over an alphabet \(S\) we mean a finite sequence of letters. We denote \(S = \{a_1, \ldots, a_n\}\), hence \(n = |S|\). \(S\) is to be interpreted as the set of generators of \(F_n\).

**Definition 3.1** [2, Definition 2.1]. A *basic automaton* (shortly a *b-automaton*) over an alphabet \(S\) with transition data \([\sigma_s]\) is a pair \((S, \{\sigma_s\})\), where \(\{\sigma_s\}_{s \in \emptyset \cup S^\pm}\) is a family of subsets of \(S^\pm\).

The *language* of a b-automaton with transition data \(\{\sigma_s\}\) is the set of all nonempty words over \(S\) beginning with a letter in \(\sigma_s\) and such that for any two consecutive letters \(ss'\) we have \(s' \in \sigma_s\).

We say that a b-automaton is \(\lambda\)-large, for some \(\lambda \in (0, 1)\), if \(\sigma_s \neq \emptyset\) and for each \(s \in S^\pm\) we have \(|\sigma_s| \geq \lambda 2n\).

**Remark 3.2** [2, Remark 2.2(i)]. There are exactly \(2^{2n(2n+1)}\) many b-automata over a fixed alphabet \(S\) of size \(n\).

**Remark 3.3** [2, Remark 2.2(ii)]. If a b-automaton is \(\lambda\)-large, then its language contains at least \([\lambda 2n]^L-1\) words of length \(L\) and at least \((|\lambda 2n| - 1)^{L-1}\) reduced words of length \(L\).

**Definition 3.4** [2, Definition 2.3]. Let \(I \subset \mathbb{N}_+\) be infinite and let \(\mathcal{L}\) be a set of reduced words over an alphabet \(S\), containing for all but finitely many \(L \in I\) at least \(ck^L\) words of length \(L\), where \(c > 0\), \(k > 1\). Then we say that the *I-growth rate of \(\mathcal{L}\)* is at least \(k\). Similarly, if \(k > k'\), then we say that the *I-growth rate of \(\mathcal{L}\)* is greater than \(k'\).

It is convenient to extend the notion of density from Definition 1.1 in the following way.

**Definition 3.5.** Let \(I \subset \mathbb{N}_+\) be infinite and let \(\mathcal{L}\) be a set of reduced words over an alphabet \(S\), containing for all but finitely many \(L \in I\) at least \(c(2n - 1)^dL\) words of length \(L\), where \(c > 0\), \(d \in (0, 1)\). Then we say that the *I-density of \(\mathcal{L}\)* is at least \(d\).

Notions of density \(d\) and growth rate \(k\) of the set \(\mathcal{L}\) are easily seen to be strictly related by \(k = (2n - 1)^d\), i.e. for such \(k, d\), with \(d \in (0, 1)\), the set \(\mathcal{L}\) has the I-growth rate at least \(k\) if and only if it has the I-density at least \(d\).

The following is a well known fact in random groups. We reprove it in a stronger form in Section 5.
Proposition 3.6 [3, Section 9.A]. Let $I \subset \mathbb{N}_+$ be infinite. Suppose $d, d' \in (0, 1)$ are such that $d + d' > 1$ and $R_I \subset F_n$ is a fixed set of relators in some fixed number $n$ of generators, of $I$-density at least $d'$. Then $w$, $I$-o.p. a random set $R$ of relators at density $d$ intersects $R_I$.

From this we get

Lemma 3.7 [2, Lemma 2.4]. Let $L$ be a set of reduced words over the alphabet $S$, of the $I$-growth rate greater than $(2n - 1)^{1-d}$, for some $d \in (0, 1)$. Then $w$, $I$-o.p. a random set of relators at density $d$ intersects the languages $L$.

We will be interested in the following consequence.

Corollary 3.8 [2, Corollary 2.5]. For given $\lambda, d \in (0, 1)$, if $n$ is sufficiently large, then $w$, o.p. a random set of relators at density $d$ intersects the languages of all $\lambda$-large b-automata over the alphabet $S$.

Proof. As the number of b-automata over $S$ is finite and depends only on $n$ (by Remark 3.2), we just need to show that there exists $n_0$, for which if $n \geq n_0$, then the conclusion holds for the language $L$ of every single $\lambda$-large b-automaton. By Remark 3.3, the $\mathbb{N}_+$-growth rate of the set of reduced words in $L$ is at least $\left\lceil \lambda 2n \right\rceil - 1$, hence, by Lemma 3.7, the following inequality suffices.

$$\left\lceil \lambda 2n \right\rceil - 1 > (2n - 1)^{1-d}$$

As $d \in (0, 1)$, this inequality holds for $n$ large enough. \hfill $\square$

For a group $G$ with presentation $G = \langle S|R \rangle$ and a word $w$ over the alphabet $S$, we will denote by $\overline{w}$ the corresponding element of $G$.

To obtain Theorem 1.5 for $n$ sufficiently large, we just need the following.

Proposition 3.9. Let $G$ be a group with presentation $G = \langle S|R \rangle$, such that $R$ intersects the languages of all $\frac{1}{2}$-large b-automata over the alphabet $S = \{a_1, \ldots, a_n\}$. Then $G$ is either trivial or non-left-orderable.

In order to prove Proposition 3.9, we use the following lemma, which is our main step towards exploiting hypothetical left-orderability of random groups.

Lemma 3.10. Let $R$ be a set of words over the alphabet $S$. Assume $R$ intersects the languages of all $\frac{1}{2}$-large b-automata over $S$. Then for every choice of signs $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$ and a number $i \in \{1, \ldots, n\}$, there exists a nonempty reduced word $w \in R$, consisting only of letters from the set $\{a_1^{\varepsilon_1}, a_2^{\varepsilon_2}, \ldots, a_n^{\varepsilon_n}\}$, with at least one occurrence of $a_i^{\varepsilon_i}$.

Proof of Lemma 3.10. Consider a b-automaton $A$ over $S$ with transition data $\sigma_0 = \{a_i^{\varepsilon_i}\}$ and $\sigma_s = \{a_1^{\varepsilon_1}, \ldots, a_n^{\varepsilon_n}\}$ for every $s \in S^\pm$. Every word in its language $L$ is reduced. $A$ is $\frac{1}{2}$-large, hence there exists some $w \in L \cap R$. The word $w$ starts with $a_i^{\varepsilon_i}$ and it satisfies conditions imposed. \hfill $\square$

Proof of Proposition 3.9. Suppose $G$ is left-orderable, but non-trivial. Let $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$ be all those elements $a_j \in S$, such that $\overline{a_j} \in G$ is non-trivial. There must be at least one, since $G$ is generated by elements $\overline{a_j}$. According to Lemma 2.4, we can find signs $\varepsilon_{i_1}, \ldots, \varepsilon_{i_m} \in \{-1, 1\}$, such that every nonempty word consisting of letters from $\{a_{i_1}^{\varepsilon_{i_1}}, \ldots, a_{i_m}^{\varepsilon_{i_m}}\}$ represents a non-trivial element of $G$ (such words are always reduced).

Now for $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_m\}$ choose $\varepsilon_j \in \{-1, 1\}$ in arbitrary way. We have thus defined a sequence $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$. By Lemma 3.10 applied to this sequence and $i = i_1$, we obtain a word $w$ which lies in $R$, so it represents the trivial element of $G$, and consists
of letters of form $a_{i_1}^{s_1}$ with at least one occurrence of $a_{i_1}^{s_1}$. As $a_{j}^{s_j}$ for $j \notin \{i_1, \ldots, i_m\}$ represent the trivial element, we can remove all occurrences of such letters from $w$ and obtain that way a word $w_1$, still representing the trivial element and consisting only of letters of form $a_{i_1}^{s_1}$. $w_1$ is, however, nonempty because of at least one occurrence of $a_{i_1}^{s_1}$. We arrive thus at a contradiction with the earlier definition of signs $\varepsilon_{i_1}, \ldots, \varepsilon_{i_m}$. \hfill \Box

For fixed $d \in (0, 1)$ and $\lambda = \frac{1}{2}$ there is $n_0$ such that the conclusion of Corollary 3.8 holds for all $n \geq n_0$. For such $n$ Theorem 1.5 is now almost immediate.

**Proof of Theorem 1.5 for $n \geq n_0$.** A random group $G$ is w.o.p. presented by $\langle S|R \rangle$, where $R$ intersects the languages of all $\frac{1}{3}$-large b-automata over $S$, so, by Proposition 3.9, it is either non-left-orderable or trivial. \hfill \Box

### 4 Increasing the number of generators

We now generalise our partial proof of Theorem 1.5 to arbitrary values of $n \geq 2$. We follow closely the ideas of [2, Section 3].

We fix $n \geq 2$ and $d \in (0, 1)$. We furthermore fix $B$ to be a natural number that is sufficiently large with respect to $n$ and $d$ in a way we will specify later.

As before, we denote by $S$ the set of generators $\{a_1, \ldots, a_n\}$. Let $\tilde{S} \subset F_n$ denote the set of reduced words of length $B$ over the alphabet $S$. The involution on $\tilde{S}$ mapping each word to its inverse does not have fixed points. Thus we can partition $\tilde{S}$ into $\tilde{S}$ and $\tilde{S}^{-1}$. We introduce notation $\tilde{S}^\pm = \tilde{S} \cup \tilde{S}^{-1}$ in place of $\tilde{S}$.

Furthermore, for $0 \leq P < B$ let $I_P \subset \mathbb{N}_+$ denote the set of those $L$ that can be written as $L = BL + P$ with $L > 0$.

**Definition 4.1** [2, Definition 3.1]. Let $r$ be a word of length $L \in I_0$ over the alphabet $S$. Divide the word $r$ into $\hat{L}$ blocks of length $B$. This determines a new word $\hat{r}$ of length $\hat{L}$ over the alphabet $\hat{S}$, which we call the word associated to $r$.

**Definition 4.2** [2, Definition 3.2]. Given a set $R$ of reduced relators over $S$ of equal length $L \in I_P$, we define the associated group $\hat{G}$ in the following way:

If $P = 0$, then we consider the set $\hat{R}$ of relators associated to relators in $R$. We define $\hat{G}$ to be the group $\langle \hat{S}|\hat{R} \rangle$.

If $1 \leq P < B$, then we do the following construction. Suppose that $r_1, r_2 \in R$ are two relators of length $L$ over $S$, satisfying $r_1 = q_1\varepsilon^{-1}$ and $r_2 = v_2q_2$ (we assume $q_1, q_2, v$ to be reduced and that there are no reductions between $q_1$ and $\varepsilon^{-1}$ or between $v$ and $q_2$), for some word $v$ over $S$ of length $P$. We then obtain a (possibly non-reduced) word $q_1q_2$ over $S$, of length $2BL$, with the property that $\overline{q_1q_2} = \varepsilon$ in $G = \langle S|R \rangle$. To this word we can associate, as before, a relator over $\tilde{S}$, of length $2\hat{L}$ (possibly non-reduced), which we denote by $\hat{r}(r_1, r_2)$. We denote by $\hat{R}$ the set of all $\hat{r}(r_1, r_2)$ as above and we define $\hat{G} = \langle \hat{S}|\hat{R} \rangle$.

The main intuition here is that $\hat{R}$ obtained from a random set $R$ of relators over $S$, at density $d$, at length $L \in I_0$ is very similar to a random set of relators over $\tilde{S}$, at the same density $d$, at length $\hat{L}$ (see [2, Section 3]).

By increasing $B$, the number $\hat{n}$ can be made arbitrarily large. We can thus have $\hat{n}$ large enough to obtain the conclusion of Corollary 3.8 for intersections of languages of $\frac{1}{3}$-large b-automata over $\tilde{S}$ with random sets of relators at density $d$. We then use the following analogue of Proposition 3.9.
Proposition 4.3. Suppose that $\hat{R}$, obtained as in Definition 4.2 from $R$ being a set of reduced relators of the same length, intersects languages of all $\frac{1}{d}$-large b-automata over $\hat{S}$. Then $G = \langle S|R \rangle$ is either trivial or non-left-orderable.

Proof. Suppose $G$ is non-trivial and left-orderable. Construction of $\hat{G}$ was performed in such a way, that by expanding elements of $\hat{S}$ into words over $\hat{S}$ we get a natural epimorphism $\phi : \hat{G} \to H$, where $H$ is the subgroup of $G$ generated by the reduced words of length $B$ over $S$.

We note that $H \subset G$ is of finite index, since every element $g \in G$ is of form $g = \overline{w}$ for some reduced word $w$ over $S$ and we may write $w = uv$ with $u$ of length at most $B$ and $v$ of length divisible by $B$. We have thus $\overline{w} \in H$, hence $g \in \overline{w}H$ and the index $[G : H]$ is not greater than the number of possible values of $\overline{w}$, which is finite.

Moreover, $H$ is non-trivial, because otherwise $G$ would be finite and non-trivial, hence not torsion-free, contradicting left-orderability (by Corollary 2.3).

Denote elements of $\hat{G}$, represented by single letters from $\hat{S}$, by $b_1, \ldots, b_n$. They generate $\hat{G}$, so $H$ is generated by $\phi(b_1), \ldots, \phi(b_n)$, not all of them being trivial. Let $\phi(b_1), \ldots, \phi(b_m)$ be all non-trivial elements of form $\phi(b_j)$. Subgroup $H$ is left-orderable, so, by Lemma 2.4, there exist signs $\varepsilon_1, \ldots, \varepsilon_m \in \{-1, 1\}$, such that every non-empty product of elements of form $\phi(b_i)$ is non-trivial. In arbitrary way we choose $\varepsilon_i \in \{-1, 1\}$ for $i \in \{1, \ldots, m\}$.

Fix $i = i_1$. For this index $i$ and the set $\hat{R}$ of words over $\hat{S}$ we apply Lemma 3.10 to conclude that there exists a product of elements of form $b_j^{\varepsilon_j}$, with at least one occurrence of $b_{i_1}^{\varepsilon_{i_1}}$, which evaluates to the trivial element in $G = \langle \hat{S}|\hat{R} \rangle$.

By evaluating $\phi$ on this product, we get a product of elements of form $\phi(b_j)^{\varepsilon_j}$, with at least one occurrence of $\phi(b_{i_1})^{\varepsilon_{i_1}}$, which evaluates to the trivial element in $H$. Finally, by leaving the non-trivial factors only, we get a non-empty product of elements of form $\phi(b_j)^{\varepsilon_j}$, evaluating to the trivial element, which is a contradiction with the definition of signs $\varepsilon_1, \ldots, \varepsilon_m$.

The last element of the proof of Theorem 1.5 is the following.

Lemma 4.4. If $B$ is sufficiently large, then, in Gromov density model with $n$ generators, a random set $R$ of relators at density $d$ has w.o.p the property, that the set $\hat{R}$, obtained from $R$ as in Definition 4.2, intersects languages of all $\frac{1}{d}$-large b-automata over $\hat{S}$.

Assuming Lemma 4.4, the proof of Theorem 1.5 is straightforward.

Proof of Theorem 1.5. Let $B$ be sufficiently large for the conclusion of Lemma 4.4 to hold. Then, by the combination of Proposition 4.3 and Lemma 4.4, a random group $G = \langle S|R \rangle$ in Gromov density model is w.o.p either non-left-orderable or trivial.

The proof of Lemma 4.4 (in slightly stronger form) is given in [2, Section 3] in the first 5 lines of the proof of [2, Theorem 1.5]. The hypothesis of [2, Proposition 2.6] for group $G = \langle S|R \rangle$, obtained from a random group $G = \langle S|R \rangle$, is checked there, which amounts to proving that $\hat{R}$, obtained from a random set $R$ of relators in Gromov model, intersects languages of all $\frac{1}{d}$-large b-automata over $\hat{S}$.

5 Intersections of high-density sets

In this section, by $I \subset \mathbb{N}_+$ we denote a fixed infinite subset and all limits with $L \to \infty$ are taken over $L \in I$. The main result of this section is the following.

Proposition 5.1. Suppose that for each $L \in I$ we have a set $R_L$ of size $c_L > 0$ with $a_L > 0$ elements distinguished. For fixed $L$ we pick uniformly and independently at random entries
of a $b_L$-tuple ($b_L > 0$) from $R_L$ and obtain this way a random variable $D_L$ equal to the number of the entries of the resulting tuple being distinguished. Assume that $\frac{a_L b_L}{c_L} \to \infty$ as $L \to \infty$. Then for every $\varepsilon > 0$ the following holds

$$
\lim_{L \to \infty} \mathbb{P} \left( (1 - \varepsilon) \frac{a_L b_L}{c_L} \leq D_L \leq (1 + \varepsilon) \frac{a_L b_L}{c_L} \right) = 1.
$$

Before proving Proposition 5.1, let us use it to give a proof of Proposition 3.6 and its generalisation.

**Proof of Proposition 3.6.** Let $c_L$, for $L \in I$, denote the number of all reduced relators of length $L$ over $S$, i.e. $c_L = |R_L| = 2n(2n-1)^L - 1$. Moreover, let $a_L = |R_I \cap R_L|$ be the number of relators of length $L$ we distinguish by wanting them to be selected in the random tuple. Let $b_L = \lceil 2(2n-1)^{d_L} \rceil$. We assume $a_L \geq C(2n-1)^{d_L}$ for $L \in I$ sufficiently large and some $C > 0$. At length $L$, $R$ is a tuple of $b_L$ elements, chosen uniformly and independently at random from $R_L$. Let $D_L$ be as in Proposition 5.1. Note that $\frac{a_L b_L}{c_L} \to \infty$ as $L \to \infty$, since $d + d' > 1$. We may thus apply Proposition 5.1 for any $\varepsilon > 0$ to see that a random set $R$ of relators at density $d$, at length $L$ has w. I-o.p. at least $D_L \geq (1 - \varepsilon) \frac{a_L b_L}{c_L} \geq (2n-1)^{(d + d' - 1)L}$ entries from $R_I$, for some $K > 0$. For $L$ sufficiently large it clearly implies that $R$ and $R_I$ intersect. 

If we moreover assume that $d < \frac{1}{2}$ and $R_I$ is roughly (not just at least) of density $d'$, then we can prove that the intersection is roughly of density $d + d' - 1$.

**Proposition 5.2.** Suppose $d, d' \in (0,1)$ are such that $d + d' > 1$ and $d < \frac{1}{2}$. Let $R_I \subset F_n$ be a fixed set of relators in some fixed numer $n$ of generators, such that for some $C_1, C_2 > 0$ the inequalities

$$
C_1(2n-1)^{d'L} \leq |R_I \cap R_L| \leq C_2(2n-1)^{d'L}
$$

hold for all sufficiently large $L \in I$.

Then for some $K_1, K_2 > 0$ a random set $R$ of relators at density $d$, at length $L$ satisfies w. I-o.p. the inequalities

$$
K_1(2n-1)^{(d + d' - 1)L} \leq |R_I \cap R| \leq K_2(2n-1)^{(d + d' - 1)L},
$$

where $|R_I \cap R|$ denotes the number of distinct entries of $R$, belonging to $R_I$.

**Proof.** We use the notation from the proof of Proposition 3.6. Analogously to that proof, for some $K_1, K_2 > 0$ we obtain

$$
K_1(2n-1)^{(d + d' - 1)L} \leq D_L \leq K_2(2n-1)^{(d + d' - 1)L},
$$

occuring w. I-o.p.

Since $d < \frac{1}{2}$, we have $\frac{b_L^2}{c_L} \to 0$ as $L \to \infty$.

Let us estimate the probability $q_L$ that in the experiment defining $D_L$ all elements of the obtained $b_L$-tuple are pairwise distinct. It is the same as the probability that every element of the tuple is different from the elements having smaller indices (we assume some fixed order on a tuple), so

$$
q_L = 1 \left( 1 - \frac{1}{c_L} \right) \left( 1 - \frac{2}{c_L} \right) \ldots \left( 1 - \frac{b_L - 1}{c_L} \right) \geq \left( 1 - \frac{b_L - 1}{c_L} \right)^{b_L}
$$

For $L \in I$ sufficiently large we have $\frac{b_L}{c_L} < 1$, so $b_L \leq b_L^2 < c_L$ and the number $x_L = \frac{b_L - 1}{c_L}$ satisfys $x_L \geq -1$. It means that we can use Bernoulli’s inequality to obtain

$$
q_L \geq \left( 1 + \left( - \frac{b_L - 1}{c_L} \right) \right)^{b_L} \geq 1 - b_L \frac{b_L - 1}{c_L}.
$$
Obviously, \( b_L \frac{1}{q_L} \to 0 \) as \( L \to \infty \), because \( \frac{\log L}{L} \to 0 \) as \( L \to \infty \). It follows that \( q_L \to 1 \) as \( L \to \infty \), so \( I \)-a.p. the number \( D_L \) is the number of distinct entries of \( R \) belonging to \( R_I \), which combined with (2) concludes the proof.

For the proof of Proposition 5.1 we will apply the following form of the Central Limit Theorem.

**Theorem 5.3** [4, Theorem 5.12]. Let \( (Y_i^{(L)})_L \in I \), \( i = 1, \ldots, b_L \), be an array of real random variables of finite variance, such that for each \( L \) the variables \( (Y_i^{(L)})_i \) are independent. Suppose that \( EY_i^{(L)} = 0 \) for all \( i, L \) and that the variances satisfy

\[
\lim_{L \to \infty} \sum_{i=1}^{b_L} \text{Var} Y_i^{(L)} = 1.
\]

Moreover, assume that the Lindeberg condition holds, i.e. for all \( \delta > 0 \)

\[
\lim_{L \to \infty} \sum_{i=1}^{b_L} E \left( \left( Y_i^{(L)} \right)^2 1_{\{|Y_i^{(L)}| > \delta\}} \right) = 0.
\]

Then we have the following convergence in distribution to the standard normal variable

\[
\sum_{i=1}^{b_L} Y_i^{(L)} \xrightarrow{L \to \infty} \mathcal{N}(0, 1).
\]

**Proof of Proposition 5.1.** We first prove the proposition in the case where for all \( L \in I \) we have \( \frac{\log L}{L} \leq \frac{2}{3} \).

Fix \( L \in I \). For \( i = 1, \ldots, b_L \) denote by \( X_i^{(L)} \) the random variable equal to 1, if \( i \)-th element of the considered random tuple is distinguished, and equal to 0, otherwise. Variables \( (X_i^{(L)})_L \) are independent and \( P(X_i^{(L)} = 1) = \frac{a_L}{c_L} = 1 - P(X_i^{(L)} = 0) = \frac{n_L}{c_L} \).

Next we check that \( \text{Var} X_i^{(L)} = \frac{a_L}{c_L} (1 - \frac{a_L}{c_L}) \). Since \( D_L = \sum_{i=1}^{b_L} X_i^{(L)} \), we have \( ED_L = \frac{a_L b_L}{c_L} \) and \( \text{Var} D_L = \frac{a_L b_L}{c_L} (1 - \frac{a_L}{c_L}) \).

For \( i = 1, \ldots, b_L \) we introduce the following variables

\[
Y_i^{(L)} = \frac{X_i^{(L)} - \frac{a_L}{c_L}}{\sqrt{\text{Var} D_L}}.
\]

We check that they satisfy assumptions of Theorem 5.3. Only Lindeberg condition (3) is non-trivial. Choose any \( \delta > 0 \). As \( X_i^{(L)} \in \{0, 1\} \) and \( \frac{a_L}{c_L} \in [0, 1] \), the absolute value of the numerator in (4) is uniformly bounded by 2. Moreover, \( \frac{a_L b_L}{L} \to \infty \) and \( 1 - \frac{a_L}{c_L} \geq \frac{2}{3} \) so \( \sqrt{\text{Var} D_L} = \sqrt{\frac{a_L b_L}{c_L} (1 - \frac{a_L}{c_L})} \to \infty \). We conclude that \( |Y_i^{(L)}| \) is uniformly bounded by \( \frac{2}{\sqrt{\text{Var} D_L}} \), which tends to 0 with \( L \to \infty \). It follows that

\[
1_{\{|Y_i^{(L)}| > \delta\}} = 0
\]

with probability 1 for \( L \) large enough and every \( i = 1, \ldots, b_L \), which settles the required Lindeberg condition.

The application of Theorem 5.3 yields now

\[
\sum_{i=1}^{b_L} Y_i^{(L)} \xrightarrow{L \to \infty} \mathcal{N}(0, 1).
\]
We see that

$$
\frac{c_L \sqrt{\text{Var} D_L}}{a_L b_L} = \frac{c_L}{a_L b_L} \sqrt{\frac{a_L b_L}{c_L} (1 - \frac{a_L}{c_L})} = \sqrt{\frac{c_L}{a_L b_L} (1 - \frac{a_L}{c_L})} \to 0
$$

(6)
as \( L \to \infty \), since we assumed that \( \frac{a_L}{c_L} \to 0 \).

Now take any \( \varepsilon > 0 \). The combination of (5) and (6) gives us

$$
\frac{c_L \sqrt{\text{Var} D_L}}{a_L b_L} \sum_{i=1}^{b_L} Y_i^{(L)} \frac{\varepsilon}{L} \to 0,
$$

which implies that

$$
P \left( -\varepsilon \leq \frac{c_L \sqrt{\text{Var} D_L}}{a_L b_L} \sum_{i=1}^{b_L} Y_i^{(L)} \leq \varepsilon \right) \to 1
$$

(7)
as \( L \to \infty \).

Note that

$$
\sum_{i=1}^{b_L} Y_i^{(L)} = \frac{1}{\sqrt{\text{Var} D_L}} \left( D_L - \frac{a_L b_L}{c_L} \right).
$$

(8)

Using (8) and (7), we calculate that

$$
P \left( \left(1 - \frac{a_L b_L}{c_L}\right) \leq D_L \leq \left(1 + \varepsilon\right) \frac{a_L b_L}{c_L} \right)
$$

$$
= P \left( -\varepsilon \frac{a_L b_L}{c_L} \leq \frac{1}{\sqrt{\text{Var} D_L}} \left( D_L - \frac{a_L b_L}{c_L} \right) \leq \varepsilon \frac{a_L b_L}{c_L} \right)
$$

$$
= P \left( -\varepsilon \frac{a_L b_L}{c_L} \leq \sum_{i=1}^{b_L} Y_i^{(L)} \leq \varepsilon \frac{a_L b_L}{c_L} \right)
$$

$$
= P \left( -\varepsilon \frac{c_L \sqrt{\text{Var} D_L}}{a_L b_L} \sum_{i=1}^{b_L} Y_i^{(L)} \leq \varepsilon \right) \to 1
$$
as \( L \to \infty \), which finishes the proof in the case where all \( L \in I \) satisfy \( \frac{c_L}{a_L} \leq \frac{1}{\varepsilon} \).

For the proof in the remaining case, let us define the sets \( I_1 = \{ L \in I | a_L = c_L = 1 \} \), \( I_2 = \{ L \in I | a_L = c_L > 1 \} \) and \( I_3 = I \setminus (I_1 \cup I_2) \).

If \( I_1 \) is infinite, then the equation (1) obviously holds if the limit is taken over \( L \in I_1 \), because for such \( L \) we have \( D_L = b_L \).

If \( I_2 \) is infinite, then for every \( L \in I_2 \) we have \( \frac{c_L}{a_L} \leq \frac{1}{\varepsilon} < \frac{1}{\varepsilon} \), so by the proof of the previous case, with \( I_2 \) in the place of \( I \), we know that the equation (1) holds if the limit is taken over \( L \in I_2 \).

Suppose \( I_3 \) is infinite. For every \( L \in I_3 \), we can write \( a_L = a_{1,L} + a_{2,L} \) for some integer \( a_{1,L}, a_{2,L} \) satisfying \( 0 < \frac{1}{2} a_L \leq a_{1,L} \leq \frac{2}{3} a_L \leq \frac{2}{3} c_L \) for \( i = 1, 2 \). Now let us for every such \( L \) divide the set of distinguished elements of \( R_L \) arbitrarily into two disjoint subsets \( A_{1,L}, A_{2,L} \) of cardinalities, respectively, \( a_{1,L}, a_{2,L} \).

Let \( i \in \{1, 2\} \). Define \( D_{i,L} \) to be the random variable obtained in the same experiment as original \( D_L \), denoting the number of entries of the resulting random \( b_L \)-tuple belonging to \( A_{i,L} \). Of course, \( D_L = D_{1,L} + D_{2,L} \). Moreover, since \( \frac{1}{2} a_L \leq a_{1,L} \), we know that \( \frac{a_{1,L} b_L}{c_L} \to \infty \) when \( L \to \infty \) over \( L \in I_3 \). The assumptions of the proposition we are now proving are thus satisfied when we substitute \( I \) with \( I_3 \), \( a_L \) with \( a_{1,L} \). Moreover, since \( \frac{3}{2} \frac{a_L}{c_L} \leq \frac{3}{2} \), we have already proved the proposition in that case, so we know that

$$
\lim_{L \to \infty} P \left( \left(1 - \varepsilon\right) \frac{a_{1,L} b_L}{c_L} \leq D_{i,L} \leq \left(1 + \varepsilon\right) \frac{a_{1,L} b_L}{c_L} \right) = 1
$$

(9)
where the limit is taken over $L \in I_3$.

Since the limits (9) for $i = 1, 2$ assert that probabilities of two events tend to 1, their intersection has the same property. By adding the sides of both inequalities, we get the following.

$$\lim_{L \to \infty} P \left( (1 - \varepsilon) \left( \frac{(a_{1,L} + a_{2,L})b_L}{c_L} \right) \leq D_{1,L} + D_{2,L} \leq (1 + \varepsilon) \left( \frac{(a_{1,L} + a_{2,L})b_L}{c_L} \right) \right) = 1,$$

where the limit is taken over $L \in I_3$.

We know thus for every $1 \leq j \leq 3$, that if $I_j$ is infinite, then equality (1) holds if the limit is taken over $L \in I_j$. As $I = I_1 \cup I_2 \cup I_3$, it means that the equality holds, when we take the limit over $L \in I$.

References

[1] Botto Mura, R., Rhemtulla, A.: Orderable groups. Lecture Notes in Pure and Applied Mathematics, Vol. 27. Marcel Dekker, New York-Basel (1977)

[2] Dahmani, F., Guirardel, V., Przytycki, P.: Random groups do not split. In: Mathematische Annalen 349(3), pp. 657-673 (2011)

[3] Gromov, M.: Asymptotic invariants of infinite groups. In: Geometric Group Theory, vol. 2 (Sussex, 1991). London Mathematical Society Lecture Note Series, vol. 182, pp. 1-295. Cambridge University Press, Cambridge (1993)

[4] Kallenberg, O.: Foundations of Modern Probability, 2nd ed. Springer Series in Statistics (2002)

[5] Ollivier, Y.: Sharp phase transition theorems for hyperbolicity of random groups. In: Geom. Funct. Anal. 14(3), 595-679 (2004)

[6] Ollivier, Y.: A January 2005 invitation to random groups. In: Ensaios Matemáticos (Mathematical Surveys), vol. 10. Sociedade Brasileira de Matemática, Rio de Janeiro (2005)