On two distributions of subgroups of free groups *

Frédérique Bassino [†]   Armando Martino [‡]   Cyril Nicaud [§]   Enric Ventura [¶]

Pascal Weil [‖]

Abstract

We study and compare two natural distributions of finitely generated subgroups of free groups. One is based on the random generation of tuples of reduced words; that is the one classically used by group theorists. The other relies on Stallings' graphical representation of subgroups and in spite of its naturality, it was only recently considered. The combinatorial structures underlying both distributions are studied in this paper with methods of analytic combinatorics. We use these methods to point out the differences between these distributions. It is particularly interesting that certain important properties of subgroups that are generic in one distribution, turn out to be negligible in the other.

1   Introduction

Algorithmic problems in combinatorial group theory have evoked a lot of interest in recent years, especially in free groups and this has led naturally to an interest in the evaluation of these algorithms and to enumeration problems. This trend has encountered another rising interest in group theory for the statistical properties of elements and subgroups of free groups. This type of investigation was pioneered by Ol'shanskiĭ [16] and Arjantseva [2, 1], who centered their work on the statistical properties of finite presentations of groups, that is, largely, of finitely generated normal subgroups of free groups, see Section 4.3 for more details.

More recently, the search for innovative group-based

cryptographic systems (see [12] for instance) has led to the investigation of the statistical properties of finitely generated subgroups of free groups, see [10, 7].

In both cases, the implicit distribution was that given by the random choice of a k-tuple (k fixed) of reduced words of length at most n, with n allowed to tend to infinity. The cited literature concentrated on the identification of generic (resp. negligible) properties: properties satisfied by a proportion p_n of k-tuples of words of length at most n, such that $\lim p_n = 1$ (resp. 0), see Section 2.4.

Bassino, Nicaud and Weil [3] explored another quite natural distribution of finitely generated subgroups of free groups. As it turns out, these subgroups are uniquely represented by a finite labeled graph, subject to certain combinatorial constraints (see Section 2.2).

Both distributions are amenable to methods from analytic combinatorics. The word-based distribution can conveniently be studied using analytic results on texts generated by Markov chains, as done in [13]. On the other hand, properties of subgroups under the graph-based distribution are directly related to properties of partial injections on $[n] = \{1, \cdots, n\}$. This properties are obtained using saddle point technics mainly. The general framework is the following: Given a property on subgroups, find necessary or sufficient conditions for this property to be satisfied, then use analytic tools to prove negligibility or genericity. Pleasantly, the questions raised are familiar to combinatorists. For instance, we have to estimate asymptotically the expected size of the domain of a random injection, the probability that a partial injection has no cycle in its functional graph, *etc.* We thus apply to algebra the same technics that were mostly developed for computer science.

Not surprisingly, the consideration of a different distribution sheds a different light on the properties of subgroups that are generic or negligible (i.e., frequent or rare). For instance, we show that an important property like malnormality (see Section 4.1), which is known to be generic in the word-based distribution, is instead negligible in the graph-based distribution.

The paper is organized as follows. In Section 2, basic algebraic definitions are recalled as well as the no-

[†] LIPN UMR 7030, Université Paris 13 et CNRS, 93430 Villetaneuse, France. email: bassino@lipn.univ-paris13.fr

[‡] School of Mathematics, University of Southampton, SO17 1BJ, United Kingdom. email: A.Martino@upc.soton.ac.uk

[§] LIGM, UMR 8049, Université Paris-Est et CNRS, 77454 Marne-la-Vallée, France. email: nicaud@univ-mlv.fr

[¶] Universitat Politecnica de Catalunya, 08240 Manresa, Catalunya, Spain. email: enric.ventura@upc.edu

[‖] LaBRI, UMR 5800, Université de Bordeaux et CNRS, 33400 Talence, France. email: pascal.weil@labri.fr

tions of negligibility and genericity. In Section 3, we present the two distributions, emphasing their combinatorial properties. In Section 4 we analyze three properties of subgroups. First, we show that though generic for the word-based distribution, malnormality is negligible for the graph-based distribution. Then, we present a property that is *intermediate* for the graph-based distribution, that is, neither negligible nor generic. Finally we discard the idea of generating finitely presented groups using the graph-based distribution, by proving that this representation is generically trivial. This is proved using the fact that generically the lengths of the cycles in a size n permutation are relatively prime.
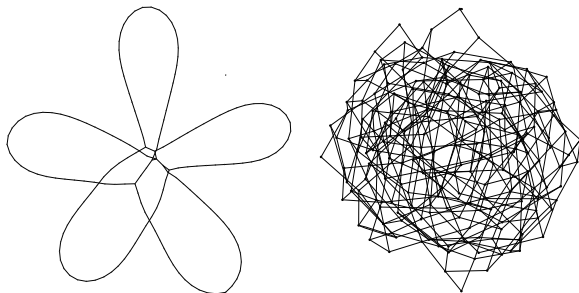

Figure 1: Two randomly generated subgroups of $F(\{a, b\})$ depicted by their graphical representation. On the left, a random subgroup for the word-based distribution with 5 words of lengths at most 40. On the right, a random subgroup with 200 vertices for the graph-based distribution. Only the shape of the graph is depicted, edges' labels and directions are not represented. The pictures have been generated by `neato`. Note that the scale (average distance between two vertices) is not the same on the two pictures. The graphical representation of a subgroup is defined in Section 2.2.

2 Definitions

2.1 Free groups and reduced words Let A be a non-empty set. We consider words on the alphabet $A \sqcup A^{-1}$, the disjoint union of A and A^{-1}, the alphabet made of formal inverses of the elements of A: $A^{-1} = \{a^{-1} \mid a \in A\}$. By convention, $(a^{-1})^{-1} = a$ for any $a \in A$. A word written on the alphabet $A \sqcup A^{-1}$ is *reduced* when it does not contain the pattern aa^{-1}, for any $a \in A \sqcup A^{-1}$. For instance for $A = \{a, b\}$, $aab^{-1}b^{-1}ab^{-1}a^{-1}$ is reduced, but $aabb^{-1}a^{-1}$ is not. If a word is not reduced, one can *reduce* it by iteratively removing every pattern of the form aa^{-1}. The resulting reduced word is uniquely determined: it does not depend on the order of the cancellations. For instance, $u = aabb^{-1}a^{-1}$ reduces to aaa^{-1}, and thence to a.

The set $F(A)$ of reduced words is naturally equipped with a structure of group, where the product $u \cdot v$ is the (reduced) word obtained by reducing the concatenation uv. This group is called the *free group* on A. More generally, every group isomorphic to $F(A)$, say, $G = \varphi(F(A))$ where φ is an isomorphism, is said to be a free group, freely generated by $\varphi(A)$. The set $\varphi(A)$ is called a *basis* of G. It is important to note that $F(A)$ has infinitely many bases: A is always a basis, but each set $\{a^n ba^m, a\}$ is one as well (if $A = \{a, b\}$). The *rank* of $F(A)$ (or of any isomorphic free group) is $|A|$, and one shows that this notion is well-defined in the following sense: free groups $F(A)$ and $F(B)$ are isomorphic if and only if $|A| = |B|$. If $r \geq 1$, we will denote by F_r a free group of rank r.

A group G is *generated* by a subset X if every element of G can be written as a product of elements of X and their inverses. It is *finitely generated* if it admits a finite set X of generators. In this paper, we are interested especially in the finitely generated subgroups of finite rank (*i.e.*, finitely generated) free groups. Recall that every subgroup of a free group is free (Nielsen-Schreier theorem), but that the rank of a subgroup may well be greater than that of the group: F_2 has subgroups of every finite rank.

2.2 Graphical representation Each finitely generated subgroup of F can be represented uniquely by a finite graph of a particular type, by means of the technique known as *Stallings foldings* [17] (see also [19, 9, 18]). This construction is informally described in Section 2.3.

An *A-graph* is defined to be a pair $\Gamma = (V, E)$ with $E \subseteq V \times A \times V$, such that

- if $(u, a, v), (u, a, v') \in E$, then $v = v'$;
- if $(u, a, v), (u', a, v) \in E$, then $u = u'$.

The elements of V are called the *vertices* of Γ, the elements of E are its *edges*, and we sometimes write $V(\Gamma)$ for V and $E(\Gamma)$ for E. We say that Γ is *connected* if the underlying undirected graph is connected. If $v \in V(\Gamma)$, we say that v is a *leaf* if v occurs at most once in (the list of triples defining) $E(\Gamma)$ and we say that Γ is *v-trim* if no vertex $w \neq v$ is a leaf. Note that v is not necessarily a leaf. Finally we say that the pair (Γ, v) is *admissible* if Γ is a v-trim and connected A-graph. Then it is known that:

- Stallings foldings associate with each finitely generated subgroup H of $F(A)$ a unique admissible pair of the form $(\Gamma, 1)$, which we call the *graphical representation* or the *Stallings graph* of H [17, 19, 9].
- every admissible pair $(\Gamma, 1)$ is the graphical representation of a unique finitely generated subgroup of

$F(A)$ [17, 19, 9];

- if $(\Gamma, 1)$ is the graphical representation of H, then $\mathsf{rank}(H) = |E(\Gamma)| - |V(\Gamma)| + 1$ [17, 19, 9];

The admissible pair $(\Gamma, 1)$ can be seen as a finite state machine that represents the subgroup H. It is very similar to finite state automata representing regular languages. To know whether a reduced word u is in H, start from vertex 1, then follow a path in the graph by reading u letter by letter: follow an edge (p, a, q) from vertex p to vertex q when reading letter $a \in A$, and follow an edge (p, a, q) backward, from vertex q to vertex p, when reading letter $a^{-1} \in A^{-1}$. From admissibility conditions, there is at most one such path for u. The reduced word u is in H if and only if the path exists and ends in 1. Hence, $(\Gamma, 1)$ is a kind of finite state automaton, which is deterministic and co-deterministic, having 1 both as initial state and unique final state, and such that one can use a transition backward while reading the inverse of a letter. Admissible pairs play a role analogous to that of minimal automata in language theory.

2.3 Stallings foldings We now present informally the computation of the graphical representation of a subgroup generated by a subset $B = \{u_1, \cdots, u_k\}$. It consists in building an $(A \sqcup A^{-1})$-graph, changing it into a A-graph, then reducing it using *foldings*. First build a vertex 1. Then, for every word u of length n in B, build a loop with label u from 1 to 1, adding $n - 1$ vertices. Change every edge (u, a^{-1}, v) labeled by a letter of A^{-1} into an edge (v, a, u). Iteratively identify the vertices v and w whenever there exists a vertex u and a letter $a \in A$ such that either both (u, a, v) and (u, a, w) or both (v, a, u) and (w, a, u) are edges in the graph (the corresponding pair of edges are folded, in Stallings's terminology).

The resulting graph Γ is such that $(\Gamma, 1)$ is admissible and, very much like in the (1-dimensional) reduction of words, it does not depend on the order used to perform the foldings. An example is depicted on Figure 2.

2.4 Genericity and negligibility Let S be a countable set, the disjoint union of finite sets S_n ($n \geq 0$), and let $B_n = \bigcup_{i \leq n} S_i$. Typically in this paper, S will be the set of Stallings graphs, of partial injections, of reduced words or of k-tuples of reduced words, and S_n will be the set of elements of S of size n.

A subset X of S is *negligible* (resp. *generic*) if the probability for an element of B_n to be in X, tends to 0 (resp. to 1) when n tends to infinity; that is, if $\lim_n \frac{|X \cap B_n|}{|B_n|} = 0$ (resp. $= 1$).
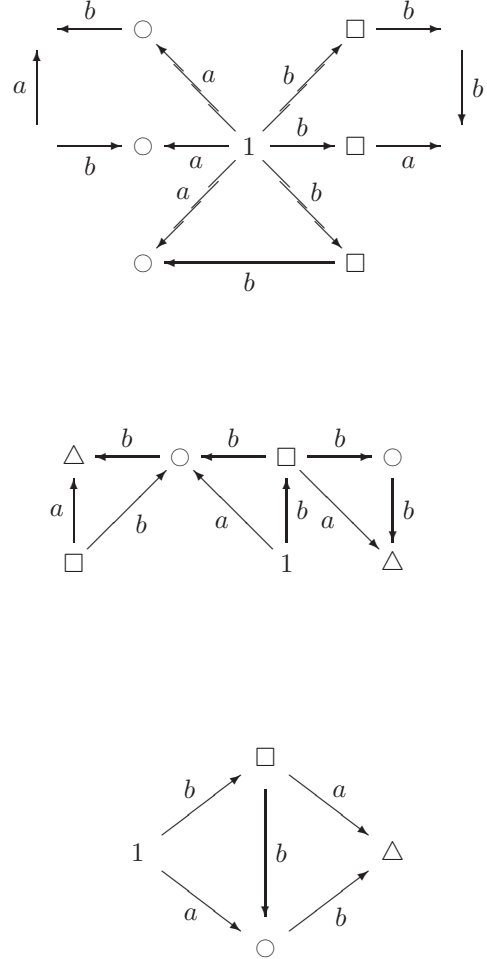
Much of the literature is also concerned with *expo-*

Figure 2: Some steps of the computation of the Stallings graph for $B = \{b^3 a^{-1} b^{-1}, aba^{-1}ba^{-1}, b^2 a^{-1}\}$.

nential negligibility or genericity, when the ratio $\frac{|X \cap B_n|}{|B_n|}$ tends to 0 or 1 exponentially fast.

The definition of negligibility and genericity above is given in terms of the balls B_n: the sets of elements of size at most n. It is sometimes more expedient to reason in terms of the proportion of elements of X in the spheres S_n. This is possible if the structures under consideration grow fast enough as stated in the following proposition.

PROPOSITION 2.1. *If* $\lim \frac{B_n}{B_{2n}} = 0$ *and* $\lim_n \frac{|X \cap S_n|}{|S_n|} = 0$ *(resp.* $= 1$*) then* X *is negligible (resp. generic). The same result holds for exponential negligibility and genericity.*

Naturally, the negligibility or the genericity of a subset X of S depends on the layering of S into the S_n, that is, on the measure used for the size of an element of S. The main focus of the article is to compare the distributions coming from two natural choices for the size of a finitely generated subgroup of a free group.

2.5 Saddle point asymptotics Several results in the following are obtained making use of the saddle point method, a powerful method to find asymptotic estimates of the coefficients of analytic functions which exhibit exponential-type growth in the neighborhood of their singularities. We refer the reader to the book by Flajolet and Sedgewick [4, Chap. VIII], and to the survey by Odlyzko [15] for a thorough presentation of saddle point analysis. Let us indicate here the main theorem we will use, Theorem 2.1 below. This result requires a particular property of analytic functions, called H-admissibility [4, Section VIII.5], which we briefly describe.

Let $f(z)$ be a function that is analytic at the origin, with radius of convergence ρ, positive on $]0, \rho[$. Put $f(z)$ into its exponential form $f(z) = e^{h(z)}$ and let

$$a(r) = rh'(r) \quad \text{and} \quad b(r) = r^2 h''(r) + rh'(r).$$

The function $f(z)$ is said to be *H-admissible* if there exists a function $\delta \colon]0, \rho[\longrightarrow]0, \pi[$ such that the following three conditions hold:

(H1) $\lim_{r \to \rho} b(r) = +\infty$.

(H2) Uniformly for $|\theta| \le \delta(r)$

$$f(re^{i\theta}) \sim f(r)e^{i\theta a(r) - \frac{1}{2}\theta^2 b(r)} \quad \text{when } r \text{ tends to } \rho.$$

[That is, $f(re^{i\theta}) = f(r)e^{i\theta a(r) - \frac{1}{2}\theta^2 b(r)}(1 + \gamma(r, \theta))$ with $|\gamma(r, \theta)| \le \tilde{\gamma}(r)$ when $|\theta| < \delta(r)$ and $\lim_{r \to \rho} \tilde{\gamma}(r) = 0$.]

(H3) and uniformly for $\delta(r) \le |\theta| \le \pi$

$$f(re^{i\theta})\sqrt{b(r)} = o(f(r)) \qquad \text{when } r \text{ tends to } \rho.$$

THEOREM 2.1. *Let* $f(z) = e^{h(z)}$ *be a H-admissible function and* $\zeta = \zeta(n)$ *be the unique solution in the interval* $]0, \rho[$ *of the saddle point equation*

$$\zeta \frac{f'(\zeta)}{f(\zeta)} = n.$$

Then

$$[z^n]f(z) = \frac{f(\zeta)}{\zeta^n \sqrt{2\pi b(\zeta)}} (1 + o(1)).$$

where $b(z) = z^2 h''(z) + z h'(z)$ *and* $h(z) = \log f(z)$.

3 Two natural distributions

In this section, we describe the basic properties of a word-based and a graph-based distribution of subgroups of free groups, from the point of view of a combinatorist. The word-based distribution is based on the distribution of tuples of generators, whereas the graph-based distribution exploits the graphical representation of subgroups. In the following, A is a fixed alphabet of size $r \ge 2$.

3.1 Word-based The main distribution considered in the literature is the word-based distribution, see [2, 1, 7, 10] for instance. For a fixed $k \ge 1$ and for any $n \in \mathbb{N}$, the set B_n consists of all k-tuples $(u_1, \cdots, u_k)$ of reduced words of length at most n. The word-based distribution is, for any n, the uniform distribution on B_n.

A reduced word of length n can be built in the following way: starting from any letter in $A \sqcup A^{-1}$, build it from left to right by adding a letter different from the former one's inverse. Hence, if R_n denotes the set of reduced words of length n, $|R_n| = 2r(2r-1)^{n-1}$ for $n \ge 1$ and $|R_0| = 1$. The set of reduced words is in bijection with Smirnov words on an alphabet of size $2r$, the words which have no consecutive equal letters [6, 4]. Reduced words can also be seen as paths of length n in a Markov chain with $2r$ states. Each state corresponds to the last produced letter, and from a state $a \in A \sqcup A^{-1}$, the probability to go to any other state but a^{-1} is $\frac{1}{2r-1}$. This Markov chain is primitive, therefore the results obtained in [13] can be applied to this model: for any pattern given by a non-degenerated regular expression, the number of occurrences of the pattern in a random reduced word of length n is asymptotically Gaussian, with mean and variance growing linearly; a local limit and large deviation bounds also hold. Large deviation bounds are of great interest here, as they often yield exponential genericity or negligibility.

In the literature, the computations are done either using elementary calculus, as $|R_n|$ has a simple expression, or using some large deviation results from probabilistic approaches. For instance, one can directly prove that each word in a random k-tuple of B_n is generically of length at least $n - f(n)$, for any $f(n)$ that tends to infinity. One important statement is that if the construction of Section 2.3 is applied to a random element of S_n, the resulting graph has exponentially generically more than $(1 - \varepsilon)kn$ vertices, for any $\varepsilon \in]0, 1[$ and the subgroup is exponentially generically of rank k. These results are proved in [7] and come from the fact that the folding phase takes only few steps, as two long reduced words only have small common prefixes or suffixes. Hence the graph is generically made of a small heart that has the shape of a tree around 1, with $2k$ leaves, and k long loops, each loop joining two leaves of the heart. The subgroup generated by a random 5-tuple of words of length at most 40 shown in Figure 1 is representative of this behavior.

3.2 Graph-based The uniform distribution on the set of size n Stallings graphs was analyzed by Bassino, Nicaud and Weil [3]. Here we summarize the principles of this distribution and some of its features, which will be used in this paper.

Let $(\Gamma, 1)$ be an admissible pair, Γ having n vertices. For every letter $a \in A$, consider the partial function f_a from V to V defined by $f_a(u) = v$ when (u, a, v) is an edge of Γ. The function is correctly defined as the foldings ensure that there are not two edges (u, a, v) and (u, a, w) with $v \neq w$. For the same reason, f_a is a partial injection: if $f_a(u) = f_a(v)$ then $u = v$. Therefore an admissible pair can be seen as a A-tuple $(f_a)_{a \in A}$ of partial injections on an n-element set, with a distinguished vertex, and such that the resulting graph (with an a-labeled edge from i to j if and only $j = f_a(i)$) is connected and has no leaf, except perhaps the origin. We may even assume that the considered n-element set is $[n] = \{1, \dots, n\}$, with 1 as the distinguished vertex, as there are no symmetry in the structure and therefore exactly $(n - 1)!$ ways to label the vertices with $[n]$, keeping 1 as distinguished vertex (see [3, Section 1.2] for details).

One shows [3, Corollary 2.7] that the probability that an A-tuple $(f_a)_{a \in A}$ of partial injections on $[n]$ induces a Stallings graph tends to 1 as n tends to infinity, and the problem of randomly generating a Stallings graph then reduces (via an efficient rejection algorithm, see [3, Section 3]) to the problem of efficiently generating a random partial injection on $[n]$.

The connected components of the functional graph of a partial injection are either cycles or nonempty

sequences, hence if I_n denotes the number of size n partial injections and $I(z)$ denotes the *exponential generating function* (EGF) of partial injections, namely $I(z) = \sum_{n \geq 0} \frac{I_n}{n!} z^n$, the following statement holds [3, Section 2.1 and Proposition 2.10].

PROPOSITION 3.1. *The EGF $I(z)$ of partial injections satisfies the following*

$$I(z) = \frac{1}{1 - z} \exp\left(\frac{z}{1 - z}\right)$$

and

$$\frac{I_n}{n!} = \frac{e^{-\frac{1}{2}}}{2\sqrt{\pi}} e^{2\sqrt{n}} n^{-\frac{1}{4}} (1 + o(1)).$$

The proof consists in verifying that $I(z)$ is H-admissible, and therefore amenable to saddle point methods. Note that $I(z)$ is in [4] as the exponential generating function of tagged permutations, and used to count the mean number of subsequences in a random permutation.

The random generator is directly computed from the specification of the set of partial injections as sets of cycles and nonempty sequences, using the recursive method [14, 5]. The specific nature of the problem provides a linear complexity for the precalculus of the I_n and for each random generation [3, Section 3.3].

Let $\mathsf{sequence}(f)$ be the number of sequences of the partial injection f. The following was established in [3, Lemma 2.11 and Corollary 4.1], using a bivariate exponential generating function and saddle point methods again.

PROPOSITION 3.2. *The expected number of sequences in a randomly chosen partial injection of size n is asymptotically equivalent to $\sqrt{n}$.*

The expected rank of a randomly chosen size n subgroup of F_r is asymptotically equivalent to $(r-1)n - r\sqrt{n}$.

If the partial injections constituting a Stallings graph have relatively few sequences, then the graph has relatively more edges: this is captured in the statement above on the expected rank of a randomly chosen subgroup, and it is illustrated by the randomly generated Stallings graph with 200 vertices shown in Figure 1.

Another consequence of Proposition 3.2 is that the expected size of the domain of a size n partial injection is $n - \sqrt{n} + o(\sqrt{n})$.

4 Generic and negligible properties of subgroups

The two distributions we described are very different. The word-based distribution is governed by two parameters – the number of generators and their length, the

latter being allowed to tend to infinity –; and the graph-based distribution is governed by a single parameter – the size of the Stallings graph. Yet both allow the discussion of properties of subgroups (of subgroups of a fixed rank k in the word-based case). There is of course no reason why a property that is generic or negligible in one distribution should have the same property in the other.

This is trivially true for the property *to have rank* ℓ, for a fixed integer $\ell \geq 1$. In the graph-based distribution, this property is negligible: this can be deduced from Proposition 3.2, see [3, Corollary 4.2]. In contrast, this property is exponentially generic in the word-based distribution *of ℓ-generated* subgroups, as already stated in Section 3.1.

4.1 Malnormal subgroups A subgroup H is malnormal if $g^{-1}Hg \cap H = 1$ for every $g \notin H$. Malnormal subgroups of free groups have received a lot of attention in group-theoretic literature, in particular because of their connection with hyperbolicity: Kharlampovich and Myasnikov showed that the amalgamated products of free groups F_r and F_s over a finitely generated subgroup H is hyperbolic if and only either H is malnormal in F_r or H is malnormal in F_s [11]. Finitely generated malnormal subgroups of free groups have a nice graphical characterization in terms of multiple occurrences of loops in their Stallings graph [8] (whereas malnormality is undecidable in hyperbolic groups).

PROPOSITION 4.1. *Let $(\Gamma, 1)$ be the graphical representation of a subgroup H. Then H is non-malnormal if and only if there exists a non-trivial reduced word u and distinct vertices $x \neq y$ such that u labels loops at x and at y.*

For the word-based distribution, Jitsukawa shows the following [7, Theorem 4 and Lemma 6].

PROPOSITION 4.2. (WORD-BASED DISTRIBUTION) *Malnormality is generic in the word-based distribution.*

The proof relies on the fact that generically, given a k-tuple $(u_1, \ldots, u_k)$ of reduced words, only short words have several occurrences as factors in the u_i and u_i^{-1}.

In contrast, we show that malnormality is generically negligible in the graph-based distribution (see Theorem 4.1 below). For this purpose, we first consider partial injections that have no cycles, the so-called *fragmented permutations*, see [4, Section II.4.2]. Let J_n be the number of size n fragmented permutations and let $J(z) = \sum_n \frac{J_n}{n!} z^n$ be the corresponding EGF. This series is studied in detail in [4, Example VIII.7, Proposition

VIII.4]. There, it is shown in particular that

$$J(z) = \exp\left(\frac{z}{1-z}\right)$$

and

$$\frac{J_n}{n!} = \frac{e^{-\frac{1}{2}}}{2\sqrt{\pi}} e^{2\sqrt{n}} n^{-\frac{3}{4}} (1 + o(1)).$$

The comparison with the asymptotic equivalent for $\frac{I_n}{n!}$ in Proposition 3.1, immediately yields the following statement.

PROPOSITION 4.3. *The probability that a size n partial injection is a fragmented permutation is equivalent to $\frac{1}{\sqrt{n}}$.*

We now consider partial injections with a single cycle, which has size 1. Standard technics and the asymptotic equivalents of J_n and I_n lead to the following proposition.

PROPOSITION 4.4. *The probability that a random partial injection of size n has a single cycle, and that cycle is a singleton, is asymptotically equivalent to $\frac{1}{\sqrt{n}}$.*

We can now state our result on malnormality.

THEOREM 4.1. (GRAPH-BASED DISTRIBUTION) *The probability that a random subgroup of size n is malnormal is $\mathcal{O}(n^{-\frac{r}{2}})$.*

To prove Theorem 4.1, first note that if $(\Gamma, 1)$ is the admissible pair of a malnormal subgroup, then for any letter $a \in A$, the partial injection f_a can either have no cycles, or only one cycle, of size one. This a consequence of Proposition 4.1. The negligibility then follows from Propositions 4.3 and 4.4.

4.2 An intermediate property In this section, we discuss an *intermediate* property of subgroups, that is, a property such that the proportion of subgroups of size n with this property has a limit which is neither 0 nor 1 (respectively the negligible and the generic cases). Recall that the conjugates of an element x are all the elements of the form gxg^{-1}. The intermediate property we identify concerns the presence of conjugates of the letters in a given subgroup.

THEOREM 4.2. *The probability that a size n subgroup of F_r contains no conjugate of the letters in A tends to e^{-r} when n tends to infinity.*

Note that the property is exponentially negligible in the word-based distribution.

It is easily verified that a subgroup H contains a conjugate of letter $a \in A$ if and only if a labels a loop at some vertex of $\Gamma(H)$, that is, if and only if the corresponding partial injection has a fixpoint. Since the drawing of the partial injections corresponding to the r different letters is independent, the theorem follows directly from the following proposition.

PROPOSITION 4.5. *The probability that a size n partial injection has no fixpoint tends to $\frac{1}{e}$ when n tends to infinity.*

The sketch of the proof of Proposition 4.5 is the following. Using the symbolic method, the EGF of partial injections with no fixed point is $L(z) = e^{-z}I(z)$. Basic computations prove that $L(z)$ is H-admissible, and saddle point asymptotics give:

$$[z^n]L(z) \sim \frac{e^{-3/2}}{2\sqrt{\pi}}n^{-1/4}e^{2\sqrt{n}}$$

4.3 Finitely presented groups One of the motivations for the study of subgroup distributions has been the investigation of the statistical properties of *finitely presented groups*, see [2, 1, 16]. Strictly speaking, this would require a notion of distribution of these groups, so that one would make a list of non-isomorphic groups and investigate the frequency of groups with certain properties within that list. No such notion is available, as far as the authors are aware and current literature operates rather with a notion of distribution of finite *presentations*.

Recall that a *finite presentation* is a pair (A, R), where A is a finite set (the alphabet of generators) and R is a tuple of elements of $F(A)$ (the relators). The resulting finitely presented group G, written $G = \langle A \mid R \rangle$, is the quotient $G = F(A)/N(R)$, where $N(R)$ is the *normal subgroup generated* by R (that is: the least normal subgroup containing R).

This is the traditional approach of finite presentations, choosing a k-tuple of relators of length at most n and letting n grow to infinity, that has been used to discuss the statistical properties of finitely presented groups. The idea we want to discuss in this section, may seem reasonable in this context, but it turns out to be disappointing. If H is the subgroup generated by the tuple of relators R, then $N(R) = N(H)$, so the group $G = \langle A \mid R \rangle$ is also specified by the pair (A, H). We propose to consider finite presentations in this form, a pair of an alphabet and a finitely generated subgroup H, and to investigate statistical properties based on the distribution of the graphical representations of subgroups.

It is known that if A and k are fixed and if the maximal length n of the relators tends to infinity, then generically $G = \langle A \mid R \rangle$ is infinite; more strongly,

it is such that every subgroup generated by $|A| - 1$ elements is free [2]. It is also known that G is generically hyperbolic (Ol'shanskii [16], proving a statement of Gromov).

Unfortunately, the graph-based approach to presentations fails at this step, in the sense that it presents generically the trivial group.

THEOREM 4.3. *Generically, the finitely presented group $\langle A \mid H \rangle$ is trivial. Equivalently, generically, the normal closure of a finitely generated subgroup of F_r is F_r itself.*

To prove Theorem 4.3, we first use elementary algebraic considerations to establish that, if for every letter a, the lengths of the cycles of the partial injection induced by letter a in $\Gamma(H)$ are relatively prime, then the finitely presented group $\langle A \mid H \rangle$ is trivial. Thus it suffices to prove the following proposition.

PROPOSITION 4.6. *Generically, the lengths of the cycles of a size n partial injection are relatively prime.*

We start with the case of permutations, which is interesting by itself. Observe that if the lengths of the cycles of a permutation are not relatively prime, then these lengths have a common prime divisor p, which is in particular a divisor of n. The following lemma is proved by induction on n, by partitioning the size n permutations in which all the cycles have size a multiple of p according to the size of the cycle that contains 1.

LEMMA 4.1. *Let $n \geq 2$ and let p be a prime divisor of n. The number of size n permutations in which all the cycles have size a multiple of p is at most $2n! \, n^{\frac{1}{p}-1}$.*

Proposition 4.7 is obtained from Lemma 4.1, bounding above by $\log_3 n$ the number of prime divisors of n that are greater than or equal to 3.

PROPOSITION 4.7. *Let $n \geq 2$. The probability that the lengths of the cycles of a size n permutation are not relatively prime is at most $2n^{-1/2} + 2n^{-1/3}\log_3 n$.*

Note that a better estimation can be obtained using singularity analysis and more precisely uniform bounds in Transfer Theorem, but the asymptotic equivalent must somehow depends on the smallest non-trivial divisor of n. As stated, the result of Proposition 4.7 is sufficient for the purpose of this article.

To prove Proposition 4.6 observe that isolating the cycles in a size n partial injection, reveals a permutation (on a subset X of $[n]$) and a fragmented permutation (i.e., a cycle-less partial injection) on the complement of X. Moreover, taking uniformly at random a size n partial injection having a size k permutation, and keeping

only the permutation part, one obtain a size k permutation uniformly at random (after renormalization of the labels). Computations show that the permutation part of a size n partial injection has size at most $n^{1/3}$ with probability bounded above by $n^{-1/6}$. Then by Proposition 4.7, the probability that the lengths of the cycles of a size n partial injection are not relatively prime is proved to be in $\mathcal{O}(n^{-1/6})$, concluding the proof.

References

[1] Goulnara N. Arzhantseva. A property of subgroups of infinite index in a free group. *Proc. Amer. Math. Soc.*, 128(11):3205–3210, 2000.

[2] Goulnara N. Arzhantseva and Alexander Yu. Ol′shanskiĭ. Generality of the class of groups in which subgroups with a lesser number of generators are free. *Mat. Zametki*, 59(4):489–496, 638, 1996.

[3] Frédérique Bassino, Cyril Nicaud, and Pascal Weil. Random generation of finitely generated subgroups of a free group. *Internat. J. Algebra Comput.*, 18(2):375–405, 2008.

[4] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. Cambridge University Press, 2009.

[5] Philippe Flajolet, Paul Zimmermann, and Bernard Van Cutsem. A calculus for the random generation of labelled combinatorial structures. *Theor. Comput. Sci.*, 132(2):1–35, 1994.

[6] Ian P. Goulden and David M. Jackson. *Combinatorial Enumeration*. John Wiley, New York, 1983.

[7] Toshiaki Jitsukawa. Malnormal subgroups of free groups. In *Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001)*, volume 298 of *Contemp. Math.*, pages 83–95. Amer. Math. Soc., Providence, RI, 2002.

[8] Ilya Kapovich and Alexei Myasnikov. Stallings foldings and subgroups of free groups. *J. Algebra*, 248(2):608–668, 2002.

[9] Ilya Kapovich, Alexey Myasnikov, and Toshiaki Jitsukawa. Stallings foldings and subgroups of free groups. *J. Algebra*, 248:608–668, 2000.

[10] Ilya Kapovich, Paul Schupp, and Vladimir Shpilrain. Generic properties of Whitehead's algorithm and isomorphism rigidity of random one-relator groups. *Pacific J. Math.*, 223(1):113–140, 2006.

[11] Olga Kharlampovich and Alexey Myasnikov. Hyperbolic groups and free constructions. *Trans. Amer. Math. Soc.*, 350:571–613, 1998.

[12] Alexei Myasnikov, Manuel Castellet, Vladimir Shpilrain, and Alexander Ushakov, editors. *Group-based Cryptography*. Advanced Courses in Mathematics - CRM Barcelona [Centre de Recerca Matemàtica]. Bâle ; Boston, Ma : Birkhüser, 2008.

[13] Pierre Nicodème, Bruno Salvy, and Philippe Flajolet. Motif statistics. *Theor. Comput. Sci.*, 287(2):593–617, 2002.

[14] Albert Nijenhuis and Herbert Saul Wilf. *Combinatorial Algorithms*. Academic Press, 1978.

[15] A. M. Odlyzko. *Asymptotic enumeration methods*, volume II, pages 1063–1229. Elsevier, 1995.

[16] A. Yu. Ol′shanskiĭ. Almost every group is hyperbolic. *Internat. J. Algebra Comput.*, 2(1):1–17, 1992.

[17] John Robert Stallings. Topology of finite graphs. *Inventiones Math.*, 71:551–565, 1983.

[18] Nicholas W. M. Touikan. A fast algorithm for Stallings' folding process. *IJAC*, 16(6):1031–1046, 2006.

[19] Pascal Weil. Computing closures of finitely generated subgroups of the free group. *Algorithmic Problems in Groups and Semigroups*, pages 289–307, 2000.