Separability and Randomness in Free Groups

Michal Buran *

Abstract

We prove new separability results about free groups. Namely, if $H_1, \ldots, H_k$ are infinite index, finitely generated subgroups of a non-abelian free group F, then there exists a homomorphism onto some alternating group $f : F \twoheadrightarrow A_m$ such that whenever H_i is not conjugate into H_j, then $f(H_i)$ is not conjugate into $f(H_j)$.

The proof is probabilistic. We count the expected number of fixed points of $f(H_i)$'s and their subgroups under a carefully constructed measure.

Keywords: Free groups, separability, probabilistic method

1 Introduction

Let's say that we want to understand a typical homomorphism between two groups. The simplest domain would be a free group because then the map is specified by its values on generators. The correspondence between the maps and the tuples is bijective, so studying maps from free groups is the same as studying tuples of elements. To make this interesting, we need a family of groups, ideally one which is easy to describe and to work with. In this paper, we take the symmetric groups.

We prove the following theorem and develop a technique to get a range of similar results.

Theorem A. *Suppose $H_1, \ldots, H_k$ are infinite index, finitely generated subgroups of a non-abelian free group F. Then there exists a surjective homomorphism $f : F \longrightarrow A_m$ such that whenever H_i is not conjugate into H_j, then $f(H_i)$ is not conjugate into $f(H_j)$. Moreover, there exists a surjective homomorphism $f' : F \longrightarrow S_{m'}$ with the same property.*

*Supported by ERC starting grant no. 714034 SMART and ERC no. 850956

This theorem gives an alternating version of *conjugacy separability (SCS)* and *subgroup into-conjugacy separability (SICS)* for free groups. These properties allow one respectively to preserve non-conjugacy of two subgroups under passing to a finite quotient and to preserve the property of one subgroup not being conjugate into another. These properties were conceived of by Bogopolski-Grunewald [BG10]. In the same paper they proved these properties for free groups and free products of finite groups [BG10]. Later Bogopolski-Bux proved these properties for surface groups and related them to curvature-type properties [BB14]. Chagas-Zalesskii proved that free-by-finite groups are SCS and property SCS is preserved under free products [CZ15] and that limit groups are SCS [CZ16].

Our theorem generalizes SICS for infinite subgroups to the setting of alternating or symmetric quotient. Indeed if H_1 is not conjugate into H_2, we can make $f(H_1)$ not conjugate into $f(H_2)$, where f is onto an alternating (resp. symmetric) group. It also generalizes SCS. Indeed the relation 'is conjugate into' is antisymmetric on the conjugacy classes of finitely generated subgroups of a free group [BG10, Lemma 2.1] and if finitely generated infinite index subgroups $H_1, H_2 < F$ are not conjugate, then without loss of generality H_1 is not conjugate into H_2 and we can make $f(H_1)$ not conjugate into $f(H_2)$ under some alternating (resp. symmetric) quotient and then $f(H_1)$ and $f(H_2)$ are not conjugate.

Once we build the probabilistic machinery, we can also easily reprove the main theorem from [Wil12], which is the alternating analogue of subgroup separability in the free group. See section 6.

As the size of a symmetric group increases, the probability that two random permutations generate the entire symmetric group or its index 2 alternating subgroup tends to 1. The proof of this fact is much harder than the trivial task of finding a pair of permutations, which generate the symmetric group. However, an explicit construction of quotients becomes trickier, more tedious or potentially unknown as the complexity of desired properties increases. The probabilistic method bypasses this by focusing on statistics of outcome rather than the individual cases.

Random actions of groups have been extensively studied before. For example, Liebeck-Shalev studied random quotients of Fuchsian groups [LS04], walks in finite groups of Lie type [LS05], spans of elements of fixed order in finite simple groups [LS02]. However, our techniques are most similar to how Puder-Parzanchevski counted fixed points of a subgroup of a free group under a random permutation action [PP15]. Probabilistic methods had been used before to prove that for every infinite class $\mathcal{C}$ of simple groups, every non-abelian free group is residually $\mathcal{C}$ [DPSS03, Theorem 3].

People had also asked before in various settings: "What is a typical quotient?"

One can take two random elements [Dix69] or even one restricted element and the other at random [Bab89]. The results of this paper enable us to impose restrictions on both (or all) generators simultaneously.

In Section 2 we say what we mean by these restrictions and state that under mild conditions most of quotients satisfying these restrictions are alternating or symmetric. The next few sections are devoted to the proof of this statement. In Section 3, we prove that the random group is transitive. In Section 4 we prove that it is also primitive. In Section 5 we prove that the random group contains a short cycle and that this together with primitivity proves the theorem.

Section 6 illustrates how to use the results from Section 2 by quickly reproving a known theorem.

In Section 7, we apply the theorem to show new separability properties of free groups. In particular, infinite index, finitely generated non-conjugate subgroups of a free group map to non-conjugate subgroups of an alternating group under some surjective homomorphism onto an alternating group.

2 Set-up

A generalisation of the following theorem allows us to show that certain groups are alternating with a large probability.

Theorem 2.1. *[Dix69] An image of a random homomorphism $F_2 \longrightarrow S_n$ is A_n, resp. S_n, with probabilities which tend to $1/4$, resp. $3/4$, as n goes to infinity.*

We generalise this result to the setting with finitely many conditions on the generators $a_1, \dots a_k$ of F_k. These conditions are given by an immersion of a finite graph into a rose via a correspondence which we now discuss. The basic idea is to start with a graph, which extends to a covering of the presentation complex. We then look at all the ways it extends to a covering.

Definition 2.2 (Schreier graphs)**.** If G is a group and $\mathcal{H} = \{H_i : i \in I\}$ a family of subgroups of G and $\mathcal{A}$ is a collection of elements of G, then *the Schreier graph associated to the subgroups $\mathcal{H}$ and elements $\mathcal{A}$* consists of:

- A vertex for every coset gH_i for every $H_i \in \mathcal{H}$.
- An edge labeled a from the vertex corresponding to gH_i to the vertex corresponding to agH_i for all $a \in \mathcal{A}$ and all cosets of H_i.

In the usual definition of the Schreier graph, there is just one subgroup, but we want to allow for disconnected graphs. We will often omit to specify $\mathcal{H}$ and $\mathcal{A}$, when they're clear from the context.

If $a_1, \dots, a_k$ is a k-tuple of elements in S_n, we can construct a graph encoding their action on $\{1, \dots, n\}$ as follows. Take n vertices labelled $1, \dots, n$ with i and $a_j(i)$ connected by an oriented edge labelled a_j for all i and j. This graph is a (not necessarily connected) covering of *the rose of k petals* R_k, a graph which has a single vertex and k edges labelled $a_1, \dots, a_k$ respectively. The covering has degree n.

Choose an arbitrary basepoint v in each component and take H_v to be the group consisting of labels of closed paths starting at v. Then the above graph is in fact the Schreier graph of $F_k = \langle a_1, \dots, a_k \rangle$ associated to subgroups $\{H_v : v \text{ is a basepoint }\}$ and elements $\{a_1, \dots, a_k\}$.

This gives a bijective correspondence between the degree n coverings of R_k and k-tuples of elements of S_n. To see the other direction, we need the following definition.

Definition 2.3 (Core graph)**.** Given a graph Y, *the core of* Y, denoted $\mathrm{Core}(Y)$ is the subgraph of Y, which consists of all vertices and edges that are contained in some cycle.

Given Γ a subgroup of a free group $F_k = \langle a_1, \dots, a_k \rangle$, let X_Γ be the Schreier graph associated to the subgroup Γ and elements $\langle a_1, \dots, a_k \rangle$. *The core of* Γ, denoted $\mathrm{Core}(\Gamma)$ is the graph $\mathrm{Core}(X_\Gamma)$.

Note that X_Γ is a cover of R_k.

We will also need to talk about subspaces of covers without explicitly referring to the fact that it's a subspace of a cover.

We will in general look at the coverings where the vertices are not labelled. This means that in fact we'll be using the correspondence between unlabelled degree n coverings and conjugacy classes of k-tuples of elements of S_n. We can use this correspondence to define conditions on a random homomorphism from a finitely generated free group to the symmetric group S_n as follows.

Definition 2.4 (Precover, random action)**.** Suppose that G is a labeled oriented graph and $G \longrightarrow R_k$ sends vertices to vertices and edges to the edges of the same label. Such a map is called a *precover* of R_k. Just as a degree n cover corresponds to a permutation $f : [n] \longrightarrow [n]$, a degree n precover corresponds to a partial injective function $f : [n] \nrightarrow [n]$.

Suppose G has at most n vertices. Add vertices to G until there are n vertices in total: let G' be disjoint union of G and a discrete graph with $n - |G|$ vertices.

Let $V_j^{no}(G')$ be the set of vertices of G' without an outgoing edge labelled a_j and $V_j^{ni}(G')$ be the set of the vertices without an incoming edge labelled a_j. For all j, choose a bijection f_j between $V_j^{no}(G')$ and $V_j^{ni}(G')$ uniformly at random. Connect v and $f_j(v)$ by an oriented edge labelled a_j.

The resulting graph $\overline{G}$ is *a random degree n completion* of G, the associated homomorphism $\varphi : F_k \longrightarrow S_n$ is *a random homomorphism with condition G* and the associated group $\Gamma_n(G) \leqslant S_n$ is *a random group with condition G*. Let's call G a *condition graph.*

We frequently take the condition graph to be a core graph, union of core graphs or some slightly larger superspace of a core graph. A core graph of a finitely generated group is a finite graph, since it is a union of only finitely many cycles. Recall from Theorem 2.1 that $\Gamma_n(\emptyset)$ is frequently S_n or A_n. If some component of a graph G is an actual covering of R_2, then $\Gamma_n(G)$ is non-transitive for $n > |G|$. We prove a converse result:

Theorem 2.5 (Main Theorem)**.** *If no component of G is a covering of R_k, then $\Gamma_n(G)$ is S_n or A_n with probabilities which tend to $1 - 2^{-k}$ or 2^{-k} respectively as n goes to infinity.*

3 Transitivity

We need to show that a random group is either S_n or A_n. Both A_n and S_n are transitive, so the transitivity is necessary. It also turns out to be one of the conditions used in the converse statement.

Lemma 3.1 ([Dix69])**.** *The group $\Gamma_n(\emptyset)$ is almost always transitive. (i.e. the probability that $\Gamma_n(\emptyset)$ generates a transitive subgroup of S_n tends to 1 as n goes to infinity).*

If a component of G is an actual covering, then no completion is transitive (except for the case when the component is all of G and there are no other vertices). That component remains a component in any completion. We need to exclude this situation in the generalised version of the theorem.

Lemma 3.2. *Assume that no component of a graph G is a covering of R_k. Then the group $\Gamma_n(G)$ is almost always transitive and a random completion $\overline{G}$ is almost always connected.*

The idea of the proof is as follows. We're starting from something which intuitively is more connected than a discrete graph. We formalise this intuition by constructing a probability preserving map between random completions of $\emptyset$ and random completions of G, which preserves connectedness. We will do this by replacing components of G with discrete graphs.

Proof. Let $G_1, G_2, \ldots, G_l$ be the connected components of G. Let $E_j(G_i)$ be the set of edges labelled a_j in G_i.

- Case 1: The number of edges $|E_j(G_i)|$ labelled a_j in G_i is the same for all j. Let H_i be the discrete graph with $|V(G_i)| - |E(G_i)|/l$ vertices. Let H be the union of all H_i. Pick a bijection between the "missing edges" at vertices of H_i and the "missing edges" at vertices of G_i - see figure 1. This induces a map between random completions. More formally, recall that if G is a graph, then $V_j^{ni}(G)$ and $V_j^{no}(G)$ are the vertices with no incoming and no outgoing edge labelled a_j, respectively. The label a_j appears the same number of times in G_i for all j, so

  $$|V_j^{ni}(G_i)| = |V_j^{no}(G_i)| = |V(G_i)| - |E_j(G_i)| = |V(G_i)| - |E(G_i)|/l$$

  is independent of j, where $E_j(G_i)$ are the edges of G_i with label a_j. The graph H_i is discrete, so we have $|V_j^{ni}(H_i)| = |V(G_i)| - |E(G_i)|/l$. Pick arbitrary bijections $f_{i,j}^{ni} : V_j^{ni}(H_i) \longrightarrow V_j^{ni}(G_i)$. Let f be a union of these bijections. These maps induce a bijection between the degree n completions of H and degree $n + |E_j(G_i)|$ completions of G as follows. Given a completion $\overline{H}$ of H, consider $(\overline{H} \setminus H) \cup G$. Now connect each open end of an edge in $(\overline{H} \setminus H)$, which was previously attached to $v \in H$ to $f(v)$. This is a completion of G. Call it $f(\overline{H})$ by abuse of notation. This correspondence is bijective as now we could excise G and connect the open ends back to H.

  Suppose $f(\overline{H}) = K_1 \sqcup K_2$, where K_i is closed non-empty. For all $v \in H$, the component of G containing $f_{i,j}^{no}(v)$ and $f_{i,j}^{ni}(v)$ does not depend on j. Hence, the closures of $K_i \setminus (G \cap K_i)$ in $\overline{H}$ are two disjoint closed subsets partitioning $\overline{H}$. They are non-empty as long as $K \not\subset G$. This is where we use that no component of G is a cover. If $\overline{H}$ is connected, then so is $f(\overline{H})$.

  The probability that a random completion of H is connected (hence the associated group is transitive) tends to 1 by Lemma 3.1 and therefore the probability that a random completion of G is connected also tends to 1.

- Case 2: Suppose $|E_j(G_i)|$ is not independent of j. We can reduce this situation to case 1, by taking a slightly larger graph G', which satisfies this condition. The key observation will be that most completions of G are also completions of G'.

  If there is some i, j and j' with $|E_j(G_i)| < |E_{j'}(G_i)|$, let v_j be a vertex of G_i with no outgoing edge labelled a_j. Replace G_i by a union of G_i and an a_j-edge

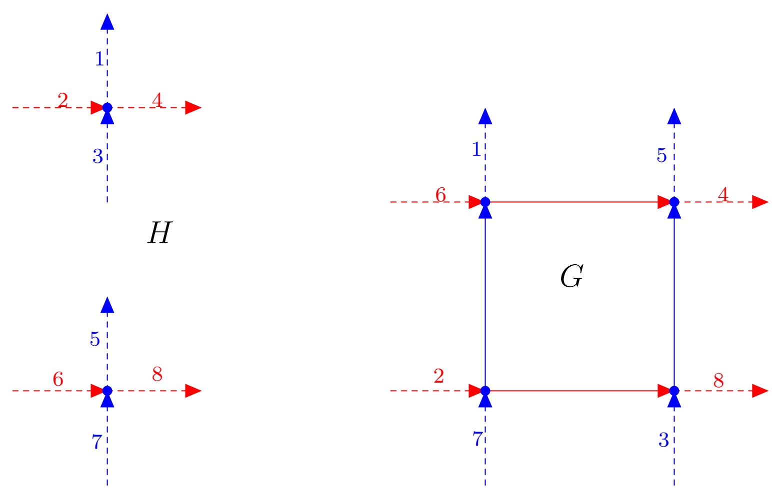

Figure 1: The graph G is the core of $\langle [a, b] \rangle$ and H consists of two vertices. Pick a bijection between the missing edges at H and the missing edges at G. A completion of H corresponds to a completion of G by reconnecting the adjacent edges according to this bijection. If the completion of H is connected, then so is the completion of G.

starting at v_j and ending at a new leaf. Repeat this process until $|E_j(G_i)|$ becomes independent of j.

This process terminates since $\sum_i \sum_j (\max_{j'}(|E_{j'}(G_i)|) - |E_j(G_i)|)$ is a non-negative integer, which decreases whenever we change the graph. Let G' be the resulting graph.

The inclusion of G to G' is a π_1-isomorphism on each component and G' contains finitely many more edges than G. If $\overline{G}$ is a random completion of G, then there is a unique map $G' \longrightarrow \overline{G}$ extending the inclusion of G. If this map is injective, then $\overline{G}$ is also a completion of G'. Let's estimate the probability of this event. Build a random completion of G in the same way, we've built G': one edge at a time.

If first edge e_1 connects to a vertex of G, then the injectivity fails. There are $n - |V(G)|$ vertices not in G. If e_1 connects to one of them, we can continue with the second edge. The second edge e_2 can fail the injectivity in at most $|V(G)|+1$ ways (it might connect back to G or to an endpoint of e_2). It can succeed in at least $n - |V(G)|-1$ ways. Continue for all new edges. The probability that $G' \longrightarrow \overline{G}$ is injective is at least

$$\frac{n - |V(G)|}{n} \frac{n - |V(G)|-1}{n} \cdots \frac{n - |V(G)|-\Delta}{n}$$

where $\Delta = |E(G')|-|E(G)|$. This quantity goes to 1 as n goes to infinity. This means $G' \longrightarrow \overline{G}$ is almost always injective and a completion of G is almost always a completion of G'. By case 1, a completion of G' is almost always connected, therefore a completion of G is almost always connected. We are implicitly using that the probabilities are compatible in the following sense.

$$\mathbb{P}(\text{ A completion of } G \text{ is } H | H \text{ is a completion of } G') = \mathbb{P}(\text{ A completion of } G' \text{ is } H)$$

This is true, because it does not matter whether we complete G to a completion containing G', or whether we complete G'.

$\square$

4 Primitivity

An action of a group Γ on a finite set X is *primitive* if it is transitive and no nontrivial partition of X is preserved by Γ. We have already dealt with the transitivity, so we just need to show non-existence of a preserved partition. Transitivity implies that all sets in the partition have the same size, hence taking n to be a prime ensures primitivity, but we do not need to do that here.

Lemma 4.1. *Assume that no component of G is a covering of R_k. Then $\Gamma_n(G)$ is almost always primitive.*

We use that imprimitive groups are extremely rare.

Proof. By Lemma 2 in [Dix69], the proportion of pairs of elements of S_n, which generate an imprimitive subgroup is at most $n2^{-\frac{n}{4}}$ (and hence this bound also applies to k-tuples).

Let's count what proportion of k-tuples of elements of S_n *respects* G (i.e. how many arise from a completion of G).

Recall that $|E_j(G)|$ is the number of edges in G labelled a_j.

The probability that a random permutation moves vertices according to the edges labelled a_j is

$$\frac{1}{n(n-1)\dots(n-|E_j(G)|+1)}.$$

If $n > 2|E(G)|$, a random completion respects G with probability at least $(2n)^{-|E(G)|}$. This is only polynomial in n. Even if all k-tuples generating imprimitive subgroups respected G, the proportion of imprimitive random completions of G would be at most

$$\frac{n2^{-\frac{n}{4}}}{(2n)^{-|E(G)|}} = (2n)^{|E(G)|}n2^{-\frac{n}{4}}$$

which goes to zero as n goes to ∞. □

5 'Jordan' condition

The final condition (in addition to being primitive) for a subgroup to be A_n or S_n is that it contains a q-cycle for some prime $q \le n-3$ [Wie14, Theorem 13.9].

Following [Dix69], we define $C_{q,n} \subset S_n$ to consist of those permutations which contain a single cycle of length divisible by q and all the other cycles are of lengths coprime to q.

In particular, if G contains an element of $C_{q,n}$, then it contains a q-cycle. The following lemma is a key step in Dixon's theorem.

Lemma 5.1 (Lemma 3 in [Dix69]). *Let $T_n = \bigcup_q C_{q,n}$, where the union is over all primes q such that*
$$(\log n)^2 \leq q \leq n-3\,.$$
Then the proportion u_n of elements of S_n which lie in T_n is at least
$$1 - 4/(3 \log\log n)$$
for all sufficiently large n.

We need to generalise this to the conditional case.

Lemma 5.2. *Let G be any graph. Take a random group action with condition G. Almost always some power of a_1 acts as a q-cycle, where $q \leq n-3$ is a prime.*

The generalisation is a bit more complicated. We separate the a_1-edges in the condition graph G into cycles and paths. We will take n very large compared to the size of the cycles. This will allow us to ignore the cycles since they will all be smaller than the prime q. To deal with the paths, one only needs to realise that paths are a typical behaviour. The corresponding walks in the random unconditional completion would almost always be injective, so we can apply the unconditional theorem.

Proof. We are only using one generator, so in this proof we can assume that there is only one generator. The condition graph G consists of cycles and paths because no vertex has valence greater than 2. We will deal with both of them separately. The paths do not really cause many issues. As in the proof of transitivity, almost every completion of an empty graph will be also a completion of a union of paths. This will reduce the statement to the unconditional version. To deal with the cycles we can use the lower bound of Lemma 5.1 and force q to be bigger than the length of all cycles. This way a suitable power of a_1 will fix the cycles pointwise, and act as a q-cycle on the remaining vertices.

The graph G consists of paths $P_1, \ldots, P_k$ and cycles $L_1, \ldots, L_l$. Let v_i be the initial vertex of P_i. Let G' be the union of all the paths P_i.

Let $n' = n - \sum_i |L_i|$. Let D_k be a graph with k vertices and no edges. Pick a bijection f between the vertices of D_k and $\{v_i\}$. Consider the random degree n' completion $\Gamma_{n'}(D_k)$. Then by lemma 5.1
$$\mathbb{P}(a_1 \text{ acts as an element of } T_{n'}) \geq 1 - 4/(3 \log\log n')$$
for sufficiently large n'.

There is unique label and orientation preserving map $\overline{f}$ from G' to a completion of a discrete graph, which extends f. If this map $\overline{f}$ is injective, then the completion of D_k is also a completion of G'. We claim that this happens with probability $1 - \mathcal{O}(1/n')$. Let's proceed by induction on the sum of length of the paths in G'. If there are no edges, the map $\overline{f}$ is just f and therefore a bijection to its image D_k.

If G' contains an edge, let e be an edge at the end of one of the paths. Let G'' be G' without e and the terminal endpoint $t(e)$, but with the initial endpoint $i(e)$. In other words, G'' is the same graph as G', just with one of the paths shorter by 1. By induction G'' injects with probability $1 - \mathcal{O}(1/n')$. Suppose G'' injects. Then the graph G' fails to inject only if $t(e)$ is one of the vertices in D_k. This happens with probability $\frac{k}{n'-|E(G'')|}$ since there are $n' - |E(G'')| - k$ vertices not in the image of G'. Therefore, G' injects with probability $(1 - \mathcal{O}((1/n'))\left(1 - \frac{k}{n'-|E(G'')|}\right) = (1 - \mathcal{O}(1/n'))$.

A random completion of D_k is almost always a random completion of G'. We can restate Lemma 5.1 as follows. A random completion of D_k has almost always the property that the induced a_1 belongs to $T_{n'}$. But then the same applies to a random completion of G', because a random completion of D_k is almost always a completion of G'. I.e. some power of a_1 in the random action with condition G' almost always acts as q-cycle, where q is a prime with $(\log n)^2 \leq q \leq n - 3$.

Take $n' > \exp(\sqrt{\max|L_i|})$. A random completion of G is just a union of a random completion of G' and the cycles L_i. Therefore a_1 almost always acts as a union of an element from $T_{n'}$ and cycles of lengths $|L_i|$. By choice of n', we have $\max|L_i| < q$. Some power of a_1 almost always acts as a union of a q-cycle and cycles shorter than q. Therefore, a higher power of a_1 almost always acts as q-cycle. □

6 Sample application - reproving alternating version of subgroup separability of free groups

We can now reprove the main theorem of [Wil12] using probabilistic methods.

Proposition 6.1 ([Wil12]). *Suppose G is a finitely generated infinite index subgroup of a non-abelian free group F_k and that $g_1, \ldots, g_l \in F_k \setminus G$. Then there exists a surjection $f : F_k \longrightarrow A_n$ onto some alternating group such that $f(g_i) \notin f(G)$ for all i.*

The technique is similar to and illustrative of the proof of theorem A.

Proof. Let X_G be the cover of R_k associated to G as before and let x_g be a basepoint in X_G such that the closed paths starting at x_g are precisely the elements of G. Let

γ_i be the loop in R_k representing g_i and let $\tilde{\gamma}_i$ be its lift to X_G starting at x_G. Let $Y \subset X_G$ be the union of all loops in X_G and all images of $\tilde{\gamma}_i$.

The graph Y consists of a single component and this component is not a covering of R_k as X_G is a connected infinite degree cover and its finite (non-empty) subgraphs are not coverings. We can apply Theorem 2.5 which says that a random group $\Gamma_n(Y)$ with condition Y is S_n or A_n with probabilities which tend to $1 - 2^{-k}$ and 2^{-k} respectively as n goes to infinity. In particular, probability that the image of G is A_n is eventually positive. The endpoint of $\tilde{\gamma}_i$ isn't x_G, therefore $f(g_i) \notin f(G)$ in any completion of Y and in particular also in those which surject onto an alternating group. $\square$

7 Subgroup conjugacy separability and randomness

In this section we prove Theorem A. A random action often demonstrates separability properties of a free group. Since the action is often alternating, this demonstrates separability within alternating groups.

Let g and h be two elements of a free group, such that g is not conjugate to either h or h^{-1}. After conjugation, we may assume that g is cyclically reduced and freely reduced. If a homomorphism $f : F_2 \longrightarrow S_n$ is such that $f(g)$ and $f(h)$ have different cycle structures, then g and h remain in different conjugacy classes in the image under f.

A random action with a suitable condition will give different expected numbers of fixed points of g and h and just a small variance. This produces actions, which keep g and h in different conjugacy classes.

Let G be a loop labelled with g. In counting fixed points of g, we need to count how often G lifts to a covering. We can categorise these lifts by their image. I.e. we can count injective lifts of possible images of G.

Definition 7.1 (Quotient of a precover)**.** If G is a precover of R_k for some k and K is a graph, then a simplicial surjective locally injective map $f : G \twoheadrightarrow K$ is *a quotient of a precover G*.

Let's say we want to count the number of lifts of a graph H. Then the image of a lift of H is some quotient of H. If we take the union with G, we get some quotient of $G \sqcup H$, where the restriction to G is injective. Counting the lifts of H is therefore the same as counting the injective lifts of those quotients of $G \sqcup H$, where the restriction to G is injective. Let's give this quantity a notation.

Definition 7.2. Suppose G and H are precovers, K is a quotient of the precover $G \sqcup H$ and $\overline{G}$ is a completion of G. By $\mu_{K \longrightarrow \overline{G}}$ we denote the number of injective maps from K to $\overline{G}$ such the the composition $G \longrightarrow K \longrightarrow \overline{G}$ is the natural inclusion of G to $\overline{G}$.

Let $\tau_{H \longrightarrow \overline{G}}$ be the total number of maps from H to G.

Note that if $G \longrightarrow K$ is not injective, then $G \longrightarrow K \longrightarrow \overline{G}$ cannot be an inclusion of G and therefore $\mu_{K \longrightarrow \overline{G}} = 0$. Let's express τ using μ.

Lemma 7.3. *Suppose that G and H are precovers and $\overline{G}$ is a completion of G. The total number of maps from H to $\overline{G}$ is given by the following.*

$$\tau_{H \longrightarrow \overline{G}} = \sum_{K = (G \sqcup H)/\sim} \mu_{K \longrightarrow \overline{G}}$$

The sum goes over quotients K of the precover $G \sqcup H$.

Proof. Given a map $f : H \longrightarrow \overline{G}$, let $K = G \cup f(H)$. Then K injects to $\overline{G}$ and $G \longrightarrow K \longrightarrow \overline{G}$ is an isomorphism onto $G \subset \overline{G}$.

Conversely, if K is a quotient of $G \sqcup H$ and it injects to $\overline{G}$ and $G \longrightarrow K \longrightarrow G$ is an isomorphism, let f be the map $H \longrightarrow K \longrightarrow G$. $\square$

We will now need to estimate each summand in the previous lemma. If G was empty then the first order estimate would be $n^{\chi(K)}$ [PP15, Theorem 1.8]. To take potentially non-empty G into account, we define the relative Euler characteristic be a difference of the Euler characteristics.

Definition 7.4 (Relative Euler Characteristic)**.** If K is a quotient of $G \sqcup H$ such that G embeds to K, then *the Euler characteristic of K relative to G* is $\chi_G(K) = \chi(K) - \chi(G)$.

The next lemma gives the expected number of lifts of a quotient of $G \sqcup H$. This quantity makes intuitive sense, since the relative Euler characteristic counts the components of K disjoint from components of G, minus the loops of K, which are not loops of G. See Figure 2.

Lemma 7.5. *Suppose G and H are precovers and K is a quotient of the precover $G \sqcup H$. Then we can express the expected number of maps from K to the random completion $\overline{G}$ which extend the inclusion of G as follows.*

$$\mathbb{E}(\mu_{K \longrightarrow \overline{G}}) = n^{\chi_G(K)} + \mathcal{O}(n^{\chi_G(K)-1})$$

Here we fix K, G and H and we let $\overline{G}$ be a random degree n completion of G.

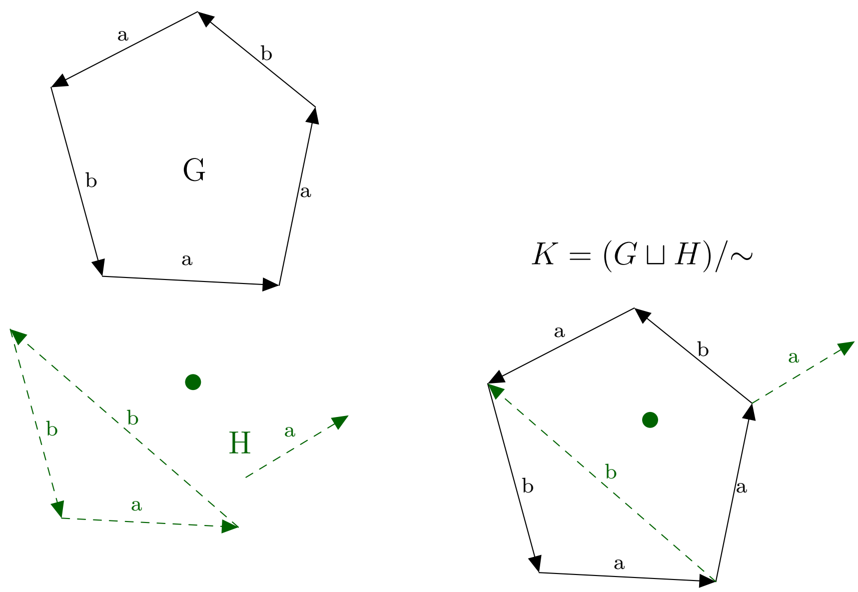

Figure 2: We expect roughly 1 lift of K, since there is about $1/n$ probability that the diagonal b-edge closes up and there are about n possibilities for the location of the isolated vertex. The green a-edge does not contribute anything, because there are roughly n options for its endpoint and each of them appears with probability roughly $1/n$.

Proof. We'll prove this by induction on the number of cells in $K \setminus G$. For the base case of $K = G$, left hand side is 1 and the right hand side is $1 + \mathcal{O}(n^{-1})$.

1. Suppose there exists an edge e of K not contained in G. Let K' be $K \setminus e$. By the induction on the number of cells, we have $\mathbb{E}(\mu_{K' \longrightarrow \overline{G}}) = n^{\chi_G(K')} + \mathcal{O}(n^{\chi_G(K')-1})$.

   There are between n and $n - |E(K')|$ ways for e to lift and only one of them allows K to lift. Hence,

   $$\mathbb{E}(\mu_{K \longrightarrow \overline{G}}) = n^{-1}\mathbb{E}(\mu_{K' \longrightarrow \overline{G}}) + \mathcal{O}(n^{-2})$$

2. If $K \setminus G$ contains no edges, then it is a disjoint union of G and vertices. Suppose $v \in K \setminus G$ is a vertex. Let $K' = K \setminus v$. To lift K, we need to lift K' and specify, where does v go. We always have between n and $n - v(K')$ options for v, so

   $$\mathbb{E}(\mu_{K \longrightarrow \overline{G}}) = n\mathbb{E}(\mu_{K' \longrightarrow \overline{G}}) + \mathcal{O}(1)$$

$\square$

In particular, we can get the highest order term approximation to the total number of expected lifts of H to a completion of G by determining the largest relative Euler characteristic among the quotients of $G \sqcup H$ and the number of quotients, which achieve this minimum.

Definition 7.6 (Relative rank, critical graphs and multiplicity)**.** *The relative rank* $r_G(H)$ *is* $\min \chi_G(K)$*, where the minimum goes over quotients of* $G \sqcup H$*.*

We call the quotients which achieve the minimum critical graphs. Relative multiplicity is the number of critical graphs.

Lemma 7.7. *Suppose G and H are precovers, and G' a random completion of G. Then the variance of $\tau_{H \longrightarrow \overline{G}}$ is as follows.*

$$\mathrm{Var}(\tau_{H \longrightarrow \overline{G}}) = \mathbb{E}(\tau_{(H \sqcup H) \longrightarrow \overline{G}}) - \mathbb{E}(\tau_{H \longrightarrow \overline{G}})^2$$

Proof. Write out the expression for the variance.

$$\mathrm{Var}(\tau_{H \longrightarrow G}) = \mathbb{E}(\tau^2_{H \longrightarrow \overline{G}}) - \mathbb{E}(\tau_{H \longrightarrow \overline{G}})^2$$

The expectation of the square $\mathbb{E}(\tau^2_{H \longrightarrow \overline{G}})$ is the same as the expected number of pairs of maps $H \longrightarrow \overline{G}$, which is the same as the number of maps $H \sqcup H \longrightarrow \overline{G}$. $\square$

We will use the Lemmas 7.3 and 7.7 to count the mean and the variance of the number of the lifts.

Example 7.8. Suppose $\gamma_1, \ldots, \gamma_k \in F_r$ and $\Gamma_1, \ldots, \Gamma_l < F_k$ and each Γ_j has rank at least 2. Suppose that $\gamma_i = u_i^{k_i}$ and that u_i is not a proper power.

Let by abuse of notation γ_i be a core graph of $\langle \gamma_i \rangle$. Let G_j be the core graph of Γ_j. Let graph G be the disjoint union of a_i copies of γ_i and b_j copies of Γ_j.

Now take a random completion of G. We'll count lifts of γ_i and Γ_j. Let's first calculate $\tau_{\gamma_i \longrightarrow \overline{G}}$. For this we'll need to calculate a contribution from each quotient of $G \cup \gamma_i$. The relative rank $r_G(\gamma_i)$ is at most $\chi(\gamma_i) = 0$. It can't be smaller, because then there would need to be a component of a critical graph, which is simply connected. That is not possible, because the quotient map is locally injective and γ_i contains no leaves. When counting the critical graphs, two types arise.

1. The image of γ_i is disjoint from all G (we're talking about the additionally copy of γ_i, not about one of the copies in G). There are $\sigma(k_i)$ such quotients, where σ counts divisors of an integer.

2. The image of γ_i lies in G. We can express this quantity as a linear function of a_j's and b_j's.
$$\tau_{\gamma_i \longrightarrow G} = \sum_j a_j \tau_{\gamma_i \longrightarrow \gamma_j} + \sum_j b_j \tau_{\gamma_i \longrightarrow G_j}$$

Use Lemma 7.5 to get

$$\mathbb{E}(\tau_{\gamma_i \longrightarrow \overline{G}}) = \tau_{\gamma_i \longrightarrow G} + \sigma(k_i) + \mathcal{O}(n^{-1})\,.$$

Let's also compute the variance of $\tau_{\gamma_i \longrightarrow \overline{G}}$. Let $H = \gamma_i \sqcup \gamma_i$. By Lemma 7.7,

$$\mathrm{Var}(\tau_{\gamma_i \longrightarrow \overline{G}}) = \mathbb{E}(\tau_{H \longrightarrow \overline{G}}) - \mathbb{E}(\tau_{\gamma_i \longrightarrow \overline{G}})^2\,.$$

We have an estimate for the second term, so let's compute the first one. Again $r_G(H) = 0$. There are four types of quotient contributing to the critical graphs.

1. Image of H are two circles disjoint from G. There are $\sigma(k_i)^2$ such graphs.

2. Both circles of H map to a single circle disjoint from G. There are $D(k_i) = \sum_{d|k_i} d$ such graphs as we need to specify the size of the circle and the distance by which are the images of the two circles shifted.

3. One of the circles maps to G and the other remains disjoint. There are $2\sigma(k_i)\tau_{\gamma_i \longrightarrow G}$ such critical graphs.

4. Both circles map to G. There are $\tau^2_{\gamma_i \longrightarrow G}$ such critical graphs.

Add up all these contributions.

$$\begin{aligned}\mathbb{E}(\tau_{H \longrightarrow \overline{G}}) &= \sigma(k_i)^2 + D(k_i) + 2\sigma(k_i)\tau_{\gamma_i \longrightarrow G} + \tau^2_{\gamma_i \longrightarrow G} + \mathcal{O}(n^{-1}) \\ &= (\sigma(k_i) + \tau_{\gamma_i \longrightarrow G})^2 + D(k_i) + \mathcal{O}(n^{-1})\end{aligned}$$

If we plug it into the expression for variance, most terms cancel out.

$$\begin{aligned}\mathrm{Var}(\tau_{\gamma_i \longrightarrow G}) &= (\sigma(k_i) + \tau_{\gamma_i \longrightarrow G})^2 + D(k_i) + \mathcal{O}(n^{-1}) - (\tau_{\gamma_i \longrightarrow G} + \sigma(k_i) + \mathcal{O}(n^{-1}))^2 \\ &= D(k_i) + \mathcal{O}(n^{-1}).\end{aligned}$$

Let's now compute the number of lifts of G_i. If $b_i \neq 0$, then $\chi_G(G_i) \geq 0$, because we can send G_i to G. Also, $\chi_G(G_i) \leq 0$ since no component of a quotient of $G \sqcup G_i$ is simply connected.

Suppose K is a quotient of $G \sqcup G_i$ such that $G \longrightarrow K$ is an injection. Let L be $q(G_i) \setminus q(G)$, where q is the quotient map. There may be open edges in L, so it is not necessarily a graph. Then $\chi_G(K) = V(L) - E(L)$. If K is a critical graph, then $V(L) = E(L)$. If L is non-empty, it must contain a component L' with $V(L') \geq E(L')$. The component L' is either a tree, a tree minus a leaf, or a rank 1 graph. If a component of L is a genuine graph, then it is also a component of K. Such a component of K is a locally injective quotient of G_i and therefore has rank at least 2. If L' is a tree minus a leaf, then another leaf of L' is a leaf of K. This is impossible since all vertices in $G \sqcup G_i \sqcup G_i$ have valence at least 2 and the quotient map is locally injective. Therefore L is empty and the critical graphs are precisely the quotients arising from the maps from G_i to G. The number of critical graphs is $\tau_{G_i \longrightarrow G}$ and we can use Lemma 7.5 to express the expected number of lifts of G_i to a completion of G. Therefore,

$$\mathbb{E}(\tau_{G_i \longrightarrow \overline{G}}) = \tau_{G_i \longrightarrow G} + \mathcal{O}(n^{-1}) = \sum_j b_j \tau_{G_i \longrightarrow G_j} + \mathcal{O}(n^{-1})\,.$$

Similarly, we can compute the variance using Lemma 7.7. We'll need to estimate $\tau_{(G_i \sqcup G_i) \longrightarrow \overline{G}}$. The relative rank of $r_G(G_i \sqcup G_i)$ is at least 0 because we can send both G_i's to a copy of G_i in G. It can't be less, since no component of a quotient of $G \sqcup G_i \sqcup G_i$ is simply connected.

Suppose K is a critical graph and $L = q(G_i \sqcup G_i) \setminus q(G)$ is non-empty. Then there exists a component L' of L, which is either a tree, a tree minus a leaf, or a rank 1 graph. If L' is a tree or a rank 1 graph, then it is a component of a quotient of $G_i \sqcup G_i$. However, the components of quotients of $G_i \sqcup G_i$ have rank at least 2. If L' is a tree minus a vertex, then another leaf of L' is a leaf of K. This is impossible because K is a locally injective quotient of a graph with minimal valence 2. Therefore L is empty, and $G_i \sqcup G_i$ maps to G in any critical quotient.

There are $(\sum_j b_j \tau_{G_i \longrightarrow G_j})^2$ critical graphs, because we need to specify the images of two copies of G_i.

Hence,

$$\mathbb{E}(\tau_{(G_i \sqcup G_i) \longrightarrow \overline{G}}) = (\sum_j b_j \tau_{G_i \longrightarrow G_j})^2 + \mathcal{O}(n^{-1}) .$$

The leading terms cancel out and we are left with a variance that goes to 0 as n goes to infinity.

$$Var(\tau_{G_i \longrightarrow \overline{G}}) = \mathbb{E}(\tau_{(G_i \sqcup G_i) \longrightarrow \overline{G}}) - \mathbb{E}(\tau_{G_i \longrightarrow \overline{G}})^2 = \mathcal{O}(n^{-1})$$

Eventually, the goal is to separate subgroups using distinct numbers of fixed points. In order to do this, we need the following technical lemmas, which promotes groups commensurable to subgroups to actual subgroups. The first lemma says that a core of a finite index subgroup is a cover of a core.

Lemma 7.9. *Suppose $A, B < F_k$ are finitely generated subgroups and A has a finite index in B. Then* $\mathrm{Core}(A)$ *is a degree $[B : A]$ cover of* $\mathrm{Core}(B)$ *and in particular* $\frac{|V(\mathrm{Core}(A))|}{|V(\mathrm{Core}(B))|} = [B : A]$.

Proof. Let X_A and X_B be the covers of R_k associated to A and B. Let $p : X_A \longrightarrow X_B$ be the covering map. Let $d = [B : A]$. Suppose $e \in E(X_A)$ with $p(e) \in \mathrm{Core}(B)$. Then there exists some loop in $\mathrm{Core}(B)$ containing $p(e)$. The d-th power of this loop lifts to a loop in X_A, which contains e, and hence $e \in \mathrm{Core}(A)$. The restriction $p_{\mathrm{Core}(A)}$ is a local homeomorphism which covers $\mathrm{Core}(B)$ evenly and $\mathrm{Core}(A)$ is a cover of $\mathrm{Core}(B)$. $\square$

Lemma 7.10. *If H_1, H_2 are finitely generated subgroups of a free group, $G < H_1 \cap H_2$ has finite index in H_1, and all divisors of $[H_1 : G]$ distinct from 1 are larger than $|V(\mathrm{Core}(H_2))|$, then H_1 is a subgroup of H_2.*

Proof. Consider $\mathrm{Core}(H_1 \cap H_2)$. We can get it as a component of the pullback of the maps $\mathrm{Core}(H_i) \longrightarrow X$, where X is the rose R_k. The pullback contains $|V(\mathrm{Core}(H_1)||V(\mathrm{Core}(H_2)|$ vertices, therefore

$$|V(\mathrm{Core}(H_1 \cap H_2)| \leq |V(\mathrm{Core}(H_1)||V(\mathrm{Core}(H_2)| .$$

The group G is a finite index subgroup of $H_1 \cap H_2$, which is a finite index subgroup of H_1. By lemma 7.9 applied to $H_1 \cap H_2 < H_1$ and to $G < H_1 \cap H_2$, $|V(\mathrm{Core}(H_1))|$

divides $|V(\mathrm{Core}(H_1 \cap H_2)|$, which divides $|V(\mathrm{Core}(G))|$. Then $|V(\mathrm{Core}(H_1 \cap H_2)|=$ $d|V(\mathrm{Core}(H_1)|$, where d divides $\frac{|V(\mathrm{Core}(G))|}{|V(\mathrm{Core}(H_1))|} = [H_1 : G]$. But every nontrivial divisor of $[H_1 : G]$ is larger than $|V(\mathrm{Core}(H_2))|$, so $|V(\mathrm{Core}(H_1 \cap H_2)|= |V(\mathrm{Core}(H_1)|$. Since $\mathrm{Core}(H_1 \cap H_2)$ is a covering of $\mathrm{Core}(H_1)$, the two graphs are in fact equal and $H_1 \cap H_2 = H_1$. $\square$

Finally, we can put everything together in the proof of the following separability property, which can be thought of as an 'alternating' refinement of subgroup into-conjugacy separability. We will do this by using that whenever H_1 is conjugate into H_2, it fixes at least as many elements as H_2. We will also use that the same is true for concrete characteristic subgroups. For example suppose H_1 is not conjugate into H_2 and H_2 is not conjugate into H_1. If H_1 fixes more points than H_2, then $f(H_2)$ is not conjugate into $f(H_1)$. If additionally the intersection of all degree 2 subgroups of H_2 fixes more points than the intersection of all degree 2 subgroups of H_1, then $f(H_1)$ is not conjugate into $f(H_2)$.

Theorem 7.11. *Suppose $H_1, H_2, \ldots, H_n < F_r$ are finitely generated subgroups of infinite index. Then there exists a surjective homomorphism $f : F_r \twoheadrightarrow A_m$ such that whenever H_i is not conjugate into H_j, then $f(H_i)$ is not conjugate into $f(H_j)$.*

Proof. Denote the relation of 'is conjugate into' by '$\prec$'. Conjugacy classes of finitely generated subgroups of F_r form a poset with respect to $\prec$ so after reordering and removing duplicates, we may assume that $H_i \prec H_j$ implies $i \leq j$.

Let $p_1, p_2, \ldots, p_n$ be primes larger than $\max_i(V(\mathrm{Core}(H_i))$ with $p_j > p_k^{(k!)^{rkH_k}} V(\mathrm{Core}(H_k))$ whenever $j < k$. Let $G_{i,j}$ be the intersection of all index p_j subgroups of H_i. Let graph G be a union of a_i copies of $\mathrm{Core}(G_{i,i})$, where a_i's are to be specified later. Let $f : F_r \longrightarrow A_m$ be a random map arising from a random completion of G. The group $f(G_{i,j})$ is the intersection of all index p_j subgroups of $f(H_i)$. Indeed, every index p_j subgroup of $f(H_i)$ is an image of an index p_j subgroup of H_i.

If $f(H_i) \prec f(H_j)$, then $fix(f(H_i)) \geq fix(f(H_j))$, but also $f(G_{i,k}) \prec f(G_{j,k})$ and hence $fix(G_{i,k}) \geq fix(G_{j,k})$.

By Example 7.8 for every ε there exists $K = K(\varepsilon)$ independent of $a_1, \ldots, a_n$ such that for all sufficiently large m

$$\mathbb{P}(\forall i, j, |fix(G_{i,j}) - \Sigma_k a_k \tau_{\mathrm{Core}(G_{i,j}) \longrightarrow \mathrm{Core}(G_{k,k})}|< K) > 1 - \varepsilon \tag{1}$$

In words, the number of fixed points of $G_{i,j}$ belongs with high probability to a specific interval of length $2K$. By controlling the center of the interval, we will ensure that these groups often fix distinct numbers of elements.

If $\tau_{\mathrm{Core}(G_{i,j})\longrightarrow\mathrm{Core}(G_{k,k})} > 0$, then $G_{i,j} < G^g_{k,k}$ for some g. Both H_i and $G^g_{k,k}$ are subgroups of a free group, and the index of $G_{i,j} < H_i \cap G^g_{k,k}$ in H_i is a power of p_j. The core of $G_{k,k}$ contains at most $p_k^{(k!)^{rkH_k}} V(\mathrm{Core}(H_k))$ vertices. If $j < k$, then $p_j > p_k^{(k!)^{rkH_k}} V(\mathrm{Core}(H_k))$ and by Lemma 7.10 $H_i < G^g_{k,k}$. This is a contradiction since the girth of $\mathrm{Core}(H_i)$ is at most $V(\mathrm{Core}(H_i))$ and the girth of $\mathrm{Core}(G_{k,k})$ is at least $p_k > V(\mathrm{Core}(H_i))$.

We also have have $p_j > V(\mathrm{Core}(H_k))$, so Lemma 7.10 applied to $H_i, G_{i,j}$ and H^g_k gives that $H_i \prec H_k$.

Let K be such that the probability in Equation 1 is at least $p = 1 - 2^{-r-1}$. Let $a_1, \ldots, a_n$ satisfy $a_j > na_{j-1}C + K$, where $C = \max_{i,j,k} \tau_{\mathrm{Core}(G_{i,j})\longrightarrow\mathrm{Core}(G_{k,k})}$.

All of the following is simultaneously true with probability at least $1 - 2^{-r-1}$. For all j, $fix(G_{j,j}) \geq a_j$. For all i, j, if H_i is not conjugate into H_j, then $\mathrm{fix}(G_{i,j}) \leq \max(0, (j-i)a_{j-1}C + K) < a_j$. Hence $f(H_i)$ is not conjugate into $f(H_j)$.

The probability that the image is A_m tends to 2^{-r} as m goes to infinity (Theorem 2.5). In particular, there exists a map f with the described separating properties. $\square$

References

[Bab89] László Babai. The probability of generating the symmetric group. *Journal of Combinatorial Theory, Series A*, 52(1):148–153, 1989.

[BB14] Oleg Bogopolski and Kai-Uwe Bux. Subgroup conjugacy separability for surface groups. *arXiv preprint arXiv:1401.6203*, 2014.

[BG10] Oleg Bogopolski and Fritz Grunewald. On subgroup conjugacy separability in the class of virtually free groups. 12 2010.

[CZ15] SC Chagas and Pavel A Zalesskii. Subgroup conjugacy separability of free-by-finite groups. *Archiv der Mathematik*, 104(2):101–109, 2015.

[CZ16] Sheila C Chagas and Pavel A Zalesskii. Limit groups are subgroup conjugacy separable. *Journal of Algebra*, 461:121–128, 2016.

[Dix69] John D Dixon. The probability of generating the symmetric group. *Mathematische Zeitschrift*, 110(3):199–205, 1969.

[DPSS03] John D Dixon, László Pyber, Ákos Seress, and Aner Shalev. Residual properties of free groups and probabilistic methods. *Journal fur die Reine und Angewandte Mathematik*, pages 159–172, 2003.

[LS02] Martin W Liebeck and Aner Shalev. Random (r, s)–generation of finite classical groups. *Bulletin of the London Mathematical Society*, 34(2):185–188, 2002.

[LS04] Martin W Liebeck and Aner Shalev. Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks. *Journal of Algebra*, 276(2):552–601, 2004.

[LS05] Martin W Liebeck and Aner Shalev. Character degrees and random walks in finite groups of lie type. *Proceedings of the London Mathematical Society*, 90(1):61–86, 2005.

[PP15] Doron Puder and Ori Parzanchevski. Measure preserving words are primitive. *Journal of the American Mathematical Society*, 28(1):63–97, 2015.

[Wie14] Helmut Wielandt. *Finite permutation groups*. Academic Press, 2014.

[Wil12] Henry Wilton. Alternating quotients of free groups. *Enseign. Math. (2)*, 58(1-2):49–60, 2012.