# Surface Words are Determined by Word Measures on Groups

Michael Magee and Doron Puder

February 13, 2019

**Abstract**

Every word $w$ in a free group naturally induces a probability measure on every compact group $G$. For example, if $w = [x, y]$ is the commutator word, a random element sampled by the $w$-measure is given by the commutator $[g, h]$ of two independent, Haar-random elements of $G$. Back in 1896, Frobenius showed that if $G$ is a finite group and $\psi$ an irreducible character, then the expected value of $\psi([g, h])$ is $\frac{1}{\psi(e)}$. This is true for any compact group, and completely determines the $[x, y]$-measure on these groups. An analogous result holds with the commutator word replaced by any surface word.

We prove a converse to this theorem: if $w$ induces the same measure as $[x, y]$ on every compact group, then, up to an automorphism of the free group, $w$ is equal to $[x, y]$. The same holds when $[x, y]$ is replaced by any surface word.

The proof relies on the analysis of word measures on unitary groups and on orthogonal groups, which appears in separate papers, and on new analysis of word measures on generalized symmetric groups that we develop here.

## Contents



## 1 Introduction

Let $\mathbf{F}_r$ be the free group on $r$ generators $x_1, \ldots, x_r$, and let $G$ be any finite, or more generally, compact group. Every word $w \in \mathbf{F}_r$ induces a map, called a *word map*,

$$w\colon \underbrace{G \times \ldots \times G}_{r \text{ times}} \to G,$$

defined by substitutions. For example, if $w = x_1 x_3 x_1 x_3^{-2} \in \mathbf{F}_3$, then $w(g_1, g_2, g_3) = g_1 g_3 g_1 g_3^{-2}$. The push-forward via this word map of the Haar probability measure (uniform measure in the finite case) on $G \times \ldots \times G$ is called the *$w$-measure* on $G$. Put differently, for each $1 \le i \le r$, substitute $x_i$ with an independent, Haar-distributed random element of $G$, and evaluate the product defined by $w$ to obtain a random element in $G$ sampled by the $w$-measure. We say the resulting element is a *$w$-random* element of $G$.

### Measures induced by surface words

The study of word measures in groups has its seeds in the 1896 work of Frobenius [Fro96]. Let $[x,y]=xyx^{-1}y^{-1}$ be[1] the commutator word. Frobenius shows that the $[x,y]$-measure on a finite group $G$ is given by

$$\frac{1}{|G|}\sum_{\psi\in\mathrm{Irr}(G)}\frac{1}{\psi(1)}\psi,$$

where $\mathrm{Irr}(G)$ marks the set of irreducible characters of $G$. As word measures on finite groups are class functions, this is equivalent to the fact that for every $\psi\in\mathrm{Irr}(G)$, the expected value of $\psi$ under the $[x,y]$-measure is $\frac{1}{\psi(1)}$. In 1906, Frobenius and Schur [FS06] showed that the $x^2$-measure on a finite group is given by

$$\frac{1}{|G|}\sum_{\psi\in\mathrm{Irr}(G)}\mathcal{FS}_\psi\cdot\psi,$$

where $\mathcal{FS}_\psi$ is the Frobenius-Schur indicator of $\psi$:

$$\mathcal{FS}_\psi=\begin{cases}1 & \psi \text{ is afforded by a real representation}\\ -1 & \psi \text{ is real but is not afforded by any real representation}\\ 0 & \psi \text{ is not real.}\end{cases}$$

The statement is equivalent to that the expected value of an irreducible character $\psi$ under the $x^2$-measure is $\mathcal{FS}_\psi$.

In fact, the same result holds for any compact group $G$ and can be generalized to any surface word:

**Theorem 1.1** (Frobenius, Frobenius-Schur)**.** *Let $G$ be a compact group and $\psi$ an irreducible character of $G$. Then,*

1. *For $w=[x_1,y_1]\cdots[x_g,y_g]$, the expected value of $\psi$ under the $w$-measure is $\frac{1}{\psi(1)^{2g-1}}$.*
2. *For $w=x_1^2\cdots x_g^2$, the expected value of $\psi$ under the $w$-measure is $\frac{(\mathcal{FS}_\psi)^g}{\psi(1)^{g-1}}$.*

Of course, here $x_1,\ldots,x_g,y_1,\ldots,y_g$ are distinct letters. See Section 2 for some details about the proof.

### Do word measures determine the word?

For $w_1,w_2\in\mathbf{F}_r$ write $w_1\overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim}w_2$ if there is $\theta\in\mathrm{Aut}(\mathbf{F}_r)$ with $\theta(w_1)=w_2$. It is easy to see that applying elementary Nielsen transformations on a word does not change the measures it induces on groups (e.g., see [MP16, Fact 2.5]), and thus

**Fact 1.2.** *If $w_1\overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim}w_2$ then $w_1$ and $w_2$ induce the same measure on every compact group.*

For example, $xyxy^{-1}\overset{\mathrm{Aut}(\mathbf{F})}{\sim}x^2y^2$ and so the expected value of $\psi$ under the $xyxy^{-1}$-measure is $\frac{(\mathcal{FS}_\psi)^2}{\psi(1)}$. More generally, every non-trivial word $w\in\mathbf{F}_r$ in which every letter appears exactly twice is mapped by $\mathrm{Aut}(\mathbf{F}_r)$ to one of the words in Theorem 1.1. By the classification of surfaces, the suitable word is determined by the homeomorphism type of the surface obtained from gluing the sides of a $|w|$-gon according to the letters of $w$ (see, for instance, [Sti12, Chapter 1.3]). The expected value of irreducible characters is then described by the suitable case in the theorem.

Several mathematicians, including A. Amit, T. Gelander, A. Lubotzky, A. Shalev and U. Vishne, conjecture that the converse is also true and that every other pair of words is "measurably separable":

**Conjecture 1.3.** *Let $w_1,w_2\in\mathbf{F}_r$. If $w_1$ and $w_2$ induce the same measure on every compact group, then $w_1\overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim}w_2$.*

[1] Throughout this paper, the letters $x$, $y$, and also $x_i$ and $y_j$ denote different generators in the same basis of $\mathbf{F}_r$.

This conjecture appears in the literature in a stronger form, where $w_1$ and $w_2$ are only assumed to induce the same measure on every *finite* group – see [AV11, Question 2.2], [Sha13, Conjecture 4.2] and [PP15, Section 8].

Conjecture 1.3 seems to be extremely challenging. Our focus here, instead, is on special cases, where $w_1$ is some fixed word. A case which attracted considerable attention was that of primitive words, namely the $\mathrm{Aut}(\mathbf{F}_r)$-orbit containing the free generators of $\mathbf{F}_r$. This special case was settled by the second author and Parzanchevski [PP15], who showed that $w$ induces the uniform measure on the symmetric group $S_N$ for all $N$ if and only if $w$ is primitive. To the best of our knowledge, the only $\mathrm{Aut}(\mathbf{F}_r)$-orbits for which the expected value of irreducible characters can be explicitly determined for every compact group, are the primitive case (where all characters but the trivial one have expectation zero) and surface words as in Theorem 1.1 – see also [PS14] and the references therein. In this sense, surface words are a natural next case to consider. And, indeed, we settle Conjecture 1.3 when $w_1$ is a surface word:

**Theorem 1.4.** *Let* $w \in \mathbf{F}_r$.

1. *If* $w$ *induces the same measure as* $[x_1,y_1]\cdots[x_g,y_g]$ *on every compact group, then* ($r \geq 2g$, *and*) $w \overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim} [x_1,y_1]\cdots[x_g,y_g]$.
2. *If* $w$ *induces the same measure as* $x_1^2\cdots x_g^2$ *on every compact group, then* ($r \geq g$, *and*) $w \overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim} x_1^2\cdots x_g^2$.

*Remark* 1.5. Let us mention another new result in the same spirit as Theorem 1.4. Let $w_0$ be either a primitive power, say $w_0 = x_1^m$, or any power of the simple commutator $w_0 = [x,y]^m$. In a forthcoming paper [HMP19], Hanani, Meiri and the second author show that if a word $w$ induces the same measure as $w_0$ on every *finite* group, then $w \overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim} w_0$. In the case of the simple commutator $[x,y]$, this strengthens Theorem 1.4, as it only relies on measures on finite groups. On the other hand, unlike the current paper where we use specific families of groups ($\mathcal{U}(N)$ and generalized permutation groups), the finite groups relied upon in [HMP19] are not specific families.

## Word measures on $\mathcal{U}(N)$, on $\mathcal{O}(N)$, and on generalized symmetric groups

Our proof of Theorem 1.4 relies on the measures induced by words on unitary groups, on orthogonal groups, and on generalized symmetric groups. While we study the former two in separate papers, we study the latter one here. In fact, it is enough to consider the expected value of the standard character, namely, the expected value of the trace, in all three families of groups[2]. We denote this expected value of the trace of a $w$-random element in a matrix group $G$ by $\mathcal{T}r_w(G)$. $\mathcal{T}r_w(G)$

To present these results, we introduce some notation. Recall that given a free group $\mathbf{F}$, the commutator subgroup $[\mathbf{F},\mathbf{F}]$ is the kernel of the homomorphism $\mathbf{F} \twoheadrightarrow \mathbb{Z}^{\mathrm{rank}(\mathbf{F})}$ mapping every generator to a different element of the standard generating set of $\mathbb{Z}^{\mathrm{rank}(\mathbf{F})}$. Similarly, for $m \in \mathbb{Z}_{\geq 2}$, let $C_m \overset{\mathrm{def}}{=} \mathbb{Z}/m\mathbb{Z}$ be the cyclic group of order $m$, and denote by $K_m(\mathbf{F})$

$$K_m(\mathbf{F}) \overset{\mathrm{def}}{=} \ker\left(\mathbf{F} \twoheadrightarrow C_m^{\mathrm{rank}(\mathbf{F})}\right)$$

the kernel of the homomorphism $\mathbf{F} \twoheadrightarrow C_m^{\mathrm{rank}(\mathbf{F})}$ mapping every generator to a different unit vector in $C_m^{\mathrm{rank}(\mathbf{F})}$. Note that even though the homomorphism $\mathbf{F} \twoheadrightarrow C_m^{\mathrm{rank}(\mathbf{F})}$ depends on the choice of basis, its kernel does not, and it consists of all words where $m$ divides the total exponent of every generator. For efficiency of presenting our results, we also denote $K_\infty(\mathbf{F}) \overset{\mathrm{def}}{=} [\mathbf{F},\mathbf{F}]$. $K_\infty(\mathbf{F})$

Is it a standard fact that $w \in \mathbf{F}$ is a product of squares if and only if $w \in K_2(\mathbf{F})$. Likewise, $w$ is a product of commutators if and only if $w \in K_\infty(\mathbf{F}) = [\mathbf{F},\mathbf{F}]$. We can now extract from [MP18, MP19] the results we need here.

**Definition 1.6.** Let $w \in \mathbf{F}_r$. The *commutator length* of $w \in \mathbf{F}_r$ is defined as $\mathrm{cl}(w)$

$$\mathrm{cl}(w) \overset{\mathrm{def}}{=} \min\left\{ g \;\middle|\; \begin{array}{c} \exists u_1,v_1,\ldots,u_g,v_g \in \mathbf{F}_r \text{ s.t.} \\ w = [u_1,v_1]\cdots[u_g,v_g] \end{array} \right\}.$$

[2]Similarly, the standard character of the symmetric group was sufficient for the result in [PP15] considering the primitive orbit.

In particular, if $w \notin [\mathbf{F}_r, \mathbf{F}_r]$, then $\mathrm{cl}(w) = \infty$. Similarly, the *square length* of $w \in \mathbf{F}_r$ is defined as  $\mathrm{sql}(w)$

$$\mathrm{sql}(w) \stackrel{\text{def}}{=} \min \left\{ g \;\middle|\; \begin{array}{c} \exists u_1, \ldots, u_g \in \mathbf{F}_r \text{ s.t.} \\ w = u_1^2 \cdots u_g^2 \end{array} \right\}.$$

In particular, if $w \notin K_2(\mathbf{F}_r)$, then $\mathrm{sql}(w) = \infty$.

**Theorem 1.7.** *[MP18, Corollary 1.8] Fix $w \in \mathbf{F}_r$ and consider the measure it induces on the unitary groups $\mathcal{U}(N)$. The expected trace of a $w$-random unitary matrix in $\mathcal{U}(N)$ satisfies*

$$\mathcal{T}r_w(\mathcal{U}(N)) = O\left(N^{1-2\cdot\mathrm{cl}(w)}\right).$$

**Theorem 1.8.** *[MP19] Fix $w \in \mathbf{F}_r$ and consider the measure it induces on the orthogonal groups $\mathcal{O}(N)$. The expected trace of a $w$-random orthogonal matrix in $\mathcal{O}(N)$ satisfies*

$$\mathcal{T}r_w(\mathcal{O}(N)) = O\left(N^{\tau(w)}\right),$$

*where $\tau(w) = \max(1 - 2\mathrm{cl}(w), 1 - \mathrm{sql}(w))$.*

In the current paper we obtain similar results for generalized symmetric groups. Specifically, let $\mathcal{S}^1 \wr S_N$ denote the wreath product of $\mathcal{S}^1$ with $S_N = \mathrm{Sym}(N)$, namely, this is the subgroup of $\mathrm{GL}_N(\mathbb{C})$ consisting of matrices with exactly one non-zero entry in every row and column and all non-zero entries having absolute value 1. Likewise, for $m \in \mathbb{Z}_{\geq 2}$, let $C_m \wr S_N$ be the wreath product[3] of $C_m$, the cyclic group of order $m$, with $S_N$. This is the subgroup of $\mathcal{S}^1 \wr S_N$ where all non-zero entries are $m$-th roots of unity. Note that when $m = 2$, the group $C_2 \wr S_N$ is the signed symmetric group, known also as the hyper-octahedral group or the Coxeter group of type $B_N = C_N$.  $\mathcal{S}^1 \wr S_N$  $C_m \wr S_N$

The first observation we make is that the expected value under the $w$-measure of the trace of any of these groups is given by a rational function in $N$:

**Lemma 1.9.** *Fix $w \in \mathbf{F}_r$ and let $G(N) = C_m \wr S_N$ for some fixed $m \in \mathbb{Z}_{\geq 2}$ or $G(N) = \mathcal{S}^1 \wr S_N$. Then there is some rational function $f \in \mathbb{Q}(x)$, such that for every large enough $N$, $\mathcal{T}r_w(G(N)) = f(N)$.*

For example, if $w = x^2y^3x^2y^{-1}$ and $m = 2$, then $\mathcal{T}r_w(C_2 \wr S_N) = \frac{3N-4}{N(N-1)}$ for all $N \geq 2$. The proof of this lemma appears in Section 3.1. We stress that a statement of this sort is not surprising: a similar statement is known to hold for various families of characters of the groups $G(N)$ when $G(N) = S_N$ [Nic94, LP10], when $G(N) = \mathcal{U}(N)$ [MP18], when $G(N) = \mathcal{O}(N)$ or $\mathcal{S}p(N)$ [MP19], or when $G(N) = \mathrm{GL}_N(\mathbb{F}_q)$ is the general linear group over the finite field $\mathbb{F}_q$ [PW19].

Our main result with respect to word measures on these generalized symmetric groups revolves around the leading term of the rational expression from Lemma 1.9. The exponent of the leading term is described by the number in the following definition.

**Definition 1.10.** Let $w \in \mathbf{F}_r$ and $m \in \mathbb{Z}_{\geq 2}$ or $m = \infty$. Denote

$$\chi_m(w) \stackrel{\text{def}}{=} 1 - \min \left\{ \mathrm{rank}(H) \;\middle|\; \begin{array}{c} H \leq \mathbf{F}_r \\ w \in K_m(H) \end{array} \right\}. \tag{1.1}$$

If the set in the right hand side of (1.1) is empty, we set $\chi_m(w) = -\infty$.

In words, we look for subgroups $H \leq \mathbf{F}_r$ of smallest rank such that $K_m(H)$ contains $w$, and take their Euler characteristic which equals $1 - \mathrm{rank}(H)$. It is easy to see that $K_m(H) \leq K_m(\mathbf{F})$ whenever $H \leq \mathbf{F}$, and so if $\chi_m(w)$ is not $-\infty$, it is in fact at least $1 - r$. Thus, in $\mathbf{F}_r$, the function $\chi_m$ takes values in $\{1, 0, -1, \ldots, 1-r\} \cup \{-\infty\}$, where $\chi_m(w) = 1 \Leftrightarrow w = 1$ and $\chi_m(w) = 0$ if and only if $w = u^m$ for some $1 \neq u \in \mathbf{F}_r$.

To illustrate, $w = x^2y^3x^2y^{-1}$ is not a proper power, so $\chi_m(w) < 0$. For $m = 2$, $w \in K_2(H)$ for $H = \langle x, y \rangle$ (as well as for $H = \langle x^2, y \rangle$ and for $H = \langle x^2y, y^2 \rangle$) and so $\chi_2(w) = -1$ . For $m \geq 3$ or $m = \infty$, $\chi_m(w) = -\infty$. As another example, consider the orientable surface word $w = [x_1, y_1] \cdots [x_g, y_g]$. Then $w \in K_m(\langle x_1, y_1, \ldots, x_g, y_g \rangle)$ for every $m \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, and one can show that $\chi_m(w) = 1 - 2g$.

[3]The group $C_m \wr S_N$ is sometimes denoted $S(m, N)$ – see, for example, https://en.wikipedia.org/wiki/Generalized_symmetric_group.

**Theorem 1.11.** *Let $w \in \mathbf{F}_r$ and $m \in \mathbb{Z}_{\geq 2}$ or $m = \infty$. If $m \in \mathbb{Z}_{\geq 2}$, consider a $w$-random matrix in the group $G(N) = C_m \wr S_N$, and if $m = \infty$ consider a $w$-random matrix in $G(N) = S^1 \wr S_N$. Then*

$$\mathcal{T}r_w(G(N)) = C \cdot N^{\chi_m(w)} + O\left(N^{\chi_m(w)-1}\right), \tag{1.2}$$

*where $C$ is a natural number counting the number of subgroups $H \leq \mathbf{F}_r$ with $\chi_m(w) = 1 - \text{rank}(H)$ and $w \in K_m(H)$. In particular, $\mathcal{T}r_w(G(N))$ vanishes if $\chi_m(w) = -\infty$.*

Namely, the coefficient $C$ in (1.2) counts the number of the subgroups $H$ demonstrating the value of $\chi_m(w)$ determined in (1.1). This number is always finite – see Section 3.1. In fact, we have a more detailed result which is required for the proof of Theorem 1.4 – see Section 3.2. Theorem 1.11 is similar in spirit to [PP15, Theorem 1.8], where $\mathcal{T}r_w(S_N)$ is analyzed. The group $S_N$ can be regarded as the $m = 1$ case in the current terminology. The analog there of $\chi_m(w)$ is the "primitivity rank" of $w$. Moreover, the more detailed version of Theorem 1.11, Theorem 3.5 below, relies on much of the analysis from [PP15]. A crucial difference between the current groups and $S_N$ is that the standard $N$-dimensional representation is reducible for $S_N$ but irreducible for the groups in Theorem 1.11. We further explain these connections in Sections 2 and 3.1.

### Overview of the proof

The proof of Theorem 1.4 uses both the measures on the classical groups $\mathcal{U}(N)$ and $\mathcal{O}(N)$, and the measures on generalized symmetric groups. The roles they play are somewhat complement. Let us illustrate these complementing roles by considering the commutator length of a word. Let $w \in \mathbf{F}_r$, and consider the measure it induces on $\mathcal{U}(N)$. If $\mathcal{T}r_w(\mathcal{U}(N)) = \Theta\left(N^{1-2g}\right)$, Theorem 1.7 yields an upper bound on the commutator length: $\text{cl}(w) \leq g$.

In contrast, if $w = [u_1, v_1] \cdots \left[u_{\text{cl}(w)}, v_{\text{cl}(w)}\right]$ then $w \in K_\infty(H) = [H, H]$, where $H = \left\langle u_1, v_1, \ldots, u_{\text{cl}(w)}, v_{\text{cl}(w)}\right\rangle$ which has rank at most $2\text{cl}(w)$ and thus $\chi_\infty(w) \geq 1 - \text{rank}(H) \geq 1 - 2\text{cl}(w)$. Hence if $\mathcal{T}r_w\left(\mathcal{S}^1 \wr S_N\right) = \Theta\left(N^{1-2g}\right)$, we deduce the lower bound $\text{cl}(w) \geq g$.

If $w$ induces the same measure as $[x_1, y_1] \cdots [x_g, y_g]$ on every compact group, then, in particular, $\mathcal{T}r_w(\mathcal{U}(N)) = \mathcal{T}r_w\left(\mathcal{S}^1 \wr S_N\right) = N^{1-2g}$. The preceding two paragraphs then show that $\text{cl}(w) = g$. Moreover, they show the group $H$ from the preceding paragraph has rank exactly $2g$, and so $u_1, v_1, \ldots, u_{\text{cl}(w)}, v_{\text{cl}(w)}$ are free words, namely, there is no non-trivial relation on them. Together with Theorem 3.5 below (a strengthening of Theorem 1.11), it is possible to deduce that $u_1, v_1, \ldots, u_{\text{cl}(w)}, v_{\text{cl}(w)}$ are, in fact, part of a basis of $\mathbf{F}_r$, and therefore $w \overset{\text{Aut}(\mathbf{F})}{\sim} [x_1, y_1] \cdots [x_g, y_g]$.

The paper is organized as follows. Section 2 contains some background regarding measures induced by surface words, as well as background regarding word measures on $S_N$ and some results from [PP15] we use here. It also introduces the notions of algebraic extensions and of core graphs. In Section 3 we analyze word measures on generalized symmetric groups and prove Lemma 1.9, Theorem 1.11, and the stronger Theorem 3.5. We prove Theorem 1.4 in Section 4 and conclude with some open questions in Section 5.

### Notation

We use the following asymptotic notation. Let $f, g \colon \mathbb{Z}_{\geq 1} \to \mathbb{R}$ be two functions defined on the positive integers. We write

- $f = O(g)$ if there is a constant $C > 0$ such that $|f(n)| \leq C \cdot g(n)$ for every large enough $n$,
- $f = \Omega(g)$ if there is a constant $C > 0$ such that $|f(n)| \geq C \cdot g(n)$ for every large enough $n$, and
- $f = \Theta(g)$ if both $f = O(g)$ and $f = \Omega(n)$.

## 2 Preliminaries

### Measures induced by surface words

We begin this section with some remarks regarding the proof of Theorem 1.1. We have already mentioned a reference [Fro96] for the case where $G$ is finite and $w = [x, y]$. In fact, this case is at the level of an exercise for an arbitrary compact group $G$, as long as one is aware of the following classical facts: matrix coefficients of unitary realizations of all irreducible representations of a compact group form an orthogonal basis for the space of complex functions on $G$, and the $L^2$-norm of a matrix coefficient of a $d$-dimensional irreducible representation is $\frac{1}{d}$.

The case of $w = x^2$ and $G$ finite was first proved in [FS06]. For an English proof see [Isa76, Chapter 4]. Although the book [Isa76] deals with finite groups, this proof applies just as well to general compact groups.

Finally, for $g \geq 2$, note that when the letters appearing in $w_1$ are distinct from those in $w_2$, then the $w_1w_2$-measure on $G$ is the convolution of the $w_1$-measure and the $w_2$-measure, and using the fact that a $w$-measure is always invariant under conjugation, we get that $\mathbb{E}_{w_1w_2}(\psi) = \frac{1}{\psi(1)}\mathbb{E}_{w_1}(\psi) \cdot \mathbb{E}_{w_2}(\psi)$ for every irreducible character $\psi$ of $G$. This explains the complete statement of Theorem 1.1. See also [PS14] and the references therein.

## Expected traces in $S_N$

Next, we extract some terminology and results from [PP15] that are needed here. That paper analyzes $\mathcal{T}r_w(S_N)$, the expected trace of a $w$-random permutation in $S_N$, where the permutation is thought of as an $N \times N$ matrix. In other words, it studies the expected number of fixed points in a $w$-random permutation. We remark that word measures on $S_N$ alone do not suffice to establish Theorem 1.4: all irreducible characters of $S_N$ are afforded by real representations, and so the words $[x, y]$ and $x^2y^2$ induce the exact same measure on $S_N$ for all $N$.

Let $|w|$ denote the length of the reduced form of $w$. A first observation in the study of $\mathcal{T}r_w(S_N)$, going back to Nica [Nic94], is that for $N \geq |w|$, $\mathcal{T}r_w(S_N)$ is a rational expression in $N$. Unlike the other groups mentioned above, this $N$-dimensional representation of $S_N$ is reducible: it is the sum of the trivial representation and an $(N-1)$-dimensional irreducible representation. It is thus not surprising that the rational expression for $\mathcal{T}r_w(S_N)$ has a contribution of 1 coming from the trivial representation, and the interesting part is the deviation from 1. This deviation is measured by the "primitivity rank" of a word $w \in \mathbf{F}_r$, denoted $\pi(w)$, which was first introduced in [Pud14]. Recall that an element of a free group is called *primitive* if it belongs to some basis (free generating set). The primitivity rank of $w \in \mathbf{F}_r$ is the following number:

$$\pi(w) \stackrel{\text{def}}{=} \min\{\text{rank}(H) \,|\, w \in H \leq \mathbf{F}_r,\ w \text{ is not primitive in } H\}. \tag{2.1}$$

The functions $\chi_m(w)$ defined above are closely related to $\pi(w)$. In fact, one can give a single definition which applies to all these functions simultaneously. Indeed, for $m \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$ define

$$\chi'_m(w) = 1 - \min\{\text{rank}(H) \,|\, H \leq \mathbf{F}_r, w \in K_m(H),\ w \text{ is not primitive in } H\}.$$

Now $\chi'_1(w) = 1 - \pi(w)$ as $K_1(H) = H$, and for $m \neq 1$, $\chi'_m(w) = \chi_m(w)$ because all elements of $K_m(H)$ are automatically non-primitive in $H$. These different functions of words also share some properties. For instance, for all $m \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$, $\chi'_m(w)$ takes values in $\{1, 0, -1, \ldots, 1-r\} \cup \{-\infty\}$ – this[4] was explained above for $m \neq 1$, and for $m = 1$, this is [Pud14, Corollary 4.2]. The role of $\pi(w)$ in the study of $\mathcal{T}r_w(S_N)$ is also analogous to the role of $\chi_m(w)$ in Theorem 1.11:

**Theorem 2.1.** *[PP15, Theorem 1.8] Let $w \in \mathbf{F}_r$. Then*

$$\mathcal{T}r_w(S_N) = 1 + C \cdot N^{1-\pi(w)} + O\left(N^{-\pi(w)}\right),$$

*where $C \in \mathbb{Z}_{\geq 1}$ is the number of subgroups $H \in \mathbf{F}_r$ of rank $\pi(w)$ containing $w$ as a non-primitive element. In particular, $\mathcal{T}r_w(S_N) \equiv 1$ for all $N$ if and only if $\pi(w) = \infty$, which holds if and only if $w$ is primitive.*

## Random subgroups in $S_N$

The results in [PP15] apply not only to random elements of $S_N$ with measures induced by words $w \in \mathbf{F}_r$, but more generally, to random subgroups of $S_N$ with measures induced by subgroups $H \leq \mathbf{F}_r$. Given $H$, sample a random subgroup of $S_N$ by choosing a homomorphism $\varphi \in \text{Hom}(\mathbf{F}_r, S_N)$ uniformly at random and

[4] To be precise, $\chi_\infty$ is never zero: a cyclic group has a trivial commutator subgroup.

considering $\varphi(H) \le S_N$. When $H = \langle w \rangle$, the resulting random subgroup is the one generated by a $w$-random permutation.

If $H \le J$ are free groups, we say that $J$ is a *free extension* of $H$, or that $H$ is a *free factor* of $J$, and denote $H \overset{*}{\le} J$, if some (and therefore every) basis of $H$ can be extended to a basis of $J$. Clearly, for $w \neq 1$, $w$ is primitive in $J$ if and only if $\langle w \rangle \overset{*}{\le} J$. Hence, the following notion of primitivity rank for subgroups generalizes (2.1). For $H \le \mathbf{F}_r$, the primitivity rank of $H$ is defined to be $H \overset{*}{\le} J$

$$\pi(H) \overset{\text{def}}{=} \min\left\{\text{rank}(J) \,|\, H \le J \le \mathbf{F}_r, H \text{ is not a free factor of } J\right\}.$$

We can now state the more general form of Theorem 2.1.

**Theorem 2.2.** *[PP15, Theorem 1.8] Let $H \le \mathbf{F}_r$ be a finitely generated subgroup, and let $\varphi \in \text{Hom}(\mathbf{F}_r, S_N)$ be a uniformly random homomorphism. The expected number of points in $\{1,\ldots,N\}$ fixed by all elements of the subgroup $\varphi(H)$ is*

$$N^{1-\text{rank}(H)} + C \cdot N^{1-\pi(H)} + O\left(N^{-\pi(H)}\right),$$

*where $C$ is the number of subgroups $J \le \mathbf{F}_r$ satisfying $\text{rank}(J) = \pi(H)$ and containing $H$ but not as a free factor.*

*In particular, this value is $N^{1-\text{rank}(H)}$ for all $N$ if and only if $\pi(H) = \infty$, which holds if and only if $H \overset{*}{\le} \mathbf{F}_r$.*

## Algebraic extensions

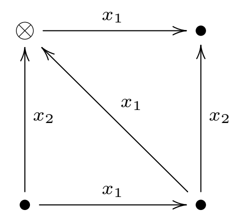
Next, we describe the notion of *algebraic extensions* in free groups which is used in Section 3.2 below. Let $\mathbf{F}$ be a free group and $H, J \le \mathbf{F}$ two subgroups. We call $J$ an algebraic extension of $H$, denoted $H \le_{\text{alg}} J$, if and only if $H \le J$ and there is no intermediate proper free factor of $J$, namely, if whenever $H \le M \overset{*}{\le} J$, we must have $M = J$. To give a sense of this notion, we mention some of its properties: algebraic extensions form a partial order on the set of subgroups of $\mathbf{F}$; for every extension of free groups $H \le J$ there is a unique intermediate subgroup $A$ satisfying $H \le_{\text{alg}} A \overset{*}{\le} J$; and every finitely generated subgroup $H$ of $\mathbf{F}$ has finitely many algebraic extensions. See the survey [MVW07] or Section 4 of [PP15] for more details. $H \le_{\text{alg}} J$

In the language of algebraic extensions, $\pi(H)$ is the smallest rank of a proper algebraic extension of $H$, and $\pi(w)$ is the smallest rank of a proper algebraic extension of $\langle w \rangle$.

## Core graphs

Recall that we have a fixed basis $x_1,\ldots,x_r$ for $\mathbf{F}_r$. Call it $X$. Associated with every (finitely generated) subgroup $H$ of $\mathbf{F}_r$ is a rooted, directed and edge-labeled (finite) graph, where the edges are labeled by $x_1,\ldots,x_r$. This graph, denoted $\Gamma_X(H)$, is called the *(Stallings) core graph* of $H$ and was introduced in [Sta83]. It can be obtained from the Schreier graph depicting the right action of $\mathbf{F}_r$ on $H\backslash\mathbf{F}_r$, the right cosets of $H$ in $\mathbf{F}_r$, by trimming all "hanging trees". For more details we refer the reader to [PP15, Section 3]. We illustrate the concept in Figure 2.1. $\Gamma_X(H)$

Figure 2.1: The core graph $\Gamma_X(H)$ where $H = \left\langle x_1 x_2^{-1} x_1, x_1^{-2} x_2 \right\rangle \le \mathbf{F}_2$.




Let us mention here a few basic facts about core graphs and some further notations that we will need below. The elements of $H$ correspond exactly to the non-backtracking closed paths at the root of $\Gamma_X(H)$. The labels and directions of the edges give rise to a graph-morphism to the bouquet of $r$ directed loops, labeled by $x_1,\ldots,x_r$, and this morphism is always an immersion. In other words, every vertex of $\Gamma_X(H)$ has at most one outgoing edge with a given label, and at most one incoming edge with a given label.

A morphism of rooted, directed and edge labeled graphs from $\Gamma_X(H)$ and $\Gamma_X(J)$ exists if and only if $H \le J$. When this morphism is surjective, we say that $H$ "*X-covers*" $J$, and denote $H \le_{\overrightarrow{X}} J$. This relation constitutes a partial order on the set of finitely generated subgroups of $\mathbf{F}_r$, a partial order which depends on the choice of basis $X$. The easiest way to explain why there is a rational expression for $\mathcal{T}r_w(S_N)$ and, moreover, to compute this formula explicitly, is by considering the finite set

$\le_{\overrightarrow{X}}$

$[H,\infty)_{\overrightarrow{X}}$

$$[H,\infty)_{\overrightarrow{X}} \overset{\text{def}}{=} \left\{ H \le \mathbf{F}_r \,\middle|\, \langle w\rangle \le_{\overrightarrow{X}} H \right\}$$

of subgroups which are $X$-covered by the subgroup $\langle w\rangle$ (see [Pud14, Section 5]). We shall use these graphs below to prove Lemma 1.9 and Theorem 1.11.

# 3 Expected trace in generalized symmetric groups

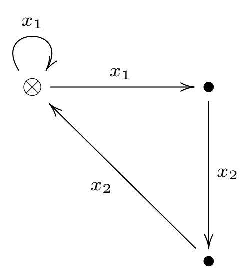
## 3.1 Rational expressions and their leading term

Fix $w \in \mathbf{F}_r$ and let $G(N)$ be one of the groups $C_m \wr S_N$ ($m \in \mathbb{Z}_{\ge 2}$), $\mathcal{S}^1 \wr S_N$, or merely $S_N$, realized as $N \times N$ complex matrices. If $w = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \cdots x_{i_\ell}^{\varepsilon_\ell} \in \mathbf{F}_r$ (here $i_1, \ldots, i_\ell \in \{1, \ldots, r\}$ and $\varepsilon_1, \ldots, \varepsilon_\ell \in \{\pm 1\}$), we analyze the following expression:

$$\mathcal{T}r_w(G(N)) = \int_{A_1,\ldots,A_r \in G(N)} \mathrm{tr}\left(w(A_1,\ldots,A_r)\right) = \sum_{j_1,\ldots,j_\ell=1}^{N} \int_{A_1,\ldots,A_r \in G(N)} \left[A_{i_1}^{\varepsilon_1}\right]_{j_1,j_2} \left[A_{i_2}^{\varepsilon_2}\right]_{j_2,j_3} \cdots \left[A_{i_\ell}^{\varepsilon_\ell}\right]_{j_\ell,j_1}, \tag{3.1}$$

where $A_1, \ldots, A_r$ are independent Haar-uniform elements of $G(N)$. In all cases considered but $\mathcal{S}^1 \wr S_N$ this is the uniform measure on $G(N)$. The Haar measure on $\mathcal{S}^1 \wr S_N$ is given by a uniform distribution on $S_N$ to determine the non-zero entries and independent Lebesgue measure on every non-zero entry of the matrix.

Consider an assignment of values in $\{1, \ldots, N\}$ to the indices $j_1, \ldots, j_\ell$. Every assignment induces a partition on $\{1, \ldots, \ell\}$, where two indices $s$ and $t$ belong to the same block if and only if $j_s = j_t$. Such a partition can be describe by a rooted, directed, edge-labeled graph as follows: the vertices correspond to the blocks in the partition on $\{1, \ldots, \ell\}$, the root is the block containing 1, and for every $t = 1, \ldots, \ell$ there is a directed edge labeled $x_{i_t}$ connecting the block of $j_t$ with the block of $j_{(t+1) \bmod \ell}$, and directed towards the $j_{(t+1) \bmod \ell}$ block if $\varepsilon_t = 1$ or towards the $j_t$ block in case $\varepsilon_t = -1$. There is at most one $x_i$-edge directed from a vertex $u$ to a vertex $v$. For example, if $w = x_1^2 x_2^2$ and the assignment is $(j_1, j_2, j_3, j_4) = (1, 1, 3, 5)$, the graph is the following:




However, this assignment contributes zero to the summation in (3.1): in all groups considered here, there is exactly one non-zero entry in every column and every line, yet the assignment $(1, 1, 3, 5)$ leads to the integral over the monomial $[A_1]_{1,1} [A_1]_{1,3} [A_2]_{3,5} [A_2]_{5,1}$, which involves two entries from the same row of $A_1$ and is thus identically zero. This happens exactly when the graph associated with the assignment has a vertex with two out-going edges with the same label, or a vertex with two incoming edges with the same label. This shows that we can restrict our attention to assignments associated with graphs which are core graphs. Moreover, these graphs are precisely the graphs which are $X$-covered by $\langle w\rangle$, namely the graphs $\Gamma_X(H)$ for $H \in [\langle w\rangle, \infty)_{\overrightarrow{X}}$.

We can now group together all assignments leading to the same core graph $\Gamma_X(H)$, and see that the contribution of all these assignments is given by a rational function in $N$ (which depends on the family of groups we consider). Because the set $[H,\infty)_{\overrightarrow{X}}$ is finite, this leads to a rational expression for $\mathcal{T}r_w(G(N))$

for families of generalized symmetric groups. The number of assignments associated with a given $\Gamma_X(H)$ is $N(N-1)\cdots(N-\#V(H)+1)$, where $\#V(H)$ denotes the number of vertices in $\Gamma_X(H)$. The probability that the uniformly random $A_i \in G(N)$ has non-zero entries which correspond to a given assignment associated with $\Gamma$ is precisely $\frac{1}{N(N-1)\cdots(N-\#E_i(H)+1)}$, where $\#E_i(H)$ is the number of $x_i$-edges in $\Gamma_X(H)$. Overall, for $H \in [\langle w\rangle, \infty)_{\vec{X}}$, if $N \geq \#E_i(H)$ for all $i$, the contribution of $H$ to (3.1) is[5] $L^X_{H,\mathbf{F}_r}(N)$

$$L^X_{H,\mathbf{F}_r}(N) \overset{\text{def}}{=} \frac{N(N-1)\cdots(N-\#V(H)+1)}{\prod_{i=1}^r N(N-1)\cdots(N-\#E_i(H)+1)}$$

times the expected value of product of non-zero entries of $A_1,\ldots,A_r$ involved in the monomial in (3.1). In the case of $S_N$, these non-zero entries are identically 1, and so, as depicted in [Pud14, Section 5] (and also, less explicitly, in [Nic94]),

$$\mathcal{T}r_w(S_N) = \sum_{H\in[\langle w\rangle,\infty)_{\vec{X}}} L^X_{H,\mathbf{F}_r}(N). \tag{3.2}$$

For example, in the case of $w = x_1^2x_2^2$, there are precisely 7 subgroups in $[\langle w\rangle, \infty)_{\vec{X}}$, and the total contribution is $1+\frac{1}{N-1}$, holding for $N \geq 2$. The detailed computation for $w = [x_1, x_2]$ is depicted in [Pud14, Page 53].

For the other groups considered here, the non-zero entries are not identically one and actually have zero expectation. So often, the contribution of an assignment to (3.1) vanishes even when the assignment correspond to some core graph. For example, in the case of the group $C_3 \wr S_N$, an assignment gives a non-zero contribution if and only if it corresponds to a core graph, *and* every entry is repeated in the monomial some multiple of 3 times, when we count with signs. E.g., if the entry $A_{3,4}$ appears in the monomial in (3.1), it must appear a total number of 0 times as in $\cdots A_{3,4}\cdots A_{3,4}^{-1}\cdots$, a total number of $-3$ times as in $\cdots A_{3,4}^{-1}\cdots A_{3,4}^{-1}\cdots A_{3,4}^{-1}\cdots A_{3,4}\cdots A_{3,4}^{-1}$, and so on. For $A \in C_3 \wr S_N$ uniformly random and every $q \in \mathbb{Z}$, conditioning on that $A_{3,4}$ is non-zero, the expected value of $[A_{3,4}]^q$ is $\mathbf{1}_{q\equiv 0 \pmod 3}$. Fortunately, this property is a feature of the core graphs and not only of the particular assignment: by definition, $H \in [\langle w\rangle, \infty)_{\vec{X}}$ if and only if $w \in H$ and every edge of $\Gamma_X(H)$ is covered by some edge of $\Gamma_X(\langle w\rangle)$ in the graph morphism $\Gamma_X(\langle w\rangle) \to \Gamma_x(H)$. In other words, the closed path at the root of $\Gamma_X(H)$ which corresponds to $w$ must go through every edge of the graph. The restriction that every non-zero entry repeats some multiple of 3 times in the monomial (counted with signs), is equivalent to that the path of $w$ goes through every edges a total signed number of times which is a multiple of 3. This generalizes to the following explicit form of Lemma 1.9:

**Lemma 3.1.** *Let $w \in \mathbf{F}_r$. For every $m \in \mathbb{Z}_{\geq 2}$ denote*

$$\mathcal{Q}_m(w) = \left\{ H \in [\langle w\rangle, \infty)_{\vec{X}} \;\middle|\; \begin{array}{c}\text{the number of times } w \text{ traverses every edge of } \Gamma_{\mathrm{X}}(\mathrm{H}) \\ \text{is a multiple of } m \text{ where traverses are counted with signs}\end{array} \right\}.$$

*Then for every large enough $N$,*

$$\mathcal{T}r_w(C_m \wr S_N) = \sum_{H\in\mathcal{Q}_m(w)} L^X_{H,\mathbf{F}_r}(N). \tag{3.3}$$

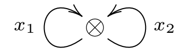
*Likewise, denote*

$$\mathcal{Q}_\infty(w) = \left\{ H \in [\langle w\rangle, \infty)_{\vec{X}} \;\middle|\; \begin{array}{c} w \text{ traverses every edge of } \Gamma_{\mathrm{X}}(\mathrm{H}) \\ \text{the same number of times in each direction}\end{array} \right\}.$$

*Then for every large enough $N$,*

$$\mathcal{T}r_w(\mathcal{S}^1 \wr S_N) = \sum_{H\in\mathcal{Q}_\infty(w)} L^X_{H,\mathbf{F}_r}(N). \tag{3.4}$$

[5] We use the notation $L^X_{H,\mathbf{F}_r}(N)$ which is used for this expression in [PP15].

For example, if $w = x_1^2 x_2^2$, six of the seven subgroups in $[\langle w \rangle, \infty)_{\vec{X}}$ belong to none of $\mathcal{Q}_m(w)$ ($m \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$). The remaining subgroup is $\mathbf{F}_2$ itself, with core graph $\Gamma =$ 

, which belongs to $\mathcal{Q}_2(w)$ but does not belong to $\mathcal{Q}_m(w)$ for $m \in \mathbb{Z}_{\geq 3} \cup \{\infty\}$. Thus, $\mathcal{T}r_{x_1^2 x_2^2}(C_2 \wr S_N) = \frac{1}{N}$ for every $N \geq 1$, whereas $\mathcal{T}r_{x_1^2 x_2^2}(C_m \wr S_N) = \mathcal{T}r_{x_1^2 x_2^2}(\mathcal{S}^1 \wr S_N) = 0$ for every $m \in \mathbb{Z}_{\geq 3}$ and $N \geq 1$. (Note how this agrees with Theorem 1.1.)

To say how large $N$ should be, one needs to go over the elements of $\mathcal{Q}_m(w)$. However, as every edge in $\Gamma_X(H)$ is covered at least twice (in the same direction or in different directions), the formulas in Lemma 3.1 holds at least for $N \geq \frac{1}{2} \max_{i \in [r]} \# E_i(w)$.

Let $H \leq \mathbf{F}_r$ be a subgroup containing $w$. Our next observation is that the conditions above regarding how many times $w$ traverses every edge of $\Gamma_X(H)$ are, in fact, algebraic:

**Lemma 3.2.** *Let $w \in \mathbf{F}_r$ and $H \in \mathbf{F}_r$ be a subgroup containing $w$, and let $m \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. The number of times, counted with signs, that $w$ traverses every edge in $\Gamma_X(H)$ is a multiple of $m$ (or 0 if $m = \infty$), if and only if $w \in K_m(H)$.*

*Proof.* Recall that $w \in K_m(H)$ if and only if when $w$ is written as a word in a fixed but arbitrary basis, the total exponent of every generator, counted with signs, is zero modulo $m$ (or zero if $m = \infty$). Let $T$ be any spanning tree in the core graph $\Gamma_X(H)$. There are $\operatorname{rank}(H)$ edges outside the tree, and after an arbitrary orientation of these $\operatorname{rank}(H)$ edges, we obtain a basis for $H$: the element associated with the oriented edge $e$ is the one corresponding to the closed path which goes from the root of $\Gamma_X(H)$ to the origin of $e$ through $T$, traverses $e$, and returns to the root through $T$. If $w$ traverses every edge a multiple of $m$ times, then any choice of spanning tree shows that $w \in K_m(H)$.

Conversely, assume that $w \in K_m(H)$, and let $e$ be an edge of $\Gamma_X(H)$. If $e$ is not a bridge (namely, not a separating edge the removal of which disconnects the graph), then there is a spanning tree not containing $e$ and thus $w$ traverses $e$ a multiple-of-$m$ times. If $e$ is a bridge, then every closed path traverses it in a "balanced" fashion, namely, the same number of times in each of the two directions. ☐

**Corollary 3.3.** *For $m \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$,*

$$\mathcal{Q}_m(w) = \left\{ H \in [\langle w \rangle, \infty)_{\vec{X}} \,\middle|\, w \in K_m(H) \right\}.$$

We can now complete the proof of Theorem 1.11 and show that for $G(N) = \mathcal{S}^1 \wr S_N$ (when $m = \infty$) or $G(N) = \mathcal{T}r_w(C_m \wr S_N)$ (for $m \in \mathbb{Z}_{\geq 2}$), $\mathcal{T}r_w(G(N)) = C \cdot N^{\chi_m(w)} + O\left(N^{\chi_m(w)-1}\right)$ with $C$ counting the number of subgroups $H \leq \mathbf{F}_r$ of rank $1 - \chi_m(w)$ with $w \in K_m(H)$.

*Proof of Theorem 1.11.* Let $m \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ and $G(N) = C_m \wr S_N$ or $G(N) = \mathcal{S}^1 \wr S_N$ accordingly. The summand corresponding to $H \in \mathcal{Q}_m(w)$ in (3.3) or in (3.4) has leading term $N^{\#V(H) - \#E(H)} = N^{1-\operatorname{rank}(H)}$, and so the summand is $N^{1-\operatorname{rank}(H)} + O\left(N^{-\operatorname{rank}(H)}\right)$. Overall, if $\chi'_m(w)$ is one minus the minimal rank of a subgroup in $\mathcal{Q}_m(w)$ and $C'$ the number of subgroups of this minimal rank in $\mathcal{Q}_m(w)$, then

$$\mathcal{T}r_w(G(N)) = C' \cdot N^{\chi'_m(w)} + O\left(N^{\chi'_m(w)-1}\right).$$

But if $H \leq \mathbf{F}_r$ satisfies $w \in K_m(H)$ but $H \notin \mathcal{Q}_m(w)$, then the morphism $\Gamma_X(\langle w \rangle) \to \Gamma_X(H)$ is *not* surjective, and the image of $\Gamma_X(\langle w \rangle)$ in $\Gamma_X(H)$ is a subgraph which is the core graph of some $M \in \mathcal{Q}_m(w)$. Moreover, $M$ is then a proper free factor of $H$ and thus has smaller rank. This shows that the subgroups $H \leq \mathbf{F}_r$ of minimal rank with the property that $w \in K_m(H)$ all belong to $\mathcal{Q}_m(w)$. In particular, their number is finite, $\chi'_m(w) = \chi_m(w)$ and $C' = C$. ☐

## 3.2 The second term of the rational expressions

Lemma 1.9 shows that for generalized symmetric groups $G(N)$, the expected trace $\mathcal{T}r_w(G(N))$ is given by a rational expression in $N$, and Theorem 1.11 gives an algebraic interpretation for the leading term of this expression. We now want to strengthen Theorem 1.11 and show that the rational expression does not only tell us about the subgroup $H \leq \mathbf{F}_r$ of minimal rank with the property that $w \in K_m(H)$, but also about the “second” minimal group. If there is more than one group of minimal rank, this is already captured by Theorem 1.11. But we want to deal also with the case that there is a unique subgroup as above of minimal rank.

To define the second minimal group, we do not rely on the set $\mathcal{Q}_m(w)$ the definition of which depends on the given basis $X$. Instead, we consider only *algebraic extensions* of $\langle w\rangle$ which also contain $w$ in their “$m$-kernel”. Namely, for $w\in\mathbf{F}_r$ and $m\in\mathbb{Z}_{\geq 2}\cup\{\infty\}$, denote $\mathcal{AE}_m(w)$

$$\mathcal{AE}_m(w)\overset{\text{def}}{=}\{A\leq\mathbf{F}_r\,|\,\langle w\rangle\leq_{\text{alg}}A\text{ and }w\in K_m(A)\}.$$

If $A$ is an algebraic extension of $\langle w\rangle$ then $\langle w\rangle$ $X$-covers $A$ for every basis $X$. Indeed, if $w\in A$ and $\langle w\rangle$ does not $X$-cover $A$ then the image of $\Gamma_X(\langle w\rangle)$ in $\Gamma_X(A)$ constitutes an intermediate subgroup which is a proper free factor of $A$. In particular, $\mathcal{AE}_m(w)\subseteq\mathcal{Q}_m(w)$. Moreover, all subgroups $H$ of minimal rank with $w\in K_m(H)$ are algebraic extensions of $\langle w\rangle$, because if $w\in K_m(H)$ and $w\in A\overset{*}{\leq}H$, then clearly $w\in K_m(A)$, so $H$ cannot be of minimal rank unless it is an algebraic extension. Thus

$$\chi_m(w)=1-\min_{A\in\mathcal{AE}_m(w)}\text{rank}(A).$$

**Definition 3.4.** Let $w\in\mathbf{F}_r$ and $m\in\mathbb{Z}_{\geq 2}\cup\{\infty\}$. If $|\mathcal{AE}_m(w)|\leq 1$, define $\chi_m^{(2)}(w)\overset{\text{def}}{=}-\infty$. Otherwise, let $A\in\mathcal{AE}_m(w)$ be an arbitrary subgroup of minimal rank, and define

$$\chi_m^{(2)}(w)\overset{\text{def}}{=}1-\min_{B\in\mathcal{AE}_m(w)\setminus\{A\}}\text{rank}(B).$$

Also, define $C_m^{(2)}(w)$ to be the number of subgroups $B$ in $\mathcal{AE}_m(w)\setminus\{A\}$ of minimal rank, namely, with $\chi_m^{(2)}(w)=1-\text{rank}(B)$.

Note that the numbers $\chi_m^{(2)}(w)$ and $C_m^{(2)}(w)$ do not depend on the arbitrary $A$. If the constant $C$ from Theorem 1.11 is at least two, then $\chi_m^{(2)}(w)=\chi_m(w)$ and $C_m^{(2)}(w)=C-1$. If $C=1$, then $\chi_m^{(2)}(w)<\chi_m(w)$.

**Theorem 3.5.** *Fix $w\in\mathbf{F}_r$ and let $m\in\mathbb{Z}_{\geq 2}$ in which case $G(N)=C_m\wr S_N$, or $m=\infty$ in which case $G(N)=\mathcal{S}^1\wr S_N$. Then*

$$\mathcal{T}r_w(G(N))=N^{\chi_m(w)}+C_m^{(2)}(w)\cdot N^{\chi_m^{(2)}(w)}+O\left(N^{\chi_m^{(2)}(w)-1}\right).$$

The point of Theorem 3.5 is that one can always read off from the expression for $\mathcal{T}r_w(G(N))$ the ranks of the two subgroups of minimal rank in $\mathcal{AE}_m(w)$. In particular, we get the following corollary which we use below in the proof of Theorem 1.4:

**Corollary 3.6.** *Fix $w\in\mathbf{F}_r$ and let $m\in\mathbb{Z}_{\geq 2}$ in which case $G(N)=C_m\wr S_N$, or $m=\infty$ in which case $G(N)=\mathcal{S}^1\wr S_N$. Then $\mathcal{T}r_w(G(N))$ is of the form $N^\chi$ (for some $\chi\in\mathbb{Z}$) if and only if $|\mathcal{AE}_m(w)|=1$.*

*Proof of Theorem 3.5.* We claim that

$$\mathcal{Q}_m(w)=\bigcup_{A\in\mathcal{AE}_m(w)}\left\{H\leq\mathbf{F}_r\,\middle|\,A\overset{*}{\leq}_{\overrightarrow{X}}H\right\}.$$

Indeed, as mentioned in Section 2 above, for every extension of free groups $H\leq J$, there is a unique intermediate subgroup $L$ such that $H\leq_{\text{alg}}A\overset{*}{\leq}J$ (see [PP15, Claim 4.5] for the proof in the finitely generated case, which is the case we need here). If $H\in\mathcal{Q}_m(w)$ and $A$ is the unique intermediate subgroup $\langle w\rangle\leq_{\text{alg}}A\overset{*}{\leq}H$ then $w\in K_m(A)$ and so $A\in\mathcal{AE}_m(w)$. Moreover, in this case $A\leq_{\overrightarrow{X}}H$ because the surjective core-graph morphism $\Gamma_X(\langle w\rangle)\to\Gamma_X(H)$ factors as $\Gamma_X(\langle w\rangle)\overset{\alpha_1}{\to}\Gamma_X(A)\overset{\alpha_2}{\to}\Gamma_X(H)$, so $\alpha_2$ must too be surjective. On the other hand, if $A\in\mathcal{AE}_m(w)$ and $A\overset{*}{\leq}_{\overrightarrow{X}}H$ then $\langle w\rangle\leq_{\overrightarrow{X}}A\leq_{\overrightarrow{X}}H$ and as “$\leq_{\overrightarrow{X}}$” is transitive, $\langle w\rangle\leq_{\overrightarrow{X}}H$. In addition, $w\in K_m(A)\leq K_m(H)$. Hence $H\in\mathcal{Q}_m(w)$.

Thus, we get that

$$\mathcal{T}r_w\left(G\left(N\right)\right)=\sum_{A\in\mathcal{AE}_m(w)}\left[\sum_{H\leq\mathbf{F}_r\text{ s.t. }A\overset{*}{\leq}_{\overrightarrow{X}}H}L^X_{H,\mathbf{F}_r}\left(N\right)\right]. \tag{3.5}$$

Now let $A\leq\mathbf{F}_r$ be an arbitrary subgroup. Recall Theorem 2.2 above (originally [PP15, Theorem 1.8]), by which the expected number of points in $\{1,\ldots,N\}$ fixed by all elements of $\varphi\left(A\right)$ in a uniformly random $\varphi\in\operatorname{Hom}\left(\mathbf{F}_r,S_N\right)$ is

$$N^{1-\operatorname{rank}(A)}+C\cdot N^{1-\pi(A)}+O\left(N^{-\pi(A)}\right), \tag{3.6}$$

where $C$ is the number of subgroups $J\leq\mathbf{F}_r$ of rank $\pi\left(A\right)$ and which contain $A$ but not as a free factor. Parallel to (3.2), which gives a formula for the expected number of fixed points of a single word, the expected number of common fixed points of $A$ can be computed by

$$\sum_{H\in[A,\infty)_{\overrightarrow{X}}}L^X_{H,\mathbf{F}_r}\left(N\right) \tag{3.7}$$

(recall that $[A,\infty)_{\overrightarrow{X}}=\left\{H\leq\mathbf{F}_r\,\middle|\,A\leq_{\overrightarrow{X}}X\right\}$, and see [Pud14, Section 5]). As in the case of single words, $\pi\left(A\right)$ is precisely the smallest rank of a proper algebraic extension of $A$. Theorem 2.2 and (3.6) can be interpreted as follows: in the formula (3.7) there is a leading term of $N^{1-\operatorname{rank}(A)}$ coming from $L^X_{A,\mathbf{F}_r}\left(N\right)$, but then all contributions coming from free extensions of $A$ in $[A,\infty)_{\overrightarrow{X}}$, together with $L^X_{A,\mathbf{F}_r}\left(N\right)-N^{1-\operatorname{rank}(A)}$, cancel out in all terms or order $N^{-\operatorname{rank}(A)},N^{-\operatorname{rank}(A)-1},\ldots,N^{1-\pi(A)}$. (The positive coefficient of $N^{1-\pi(A)}$ comes from algebraic extensions of $A$, not from free extensions.) Hence,

$$\sum_{H\leq\mathbf{F}_r\text{ s.t. }A\overset{*}{\leq}_{\overrightarrow{X}}H}L^X_{H,\mathbf{F}_r}\left(N\right)=N^{1-\operatorname{rank}(A)}+O\left(N^{-\pi(A)}\right). \tag{3.8}$$

We may assume that $\chi^{(2)}_m\left(w\right)<\chi_m\left(w\right)$, for otherwise Theorem 3.5 follows immediately from Theorem 1.11. Let $A_0\in\mathcal{AE}_m\left(w\right)$ be the unique algebraic extension with $w\in K_m\left(A_0\right)$ of rank $1-\chi_m\left(w\right)$, and let $A_1,\ldots,A_{C^{(2)}_m(w)}$ be those of rank $1-\chi^{(2)}_m\left(w\right)$. Because algebraic extensions is a transitive relation and $H\leq J\Longrightarrow K_m\left(H\right)\leq K_m\left(J\right)$, every proper algebraic extension of some $A\in\mathcal{AE}_m\left(w\right)$ is also in $\mathcal{AE}_m\left(w\right)$ and so its rank is at least $1-\chi^{(2)}_m\left(w\right)$. In particular, $\pi\left(A\right)\geq1-\chi^{(2)}_m\left(w\right)$ for every $A\in\mathcal{AE}_m\left(w\right)$. From (3.8) it now follows that

$$\sum_{H\leq\mathbf{F}_r\text{ s.t. }A\overset{*}{\leq}_{\overrightarrow{X}}H}L^X_{H,\mathbf{F}_r}\left(N\right)=\begin{cases}N^{\chi_m(w)}+O\left(N^{\chi^{(2)}_m(w)-1}\right) & \text{if }A=A_0\\ N^{\chi^{(2)}_m(w)}+O\left(N^{\chi^{(2)}_m(w)-1}\right) & \text{if }A=A_1,\ldots,A_{C^{(2)}_m(w)}\\ O\left(N^{\chi^{(2)}_m(w)-1}\right) & \text{if }A\in\mathcal{AE}_m\left(w\right)\setminus\left\{A_0,A_1,\ldots,A_{C^{(2)}_m(w)}\right\}\end{cases}.$$

Plugging these expressions in (3.5) is completes the proof of Theorem 3.5. □

A nice corollary of Theorem 1.11 is the following. Recall from Definition 1.6 that $\operatorname{cl}\left(w\right)$ denotes the commutator length of $w$ and $\operatorname{sql}\left(w\right)$ denotes the square length of $w$.

**Corollary 3.7.** *We have*

$$\chi_\infty\left(w\right)\geq1-2\cdot\operatorname{cl}\left(w\right)\qquad\text{and}\qquad\chi_2\left(w\right)\geq1-\operatorname{sql}\left(w\right).$$

*In particular,*

$$\mathcal{T}r_w\left(\mathcal{S}^1\wr S_N\right)=\Omega\left(N^{1-2\operatorname{cl}(w)}\right)\qquad\text{and}\qquad\mathcal{T}r_w\left(C_2\wr S_N\right)=\Omega\left(N^{1-\operatorname{sql}(w)}\right).$$

*Proof.* If $g = \mathrm{cl}(w)$ then there are $2g$ words $u_1, v_1, \ldots, u_g, v_g \in \mathbf{F}_r$ such that $w = [u_1, v_1] \cdots [u_g, v_g]$. Let $J = \langle u_1, v_1, \ldots, u_g, v_g \rangle$, and let $A$ be the corresponding algebraic extension of $\langle w \rangle$, so $\langle w \rangle \leq_{\mathrm{alg}} A \overset{*}{\leq} J$. Then $A \in \mathcal{AE}_\infty(w)$, and $rk(A) \leq \mathrm{rk}(J) \leq 2g$. Thus $\chi_\infty(w) \geq 1 - \mathrm{rk}(A) \geq 1 - 2g$.

Similarly, if $g = \mathrm{sql}(w)$ then there are $g$ words $u_1, \ldots, u_g \in \mathbf{F}_r$ such that $w = u_1^2 \cdots u_g^2$. Let $J = \langle u_1, \ldots, u_g \rangle$, and let $A$ be the corresponding algebraic extension of $\langle w \rangle$, so $\langle w \rangle \leq_{\mathrm{alg}} A \overset{*}{\leq} J$. Then $A \in \mathcal{AE}_2(w)$, and $rk(A) \leq \mathrm{rk}(J) \leq g$. Thus $\chi_2(w) \geq 1 - \mathrm{rk}(A) \geq 1 - g$. $\square$

# 4 Surface words and the proof of Theorem 1.4

## 4.1 Orientable surface words

First, we prove the first part of Theorem 1.4, which deals with the orientable surface word $[x_1, y_1] \cdots [x_g, y_g]$.

*Proof of Theorem 1.4, orientable case.* Assume that some word $w \in \mathbf{F}_r$ induces the same measure as $[x_1, y_1] \cdots [x_g, y_g]$ on every compact group $G$. In particular, the expected value of any irreducible character $\psi$ of $G$ under the $w$-measure in $(\psi(1))^{1-2g}$. In the case of the unitary groups $\mathcal{U}(N)$, the trace is an irreducible $N$-dimensional character and thus $\mathcal{T}r_w(\mathcal{U}(N)) = N^{1-2g}$. From Theorem 1.7 it now follows that $\mathrm{cl}(w) \leq g$.

On the other hand, the trace of $\mathcal{S}^1 \wr S_N$ is also $N$-dimensional irreducible, and so $\mathcal{T}r_w(\mathcal{S}^1 \wr S_N) = N^{1-2g}$. From Theorem 1.11 it follows that $\chi_\infty(w) = 1 - 2g$. If $w = [u_1, v_1] \cdots [u_{\mathrm{cl}(w)}, v_{\mathrm{cl}(w)}]$ then $w \in K_\infty(H)$ where $H = \langle u_1, v_1, \ldots, u_{\mathrm{cl}(w)}, v_{\mathrm{cl}(w)} \rangle$. Hence

$$1 - 2g = \chi_\infty(w) \geq 1 - \mathrm{rank}(H) \geq 1 - 2\mathrm{cl}(w) \tag{4.1}$$

and we obtain that $\mathrm{cl}(w) \geq g$.

Thus $\mathrm{cl}(w) = g$. Moreover, all the weak inequalities in (4.1) are equalities, and $\mathrm{rank}(H) = 2\mathrm{cl}(w) = 1 - \chi_\infty(w)$. This shows that $H$ has minimal rank among the subgroups with $w \in K_\infty(w)$, and so $H \in \mathcal{AE}_\infty(w)$. In addition, $H$ is a free factor of $\mathbf{F}_r$: otherwise, it has a non-trivial algebraic extension $H \lneqq_{\mathrm{alg}} A \overset{*}{\leq} \mathbf{F}_r$, and then $A \in \mathcal{AE}_\infty(w)$ and $|\mathcal{AE}_\infty(w)| \geq 2$, in contradiction to Corollary 3.6 which applies in this case.

As $\mathrm{rank}(H) = 2\mathrm{cl}(w)$, the words $u_1, v_1, \ldots, u_{\mathrm{cl}(w)}, v_{\mathrm{cl}(w)}$ are free and constitute a basis for $H$, and as $H \overset{*}{\leq} \mathbf{F}_r$, they are part of a basis for $\mathbf{F}_r$. Therefore $w \overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim} [x_1, y_1] \cdots [x_g, y_g]$. $\square$

*Remark* 4.1. We mentioned above that Conjecture 1.3 sometimes appears in the literature in a stronger version, where only finite groups are involved rather than all compact groups. In our proof of the conjecture for the case of orientable surface words, we used two compact infinite groups: $\mathcal{U}(N)$ and $\mathcal{S}^1 \wr S_N$. However, the latter can be easily replaced by finite groups: let $|w|$ denote the length of the word $w$. If $m > |w|$, then $w$ cannot traverse any edge of a core graph $m$ times, $2m$ times, or $-m$ times (when counted with signs). So in this case, if $w \in K_m(H)$ then also $w \in K_\infty(H)$, and $\mathcal{T}r_w(C_m \wr S_N) = \mathcal{T}r_w(\mathcal{S}^1 \wr S_N)$ for all $N$. So for every $w$, one may replace the group $\mathcal{S}^1 \wr S_N$ in the proof above with the group $C_m \wr S_N$ for any $m \geq |w|$. This means that the only infinite groups one actually needs for the proof are $\mathcal{U}(N)$. See also Question 1 in Section 5.

## 4.2 Non-orientable surface words

*Proof of Theorem 1.4, non-orientable case.* Assume that some word $w \in \mathbf{F}_r$ induces the same measure as $x_1^2 \cdots x_g^2$ on every compact group. In particular, the expected value of any irreducible character $\psi$ of $G$ under the $w$-measure in $\frac{(\mathcal{FS}_\psi)^g}{(\dim \psi)^{g-1}}$. In the case of the group $\mathcal{S}^1 \wr S_N$, the trace is an irreducible $N$-dimensional character with $\mathcal{FS} = 0$ and thus $\mathcal{T}r_w(\mathcal{S}^1 \wr S_N) = 0$. From Corollary 3.7 we deduce that $\mathrm{cl}(w) = \infty$, namely, $w \notin [\mathbf{F}_r, \mathbf{F}_r]$.

In the case of the orthogonal groups $\mathcal{O}(N)$, the trace is an irreducible $N$-dimensional real character with $\mathcal{FS} = 1$ and thus $\mathcal{T}r_w(\mathcal{O}(N)) = N^{1-g}$. As $\mathrm{cl}(w) = \infty$, Theorem 1.8 says in this case that $\mathcal{T}r_w(\mathcal{O}(N)) = O(N^{1-\mathrm{sql}(w)})$. It follows that $\mathrm{sql}(w) \leq g$.

On the other hand, the trace of $C_2 \wr S_N$ is also $N$-dimensional irreducible with $\mathcal{FS} = 1$, and so $\mathcal{T}r_w(C_2 \wr S_N) = N^{1-g}$. From Theorem 1.11 it follows that $\chi_2(w) = 1 - g$. If $w = u_1^2 \cdots u_{\mathrm{sql}(w)}^2$ then $w \in K_2(H)$ where $H = \langle u_1, \ldots, u_{\mathrm{sql}(w)} \rangle$. Hence

$$1 - g = \chi_2(w) \geq 1 - \mathrm{rank}(H) \geq 1 - \mathrm{sql}(w) \tag{4.2}$$

and we obtain that $\mathrm{sql}(w) \geq g$.

Thus $\mathrm{sql}(w) = g$. Moreover, all the weak inequalities in (4.2) are equalities, and $\mathrm{rank}(H) = \mathrm{sql}(w) = 1 - \chi_2(w)$. This shows that $H$ has minimal rank among the subgroups with $w \in K_2(w)$, and so $H \in \mathcal{AE}_2(w)$. In addition, $H$ is a free factor of $\mathbf{F}_r$: otherwise, it has a non-trivial algebraic extension $H \lneqq_{\mathrm{alg}} A \overset{*}{\leq} \mathbf{F}_r$, and then $A \in \mathcal{AE}_2(w)$ and $|\mathcal{AE}_2(w)| \geq 2$, in contradiction to Corollary 3.6 which applies in this case.

As $\mathrm{rank}(H) = \mathrm{sql}(w)$, the words $u_1, \ldots, u_{\mathrm{sql}(w)}$ are free and constitute a basis for $H$, and as $H \overset{*}{\leq} \mathbf{F}_r$, they are part of a basis for $\mathbf{F}_r$. Therefore $w \overset{\mathrm{Aut}(\mathbf{F}_r)}{\sim} x_1^2 \cdots x_g^2$. ☐

*Remark* 4.2. As in the orientable case, the small role of the infinite group $\mathcal{S}^1 \wr S_N$ in the last proof can be also played by the groups $C_m \wr S_N$ for large enough $m$.

# 5 Open Questions

We conclude with some open questions naturally arising from the results in this paper.

1. Can Theorem 1.4 be proven also based on word measures on finite groups only? Namely, can the role played in the proof by $\mathcal{U}(N)$ and $\mathcal{O}(N)$ be also played by some finite groups? (And see Remarks 4.1 and 4.2.)

2. Corollary 3.6 has the potential of yielding a solution of more special cases of Conjecture 1.3. Namely, if there is a relatively small set of $\mathrm{Aut}(\mathbf{F}_r)$-orbits, along surface words, with the property that $|\mathcal{AE}_m| = 1$ for some $m \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, then one can hope to prove Conjecture 1.3 for these orbits. Let us mention two examples: the words $[x,y]^2$ and $[x,y][x,z]$ both satisfy that $|\mathcal{AE}_\infty(w)| = 1$.

# Acknowledgments

We thank Henry Wilton and Liviu Păunescu for beneficial comments. D.P. was supported by ISF grant 1071/16.

# References

[AV11] Alon Amit and Uzi Vishne. Characters and solutions to equations in finite groups. *J. Algebra Appl.*, 10(4):675–686, 2011. 3

[Fro96] Georg Frobenius. Über gruppencharaktere. *Sitzungsberichte Akademie der Wissenschaften zu Berlin*, pages 985–1021, 1896. 2, 5

[FS06] Georg Frobenius and Issai Schur. Über die reellen darstellungen der endlichen gruppen. *Sitzungsberichte Akademie der Wissenschaften zu Berlin*, pages 186–208, 1906. 2, 6

[HMP19] Liam Hanani, Chen Meiri, and Doron Puder. Some orbits of free words that are determined by measures on finite groups. In preparation, 2019. 3

[Isa76] I. Martin Isaacs. *Character theory of finite groups*, volume 69. Academic Press, 1976. 6

[LP10] Nati Linial and Doron Puder. Word maps and spectra of random graph lifts. *Random Structures and Algorithms*, 37(1):100–135, 2010. 4

[MP16] Michael Magee and Doron Puder. Word measures on unitary groups. arXiv preprint 1509.07374v2 [math.GR], 2016. 2

[MP18] Michael Magee and Doron Puder. Unitary group integrals, surfaces, and mapping class groups. preprint arXiv:1802.04862v1, 2018. 3, 4

[MP19] Michael Magee and Doron Puder. Matrix integrals, surfaces, and mapping class groups II: Orthogonal and symplectic groups. In preparation, 2019. 3, 4

[MVW07] Alexei Miasnikov, Enric Ventura, and Pascal Weil. Algebraic extensions in free groups. In *Geometric group theory*, pages 225–253. Springer, 2007. 7

[Nic94] Alexandru Nica. On the number of cycles of given length of a free word in several random permutations. *Random Structures & Algorithms*, 5(5):703–730, 1994. 4, 6, 9

[PP15] Doron Puder and Ori Parzanchevski. Measure preserving words are primitive. *Journal of the American Mathematical Society*, 28(1):63–97, 2015. 3, 5, 6, 7, 9, 11, 12

[PS14] Ori Parzanchevski and Gili Schul. On the Fourier expansion of word maps. *Bulletin of the London Mathematical Society*, 46(1):91–102, 2014. 3, 6

[Pud14] Doron Puder. Primitive words, free factors and measure preservation. *Israel J. Math.*, 201(1):25–73, 2014. 6, 8, 9, 12

[PW19] Doron Puder and Danielle West. Word measures on $GL_n(F_q)$. In preparation, 2019. 4

[Sha13] Aner Shalev. Some results and problems in the theory of word maps. In L. Lovász, I. Ruzsa, V.T. Sós, and D. Palvolgyi, editors, *Erdös Centennial (Bolyai Society Mathematical Studies)*, pages 611–650. Springer, 2013. 3

[Sta83] John R. Stallings. Topology of finite graphs. *Inventiones Mathematicae*, 71(3):551–565, 1983. 7

[Sti12] John Stillwell. *Classical topology and combinatorial group theory*, volume 72 of *Graduate texts in mathematics*. Springer, 2012. 2



Michael Magee,
Department of Mathematical Sciences,
Durham University,
Lower Mountjoy, DH1 3LE Durham,United Kingdom
michael.r.magee@durham.ac.uk

Doron Puder,
School of Mathematical Sciences,
Tel Aviv University,
Tel Aviv, 6997801, Israel
doronpuder@gmail.com