Independent Words are Freely Separated

Yotam Shomroni[1] Noam Ta Shma[2]

July 2026

[1]Weizmann Institute of Science [2]Tel Aviv University

Independent words

Words and word measures

Let F be a finitely generated free group, $w \in \mathrm{F}$ a word, and G a finite group.

- Substitute independent, uniformly random elements of G for the letters of w. This produces a G-valued random element.
- Its distribution is the *word measure* of w on G.

Words and word measures

Let F be a finitely generated free group, $w \in \mathrm{F}$ a word, and G a finite group.

- Substitute independent, uniformly random elements of G for the letters of w. This produces a G-valued random element.
- Its distribution is the *word measure* of w on G.

Equivalently, the random element is $\alpha(w)$, where $\alpha \colon \mathrm{F} \to G$ is a uniformly random homomorphism,

$$\alpha \sim \mathrm{Unif}(\mathrm{Hom}(\mathrm{F}, G)).$$

Words and word measures

Let F be a finitely generated free group, $w \in \mathsf{F}$ a word, and G a finite group.

- Substitute independent, uniformly random elements of G for the letters of w. This produces a G-valued random element.
- Its distribution is the *word measure* of w on G.

Equivalently, the random element is $\alpha(w)$, where $\alpha \colon \mathsf{F} \to G$ is a uniformly random homomorphism,

$$\alpha \sim \mathrm{Unif}(\mathrm{Hom}(\mathsf{F}, G)).$$

Example. For $w = xyx^{-1}y^{-1}$, the random variable $\alpha(w)$ is $= [g, h]$ with g, h independent and uniform in G.

Previous work

Note that if $w = x$ has a single letter, then by definition, $\alpha(w)$ distributes uniformly over G, for every finite group G.

Previous work

Note that if $w = x$ has a single letter, then by definition, $\alpha(w)$ distributes uniformly over G, for every finite group G.

Puder and Parzanchevski showed a converse to this observation: if a word w induces a uniformly distributed random variable on every finite group G, then w is primitive (a part of a free basis).

When are two words independent?

Fix two words $w_1, w_2 \in \mathsf{F}$. A single $\alpha \sim \mathrm{Unif}(\mathrm{Hom}(\mathsf{F}, G))$ produces two G-valued random elements $\alpha(w_1), \alpha(w_2)$.

When are two words independent?

Fix two words $w_1, w_2 \in \mathsf{F}$. A single $\alpha \sim \mathrm{Unif}(\mathrm{Hom}(\mathsf{F}, G))$ produces two G-valued random elements $\alpha(w_1), \alpha(w_2)$.

If w_1 and w_2 use disjoint letters, they are functions of disjoint, independent inputs, So they are independent, for every finite group G.

When are two words independent?

Fix two words $w_1, w_2 \in \mathsf{F}$. A single $\alpha \sim \mathrm{Unif}(\mathrm{Hom}(\mathsf{F}, G))$ produces two G-valued random elements $\alpha(w_1), \alpha(w_2)$.

If w_1 and w_2 use disjoint letters, they are functions of disjoint, independent inputs, So they are independent, for every finite group G.

Question

Is the converse true? If $\alpha(w_1)$ and $\alpha(w_2)$ are independent for every finite group G, must w_1 and w_2 use disjoint letters?

The naive converse fails

The answer is no, at least not in the obvious sense.

- Take $w_1 = x^2$ and $w_2 = (xy)^3$ in $\mathrm{F} = \langle x, y \rangle$. They share the letter x.
- But $\{x,\, xy\}$ is also a basis of F, and in that basis w_1, w_2 use disjoint letters.
- Hence $\alpha(w_1)$ and $\alpha(w_2)$ are independent for every finite group G.

Why the basis does not matter

Invariance under Aut(F)

Let $\varphi \in \mathrm{Aut}(F)$. Precomposition $\beta \mapsto \beta \circ \varphi$ permutes the finite set $\mathrm{Hom}(F, G)$, so it preserves the uniform measure. Therefore

$$\alpha \circ \varphi \;\sim\; \mathrm{Unif}(\mathrm{Hom}(F, G)) \qquad \text{whenever} \qquad \alpha \sim \mathrm{Unif}(\mathrm{Hom}(F, G)).$$

Consequently $\big(\alpha(\varphi w_1), \alpha(\varphi w_2)\big)$ has the same joint distribution as $\big(\alpha(w_1), \alpha(w_2)\big)$. Independence depends on the pair (w_1, w_2) only up to a change of basis.

So the right condition is not "disjoint letters", but "disjoint letters in *some* basis".

Main theorem (special case)

Definition

Call w_1, w_2 *freely separated* if some basis of F writes them in disjoint letters; equivalently, $\mathsf{F} = J_1 * J_2$ with $w_1 \in J_1$ and $w_2 \in J_2$.

Main theorem (special case)

Definition

Call w_1, w_2 *freely separated* if some basis of F writes them in disjoint letters; equivalently, $\mathrm{F} = J_1 * J_2$ with $w_1 \in J_1$ and $w_2 \in J_2$.

Theorem

$\alpha(w_1)$ and $\alpha(w_2)$ are independent for every finite group G if and only if w_1, w_2 are freely separated.

One direction is the easy observation above.

A refined equivalence

For two events, dependence is measured by their (unnormalized) correlation:

$$\mathrm{Corr}(A, B) \stackrel{\text{def}}{=} \Pr(A \cap B) - \Pr(A)\Pr(B).$$

For $G = S_n$, let $A_i = \{\alpha(w_i) \in S_{n-1}\}$, the event that $\alpha(w_i)$ fixes n.

A refined equivalence

For two events, dependence is measured by their (unnormalized) correlation:

$$\mathrm{Corr}(A, B) \stackrel{\mathrm{def}}{=} \Pr(A \cap B) - \Pr(A)\Pr(B).$$

For $G = S_n$, let $A_i = \{\alpha(w_i) \in S_{n-1}\}$, the event that $\alpha(w_i)$ fixes n.

Theorem

The following are equivalent:

1. w_1, w_2 *are freely separated.*
2. $\alpha(w_1), \alpha(w_2)$ *are independent for every finite group* G.
3. $\mathrm{Corr}(A_1, A_2) = 0$ *for all* n.
4. $\mathrm{Corr}(A_1, A_2) \leq 0$ *for infinitely many* n.

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are immediate.

Positivity is only asymptotic

A_i is the event $\{\alpha(w_i) \in S_{n-1}\}$ for $i = 1, 2$ (i.e., $\alpha(w_i)$ fixes n).
$\mathrm{Corr}(A_1, A_2) = \Pr(A_1 \cap A_2) - \Pr(A_1)\Pr(A_2)$ is non-negative only for *large* n.

Example. $n \geq 3,\; w_1 = x^2,\; w_2 = x^3$.

$$\Pr(A_1) = \Pr(A_2) = \tfrac{2}{n}, \qquad \Pr(A_1 \cap A_2) = \tfrac{1}{n}.$$

$$\mathrm{Corr}(A_1, A_2) = \frac{1}{n} - \frac{4}{n^2} = \begin{cases} < 0 & n = 3, \\ 0 & n = 4, \\ > 0 & n \geq 5. \end{cases}$$

The phenomenon of positive correlation starts at $n \gg |w_1| + |w_2|$.

The quantitative theorem

Separation rank

Definition

$$\mathrm{sep}(w_1, w_2) \stackrel{\text{def}}{=} \min \left\{ \mathrm{rk}(J) \;\middle|\; \begin{array}{l} w_1, w_2 \in J \leq \mathrm{F}, \text{ and} \\ w_1, w_2 \text{ are } \textit{not} \text{ freely separated in } J \end{array} \right\},$$

with $\min \emptyset \stackrel{\text{def}}{=} \infty$. ($J \leq F$ is free by Nielsen–Schreier, so $\mathrm{rk}(J)$ makes sense).

Separation rank

Definition

$$\operatorname{sep}(w_1, w_2) \stackrel{\text{def}}{=} \min \left\{ \operatorname{rk}(J) \;\middle|\; \begin{array}{l} w_1, w_2 \in J \leq \mathrm{F}, \text{ and} \\ w_1, w_2 \text{ are } \textit{not} \text{ freely separated in } J \end{array} \right\},$$

with $\min \emptyset \stackrel{\text{def}}{=} \infty$. ($J \leq F$ is free by Nielsen–Schreier, so $\operatorname{rk}(J)$ makes sense).

- $\operatorname{sep}(w_1, w_2) = \infty$ if and only if w_1, w_2 are freely separated.
- On the other extreme, $\operatorname{sep}(w_1, w_2) = 1$ if and only if w_1, w_2 commute (equivalently, they have a common root).

The quantitative theorem (special case)

Theorem

As $n \to \infty$, *for* $\alpha \sim \mathrm{Unif}(\mathrm{Hom}(\mathsf{F}, S_n))$,

$$\mathrm{Corr}(A_1, A_2) = \Theta\big(n^{-\operatorname{sep}(w_1, w_2)}\big),$$

with a positive leading coefficient when w_1, w_2 *are not freely separated, and identically* 0 *when they are.*

In particular $\mathrm{Corr}(A_1, A_2) > 0$ for all large n, which gives (4) $\Rightarrow$ (1).

Computation example

Example

Take $w_1 = x^2$ and $w_2 = xyx^{-1}y^{-1}$. Then
$\Pr(\alpha(w_1) \in S_{n-1}) = \frac{2}{n}$, $\quad$, $\Pr(\alpha(w_2) \in S_{n-1}) = \frac{1}{n-1}$, and $\mathrm{Corr}(A_1, A_2) = \frac{n-3}{n^3-n^2}$.
Indeed, $\mathrm{sep}(w_1, w_2) = 2$.

Computation example

Example

Take $w_1 = x^2$ and $w_2 = xyx^{-1}y^{-1}$. Then
$\Pr(\alpha(w_1) \in S_{n-1}) = \frac{2}{n}, \quad , \Pr(\alpha(w_2) \in S_{n-1}) = \frac{1}{n-1}$, and $\mathrm{Corr}(A_1, A_2) = \frac{n-3}{n^3-n^2}$.
Indeed, $\mathrm{sep}(w_1, w_2) = 2$.

In general, these probabilities always concide with rational functions in n when n is large enough.

Computation example

Example

Take $w_1 = x^2$ and $w_2 = xyx^{-1}y^{-1}$. Then
$\Pr(\alpha(w_1) \in S_{n-1}) = \frac{2}{n}$, $\quad$, $\Pr(\alpha(w_2) \in S_{n-1}) = \frac{1}{n-1}$, and $\mathrm{Corr}(A_1, A_2) = \frac{n-3}{n^3-n^2}$.
Indeed, $\mathrm{sep}(w_1, w_2) = 2$.

In general, these probabilities always concide with rational functions in n when n is large enough.

Example

Take $w_1 = [x, y]$ and $w_2 = [x, z]$. Then
$\Pr(\alpha(w_i) \in S_{n-1}) = \frac{1}{n-1}$ $(i = 1, 2)$, and $\mathrm{Corr}(A_1, A_2) = \frac{2n-4}{n^4-2n^3+n^2}$.
Indeed, $\mathrm{sep}(w_1, w_2) = 3$.

Thank you.

Questions?

Ingredients of the proof

We use techniques developed by Puder–Parzanchevski and Hanany–Puder.

- Each probability $\Pr\left(\alpha(w_i) \in S_{n-1}\ \forall i\right)$ and $\prod_{i=1}^{2} \Pr\left(\alpha(w_i) \in S_{n-1}\right)$ can be written as a sum, over subgroups J containing w_1, w_2, of positive functions of n that are close to $n^{1-\mathrm{rk}(J)}$.
- The correlation is the difference of these sums. Each subgroup either contributes equally to both, and so cancels, or contributes a strictly positive difference; the latter case appears only at subgroups in which the words are not freely separated.
- The minimal-rank surviving subgroup dominates, giving the order $n^{-\,\mathrm{sep}}$ and the count $|\,\mathrm{Crit}_{\mathrm{sep}}\,|$.