PRIMITIVITY RANK FOR RANDOM ELEMENTS IN FREE GROUPS

ILYA KAPOVICH

ABSTRACT. For a free group F_r of finite rank $r \geq 2$ and a nontrivial element $w \in F_r$ the *primitivity rank* $\pi(w)$ is the smallest rank of a subgroup $H \leq F_r$ such that $w \in H$ and that w is not primitive in H (if no such H exists, one puts $\pi(w) = \infty$). The set of all subgroups of F_r of rank $\pi(w)$ containing w as a non-primitive element is denoted $Crit(w)$. These notions were introduced by Puder in [20]. We prove that there exists an exponentially generic subset $V \subseteq F_r$ such that for every $w \in V$ we have $\pi(w) = r$ and $Crit(w) = \{F_r\}$.

1. INTRODUCTION

Recall that an element g of a free group F is *primitive* in F if g belongs to some free basis of F. Let $r \geq 2$ be an integer and let $F_r = F(A)$, where $A = \{a_1, \ldots, a_r\}$ be the free group of rank r. In [20] Puder introduced the following natural measure of algebraic complexity for elements of F_r. For an element $1 \neq g \in F_r$ the *primitivity rank* $\pi(g)$ in F_r is defined as the smallest rank of a subgroup $H \leq F_r$ containing w as a non-primitive element; if no such H exists put $\pi(g) = \infty$. Puder observed that for $1 \neq g \in F_r$ one has $\pi(g) = \infty$ if and only if g is primitive in F_r. For any non-primitive nontrivial $g \in F_r$ one obviously has $\pi(w) \leq r$. For $1 \neq g \in F_r$ the *critical set of* g, denoted $Crit(g)$, is the set of all subgroups H of F_r containing g as a non-primitive element and such that $rank(H) = \pi(g)$. It is known that the set $Crit(g)$ is always finite (see [22]) and that given g one can algorithmically compute $\pi(g)$ and the set $Crit(g)$. Note that the primitivity rank is obviously automorphically invariant. For any $1 \neq g \in F_r$ and $\varphi \in \mathrm{Aut}(F_r)$ we have $\pi(g) = \pi(\varphi(g))$. Moreover, in this case $Crit(\varphi(g)) = \varphi(Crit(g)) = \{\varphi(H) | H \in Crit(g)\}$. Puder [20] and later Puder-Parzanchevski [22] and Hanany-Puder [8] showed that the primitivity rank and the critical set are closely related to understanding the behavior of the *word measures* on finite symmetric groups S_N corresponding to words in F_r. Here for a word $w = w(a_1, \ldots, a_r) \in F_r$ the corresponding word measure on S_N is the image under the map $w : (S_N)^r \to S_r$ of the uniform probability distribution on $(S_N)^r$. This connection is illustrated in Corollary 1.2 to our main result below.

However, the primitivity rank and the critical set for an element of F_r are natural algebraic notions that deserve to be studied in more detail in their own right. Indeed, Klimakov [14] extended the notion of primitivity rank to the context of free algebras of Schreier varieties and obtained some structural results there. Also, a recent series of papers of Louder and Wilton [15, 16] shows that for $w \in F_r$ there is a connection between the primitivity rank $\pi(w)$ and subgroup properties of the one-relator group $G_w = \langle a_1, \ldots, a_r | w = 1 \rangle$. In particular they prove that if $r \geq 3$ and $\pi(w) \geq 3$ then the group G_w is coherent, that is all of its finitely generated subgroups are finitely presented.

2020 *Mathematics Subject Classification.* Primary 20E05, Secondary 20F65, 20F69, 37D99, 60B15.

Key words and phrases. free group, genericity, primitive elements, random walks.

The author was supported by the individual NSF grant DMS-1905641.

In the present paper we study the primitivity rank and the critical set for "generic" or "random" freely reduced and cyclically reduced elements in F_r. The idea of "genericity" in the context of infinite groups arose in the 1990s in the work of Gromov [6], Ol'shanskii [19], Arzhantseva [1, 2, 3] and others. The notion of genericity for subsets of free groups that we use in this paper was formalized [12] when defining generic-case complexity of group-theoretic algorithms. If $Z \subseteq F_r$, a subset $S \subseteq Z$ is *exponentially generic* in Z if

$$\frac{\#\{w \in S : |w|_A \le n\}}{\#\{w \in Z : |w|_A \le n\}} \to_{n\to\infty} 1$$

with exponentially fast convergence. See Section 2.2 for more precise definitions and additional details. In this paper we are particularly interested in the cases $Z = F_r$ and $Z = U_r$, where U_r is the set of all cyclically reduced words in $F_r = F(A)$.

Our main result is:

Theorem 1.1. *Let $r \ge 2$ be an integer and let $F_r = F(A)$, where $A = \{a_1, \dots, a_r\}$, be the free group of rank r.*

1. *There exists a subset $Y_r \subseteq F_r$ such that Y_r is exponentially generic in F_r and that for every $w \in Y_r$ we have $\pi(w) = r$ and $Crit(w) = \{F_r\}$.*
2. *There exists a subset $Q_r \subseteq U_r$ such that Q_r is exponentially generic in U_r and that for every $w \in Q_r$ we have $\pi(w) = r$ and $Crit(w) = \{F_r\}$.*
3. *Let $W_n \in F(A)$ be obtained by a simple non-backtracking random walk of length n. Then, with probability tending to 1 exponentially fast as $n \to \infty$, the word W_n has the property that $\pi(W_n) = r$ and $Crit(W_n) = \{F_r\}$.*

Note that the generic sets Q_r and Y_r in the conclusion of Theorem 1.1 can in fact be chosen to be algorithmically recognizable because the conditions $P'(\lambda, \mu, r)$ and $(P'(\lambda, \mu, r))^\circ$ defining these sets in the proof of Theorem 1.1 are algorithmic if λ and μ are chosen to be rational numbers.

Puder [21, Corollary 8.3] also proved the existence of a generic subset of F_r such that for all elements of that subset w the primitivity rank is equal to r. His method of proof was very different from ours and it did not imply that $Crit(w) = \{F_r\}$ for generic elements.

As an application of Theorem 1.1, combined with the result of Puder and Parzanchevski, we obtain precise asymptotics for the number of fixed points $\#fix(\sigma)$ of a random permutation σ in S_N with respect to the "word measure" on the symmetric group S_N defined by a generic word $w \in F_r$:

Corollary 1.2. *Let $r \ge 2$ be an integer and let $F_r = F(A)$, where $A = \{a_1, \dots, a_r\}$. Let $Y_r \subseteq F_r, Q_r \subseteq U_r$ be the exponentially generic subsets provided by Theorem 1.1. Then for every $w \in Y_r$ and every $w \in Q_r$ we have*

$$\mathbb{E}_w[\#fix(\sigma)] \underset{N\to\infty}{=} 1 + \frac{1}{N^{r-1}} + O\left(\frac{1}{N^r}\right)$$

Here the expectation is taken with respect to the word measure *on the symmetric group S_N defined by the word $w(a_1, \dots, a_r)$, that is $\sigma = w(\sigma_1, \dots, \sigma_r)$, where $\sigma_1, \dots \sigma_r \in S_N$ are chosen uniformly independently at random in S_N.*

Proof. Puder and Parzanchevski proved [22, Theorem 1.8] that for every $1 \ne w \in F_r$ one has

$$\mathbb{E}_w[\#fix(\sigma)] \underset{N\to\infty}{=} 1 + \frac{|Crit(w)|}{N^{\pi(w)-1}} + O\left(\frac{1}{N^{\pi(w)}}\right).$$

The statement of the corollary now follows directly from Theorem 1.1. □

As noted above, the results of Louder and Wilton [15, 16] imply that if $r \geq 3$ and $w \in F_r$ has $\pi(w) \geq 3$ then the group $G_w = \langle a_1, \dots, a_r | w = 1 \rangle$ is coherent. Since generic elements $w \in F_r$ have $\pi(w) = r$, it follows that for $r \geq 3$ and a generic $w \in F_r$ the group G_w is coherent. This fact was first proved by Sapir and Spukalova [23], and also observed by Louder and Wilton [16], with a reference to Puder's result on the primitivity rank of generic elements [21].

Louder and Wilton conjectured [15] that if $1 \neq w \in F_r$ is not a proper power and has $\pi(w) > 2$ then the corresponding one-relator group G_w is word-hyperbolic (note that by [15, Theorem 1.4] all 2-generator subgroups in G_w are free and hence G_w has no Baumslag-Solitar subgroups). Cashen and Hoffmann [4] obtained some experimental evidence for this conjecture, verifying it for all w with $|w| \leq 17$ and $r \leq 4$. For $1 \neq w \in F_r$ which is not a proper power Louder and Wilton define *w-subgroups* of F_r as maximal with respect to inclusion elements of $Crit(w)$. They show in [15] that for w as above if $\pi(w) = 2$ then w has a unique w-subgroup. In [4] raise the question of whether the a w-subgroup is always unique. Note that if $\pi(w) = r$ then obviously F_r is the unique maximal element in $Crit(w)$, and thus, in particular, generic elements w of F_r have unique w-subgroups. Our Theorem 1.1 provides a maximally sharpened version of this statement for generic elements, since in that case we conclude that the entire set $Crit(w)$ consists of a single element, namely F_r itself.

As shown in [22], both $\pi(w)$ and the set $Crit(w)$ are algorithmically computable in terms of w. If $w \in F_r$ is a nontrivial cyclically reduced word (if we are given a word that is not cyclically reduced, we first cyclically reduce it), we write w on a circle of length w to get an A-graph C_w. Then we consider all possible "quotients" of C_w under surjective morphisms of folded A-graphs. That amounts to picking a partition of the vertex set of C_w, collapsing each element of that partition and then folding. For each resulting A-graph Γ we check, using Whitehead's algorithm, if the closed path γ_w labeled by w at the base-vertex $*$ of Γ is a primitive element of $\pi_1(\Gamma, *)$. We keep those Γ for which this path γ_w is not primitive in $\pi_1(\Gamma, *)$ and take the minimum of the ranks of all such $\pi_1(\Gamma, *)$. That minimum equals $\pi(w)$ and the A-graphs Γ that realize this minimum give us elements of $Crit(w)$. Note, however, that this algorithm sheds no light on the behavior of $\pi(w)$ and $Crit(w)$ for "random" cyclically reduced elements $w \in F_r$. Therefore we use rather different considerations in order to prove Theorem 1.1. The key tools there are provided by the "graph non-readability" conditions for generic elements of F_r obtained by Arzhantseva and Ol'shanskii in [1, 2], see Section 3 below. These genericity conditions also play a key role in the isomorphism rigidity results for "random" one-relator groups obtained in [11, 13].

The concept of the primitivity rank is dual to the notion of "primitivity index" for elements of free groups introduced by Gupta and Kapovich in [7]. For $1 \neq g \in F_r$ the *primitivity index* $d_{prim}(g, F_r)$ of g in F_r is the smallest index of a subgroup $H \leq F_r$ such that H contains g as a primitive element. It is shown in [7] that $d_{prim}(g, F_r)$ is always finite and moreover $d_{prim}(g, F_r) \leq ||g||_A$, where $||g||_A$ is the cyclically reduced length of g in $F(A)$. One of the main results of [7] shows that for a "random" freely reduced $w_n \in F(A)$ of length n the primitivity index $d_{prim}(w_n, F_r)$ is $\geq const \log^{1/3} n$. Thus we see that the primitivity index and primitivity rank of generic elements in F_r exhibit rather different quantitative behavior. However, a certain type of duality in these results is still preserved. They show that for a long "generic" $w \in F_r$ it is "hard" for w to be non-primitive in a subgroup of small rank containing w and it is "hard" for w to be primitive in a subgroup of small index in F_r containing w.

As part (3) of Theorem 1.1 shows, we can interpret genericity in the context of this theorem in terms of the element $W_n \in F_r = F(A)$ being produced by a simple non-backtracking random walk of length n on $F_r = F(A)$. It would be interesting to understand if the conclusion of Theorem 1.1 holds for other types of random walks on F_r. For example, let $\mu : F_r \to [0,1]$ be a discrete probability measure with finite support which generates F_r. Let $W_n = s_1 \dots s_n \in F_r$ be obtained by a random walk of length n on F_r defined by μ (where the increments $s_1, s_2, ..$ are chosen using an i.i.d. sequence of random variables, each with distribution μ). Is it then true that with probability tending to 1 as $n \to \infty$ we have $\pi(W_n) = r$ and $Crit(W_n) = \{F_r\}$? We suspect that the answer should be positive but proving this fact would require establishing a suitable version of Proposition 3.4 below for W_n. The original proof of Proposition 3.4 by Arzhantseva and Ol'shanskii deployed heavy duty counting arguments relying on certain entropy lowering considerations that were specific to the simple non-backtracking random walk context. Thus a new approach would be required for further generalizations.

We are grateful to Doron Puder for bringing to our attention his result from [21] that generic elements of F_r have primitivity rank r and for pointing out that the primitivity rank plays a key role in the work of Louder and Wilton [15, 16]. We also thank Henry Wilton for pointing us to the work of Cashen and Hoffmann [4].

2. Preliminaries

2.1. **A-graphs.** For the remainder of this paper, unless specified otherwise, let $r \geq 2$ be an integer, $A = \{a_1, \dots, a_r\}$ and let $F_r = F(A)$ be the free group of rank r with the free basis A.

We adopt the same language and convention regarding Stallings subgroup graphs for F_r and A-graphs more generally as in [10]. Thus an *A-graph* is a labelled directed graph Γ where every oriented edge e is given a label $\mu(e) \in A^{\pm 1}$ satisfying $\mu(e^{-1}) = (\mu(e))^{-1}$. An edge-path γ in Γ is then naturally assigned a label $\mu(\gamma)$ which is a word in the alphabet $A^{\pm 1}$. An A-graph Γ is *folded* if whenever e_1, e_2 are two distinct oriented edges of Γ with the same initial vertex $o(e_1) = o(e_2)$ then $\mu(e_1) \neq \mu(e_2)$. Thus every vertex in a folded A-graph has degree $\leq 2r$.

A connected A-graph Γ with a base-vertex $*$ is a *core graph* with respect to $*$ if Γ equals to the union of all non-backtracking closed edge-paths from $*$ to $*$. A connected A-graph Γ is a *core graph* if it is a core graph with respect to each of its vertices.

For a finite A-graph Γ we denote by $vol(\Gamma)$ the number of topological edges of Γ (where for every oriented edge e of Γ the unordered pair e, e^{-1} counts as a single topological edge).

Every subgroup $H \leq F_r$ is uniquely represented by its *Stallings subgroup graph* Γ_H, which is a connected folded A-graph with a base-vertex $*$ such that Γ_H is a core graph with respect to $*$ and that a freely reduced word $w \in F(A)$ belongs to H if and only if w labels a closed path from $*$ to $*$ in Γ_H. In this case the labeling map μ provides a natural isomorphism between $\pi_1(\Gamma_H, *)$ and H. A subgroup $H \leq F(A)$ is finitely generated if and only if Γ_H is finite. Moreover, H has finite index in $F(A)$ if and only if every vertex of Γ_H has degree $2r$, and in this case the index $[F(A) : H]$ is equal to the number of vertices in Γ_H.

For $H = F_r$ the corresponding Stallings subgroup graph is the *A-rose* R_A, which is a wedge of r-loop edges, labelled $a_1, \dots, a_r$, wedged at a single vertex x_0. For an arbitrary $H \leq F(A)$ one can obtain Γ_H by first taking the covering space $(\widehat{R}_A, *)$ of (R_A, x_0) corresponding to $H \leq \pi_1(R_A, x_0)$ and then taking the topological core of this covering that is the smallest connected subgraph of $\widehat{R}_A$ containing $*$ whose inclusion into $\widehat{R}_A$ is a homotopy equivalence.

We refer the reader to [24, 10, 11] for additional background on A-graphs and Stallings subgroup graphs.

For an element $g \in F_r$ we denote by $|g|_A$ the freely reduced length of g with respect to A and we denote by $||g||_A$ the cyclically reduced length of g with respect to A. For a word w over $A^{\pm 1}$ (not necessarily freely reduced) we denote by $|w|$ the length of w. Similarly, for an edge-path γ in an A-graph Γ, we denote by $|\gamma$ the length of γ.

Let Γ be a finite connected A-graph with a base-vertex $*$. The *maximal arcs* in Γ are closures of the connected components of the space obtained by removing from Γ all vertices of degree ≥ 3 and the vertex $*$. It's easy to check that if Γ is a finite connected A-graph with $\pi_1(\Gamma)$ of rank m then Γ has $\leq 3m$ maximal arcs.

2.2. **Genericity.** The definitions in this section follow [12, 11]. See [9] and [5, Ch. 1] for more general treatment of genericity.

For a sequence $(x_n)_{n \geq n_0}$ of real numbers and $x \in \mathbb{R}$ we say that $\lim_{n\to\infty} x_n = x$ *with exponentially fast convergence* if there exist constants $C > 0$ and $0 < \sigma < 1$ such that for all $n \geq n_0$ we have

$$|x_n - x| \leq C\sigma^n.$$

Let $S \subseteq F(A)$. For $n \geq 0$ we denote by $\rho_n(S)$ the number of elements $w \in F(A)$ with $|w|_A \leq n$ and we denote by $\gamma_n(S)$ the number of elements $w \in F(A)$ with $|w|_A = n$.

Definition 2.1 (Exponentially generic subsets)**.** Let $Z \subseteq F_r$ be a subset such that there is $n_0 \geq 1$ such that for all $n \geq n_0$ we have $\rho_n(S) \neq 0$.

(1) A subset $S \subseteq Z$ is *exponentially negligible* in Z if

$$\lim_{n\to\infty} \frac{\rho_n(S)}{\rho_n(Z)} = 0$$

and the convergence in this limit is exponentially fast.

(2) A subset $S \subseteq Z$ is *exponentially generic* in Z if $Z \setminus S$ is exponentially negligible in Z.

Recall that U_r denotes the set of all cyclically reduced words in $F_r = F(A)$.

Both n-balls and n-spheres in F_r and U_r grow like $(2r-1)^n$. This fact has the following useful consequences, see [13, Lemma 6.1].

Proposition 2.2. *The following hold:*

(a) Let $S \subseteq F_r$. Then S is exponentially negligible in F_r if and only if $\lim_{n\to\infty} \frac{\gamma_n(S)}{(2r-1)^n} = 0$ with exponentially fast convergence.

(b) Let $S \subseteq U_r$. Then S is exponentially negligible in U_r if and only if $\lim_{n\to\infty} \frac{\gamma_n(S)}{(2r-1)^n} = 0$ with exponentially fast convergence.

(c) Let $S \subseteq F_r$. Then S is exponentially generic in F_r if and only if $\lim_{n\to\infty} \frac{\gamma_n(S)}{\gamma_n(F_r)} = 1$ with exponentially fast convergence.

(d) Let $S \subseteq U_r$. Then S is exponentially generic in F_r if and only if $\lim_{n\to\infty} \frac{\gamma_n(S)}{\gamma_n(U_r)} = 1$ with exponentially fast convergence.

We also need the following statement, see [13, Proposition 6.2].

Proposition-Definition 2.3. *Let $Z \subseteq U_r$. Let Z° denote the set of all freely reduced words in F_r whose cyclically reduced forms belong to Z.*

(1) If Z is exponentially negligible in U_r then Z° is exponentially negligible in F_r.
(2) If Z is exponentially generic in U_r then Z° is exponentially generic in F_r.

3. The genericity condition

Recall that $r \geq 2$ is fixed, $A = \{a_1, \dots, a_r\}$ and $F_r = F(A)$. We will need the following genericity condition introduced by Arzhantseva and Ol'shanskii in [1].

Definition 3.1. [1] Let $0 < \mu \leq 1$ be a real number. A nontrivial freely reduced word w in $F(A) = F(a_1, \dots, a_r)$ is called *μ-readable* if there exists a connected folded A-graph Γ such that:

(1) The number of edges in Γ is at most $\mu|w|$.
(2) The free group $\pi_1(\Gamma)$ has rank at most $r-1$.
(3) There exists a reduced path in Γ with label w.

Definition 3.2. [2] Let $0 < \mu \leq 1$ be a real number and let $L \geq 2$ be an integer. A nontrivial freely reduced word w in $F(A)$ is called *(μ, L)-readable* if there exists a connected folded A-graph Γ such that:

(1) The number of edges in Γ is at most $\mu|w|$.
(2) The free group $\pi_1(\Gamma)$ has rank at most L.
(3) There is a path in Γ with label w.
(4) The graph Γ has at least one vertex of degree $< 2r$.

Definition 3.3. Let $0 < \mu \leq 1$ be a real number, let $L \geq 2$ be an integer and let $0 < \lambda < 1$ be a real number such that

$$\lambda \leq \frac{\mu}{15L + 3\mu} \leq \frac{\mu}{15r + 3\mu} < 1/6.$$

We will say that a cyclically reduced word w in $F(A)$ satisfies the *(λ, μ, L)-condition* if:

(1) The (symmetrized closure) of the word w satisfies the $C'(\lambda)$ small cancellation condition.
(2) The word w is not a proper power in $F(A)$.
(3) If w' is a subword of a cyclic permutation of w and $|w'| \geq |w_i|/2$ then w' is not μ-readable and not (μ, L)-readable.

We denote by $P(\lambda, \mu, L)$ the set of all cyclically reduced words $w \in F_r$ satisfying the (λ, μ, L)-condition.

We refer the reader to [17] for the basic definitions and background information regarding small cancellation theory.

Note that (3) in Definition 3.3 implies that if $w \in P(\lambda, \mu, L)$ then w is not μ-readable and not (μ, L)-readable.

The results of Arzhantseva and Ol'shanskii [1, 2] impliy the following result (c.f. [11, Theorem 4.6]).

Proposition 3.4. *Let $r \geq 2$ and $F_r = F(a_1, \dots, a_r)$. Let λ, μ, L be as in Definition 3.3.*

Then the set $P(\lambda, \mu, L)$ is exponentially generic in U_r.

Remark 3.5. Note that it is fairly easy to see that for any $\lambda \in (0, 1)$ the set all of non-proper power words satisfying $C'(\lambda)$ is exponentially generic in U_r. The main substance and power of Proposition 3.4 consists in verifying genericity of the non-readability conditions.

Note also that we don't actually need the full strength of the (λ, μ, L)-condition for the proofs in this paper. In particular, we don't use the "not a proper power" assumption on w. Also, in part (3) of Definition 3.3 we only really need non-readability of w itself rather than of its sufficiently long subwords. Nevertheless, we state the (λ, μ, L)-condition in its original stronger form, as it was defined by Arzhantseva and Ol'shanskii, for which they established Proposition 3.4.

We also need the following slightly more restricted version of the set $P(\lambda, \mu, L)$.

Definition 3.6. Let $r \geq 2$ and $F_r = F(a_1, \dots, a_r)$. Let λ, μ, L be as in Definition 3.3.

Denote by $P'(\lambda, \mu, L)$ the set of all words $w \in P(\lambda, \mu, L)$ such that every freely reduced word of length 2 in F_r occurs as a subword of w.

Proposition 3.7. *Let $r \geq 2$ and $F_r = F(a_1, \dots, a_r)$. Let λ, μ, L be as in Definition 3.3.*

Then the set $P'(\lambda, \mu, L)$ is exponentially generic in U_r.

Proof. For a given freely reduced word z of length 2, the set of all words in U_r containing z as a subword is exponentially generic in U_r; see, for example [13, Proposition 6.3]. Since the intersection of finitely many exponentially generic subsets of U_r is again exponentially generic in U_r, the conclusion of the proposition now follows from Proposition 3.4. □

4. Primitivity rank of generic elements

Theorem 4.1. *Let $r \geq 2$. Let $0 < \lambda, \mu < 1$ be such that*

$$\lambda \leq \frac{\mu}{15L + 3\mu} \leq \frac{\mu}{15r + 3\mu} < 1/6$$

and that

$$\lambda < \frac{\mu}{3r}.$$

Then for every nontrivial cyclically reduced word $w \in P'(\lambda, \mu, r)$ we have

$$\pi(w) = r \quad \text{and} \quad Crit(w) = \{F_r\}.$$

Proof. Let $1 \neq w \in P'(\lambda, \mu, r)$ where λ, μ are as in the assumptions of the theorem.

a) Note first that w is not primitive in F_r because w contains all freely reduced words in $F_r = F(A)$ of length 2 as subwords and hence the Whitehead graph of the cyclic word corresponding to w is complete [25]. Hence $\pi(w) \neq \infty$ and so $\pi(w) \leq r$.

b) We claim that $\pi(w) = r$. Indeed, suppose not. Thus $\pi(w) < r$. Take a subgroup $H \in Crit(w)$.

Thus $H \leq F_r$ is a subgroup of the smallest possible rank containing w as a non-primitive element and $rank(H) = \pi(w) < r$.

Let Γ_H be the Stallings subgroup graph for H and let $*$ be the base-vertex of Γ_H. Then the cyclically reduced word w is readable along a closed path γ_w from $*$ to $*$ in Γ_H. The minimality assumption on the rank of H implies that γ_w crosses every topological edge of Γ_H. Moreover, since Γ_H is folded and w is cyclically reduced, the vertex $*$ has degree > 1 in Γ_H, that is Γ_H is a folded connected finite core A-graph.

Put $m = rank(H) < r$.

The graph Γ_H has $\leq 3m$ maximal arcs (recall that we view $*$ as an endpoint of maximal arcs even if $*$ has degree 2 in Γ_H).

The case $vol(\Gamma_H) \le \mu|w|$ is impossible since w is readable in the graph Γ_H of rank $\le r-1$ and since by assumption w satisfies the (λ, μ, r)-condition.

Therefore $vol(\Gamma_H) \ge \mu|w|$. Let α be the longest maximal arc of Γ_H. Since Γ_H has $\le 3m$ maximal arcs, we have

$$|\alpha| \ge vol(\Gamma_H)/3m \ge \mu|w|/3m \ge \mu|w|/3r > \lambda|w|.$$

The path γ_w crosses over the arc α (in some direction) at least once, and the $C'(\lambda)$ assumption on w implies that it does so exactly once. Since γ_w is a closed path at $*$ in Γ_H, it follows that α is a non-separating arc in Γ_H and that γ_w represents a primitive element in $\pi_1(\Gamma_H, *)$. Hence w is primitive in H, yielding a contradiction with our assumption about w and H.

Thus indeed $\pi(w) = r$, as claimed.

c) We now claim that $Crit(w) = \{F_r\}$.

We have already seen in a) that w is not primitive in F_r and we have just proved that $\pi(w) = r$, so that $F_r \in Crit(w)$.

Suppose that $Crit(w) \ne \{F_r\}$. Then there exists a subgroup $H \in Crit(w)$, such that $H \ne F_r$. Thus H contains w as a non-primitive element and $rank(H) = r$. Since $H \ne F_r$, it follows that H has infinite index in F_r.

Again, let Γ_H be the Stallings subgroup graph for H with base-vertex $*$. Since $w \in H$, there is a closed path from $*$ to $*$ labelled by w. As in b), we see that Γ_H is a finite connected folded core A-graph. Also, the minimality assumption on the rank of H implies that γ_w crosses every edge of Γ_H. Since $[F_r : H] = \infty$, the graph Γ_H has a vertex of degree $< 2r$.

Since w is readable in Γ_H but w is not (μ, r)-readable by our assumption that $w \in P'(\lambda, \mu, r)$, it follows that the case $vol(\Gamma_H) \le \mu|w|$ is impossible. Hence $vol(\Gamma_H) \ge \mu|w|$.

Since $\pi_1(\Gamma_H)$ has rank r, the graph Γ_H has $\le 3r$ maximal arcs. Let α be the longest maximal arc of Γ_H. Then

$$|\alpha| \ge vol(\Gamma_H)/3r \ge \mu|w|/3r > \lambda|w|.$$

As in b), the path γ_w crosses the arc α at least once in some direction, and the $C'(\lambda)$ condition implies that it crosses α exactly once. Since γ_w is a closed path, it again follows that α is a non-separating arc in Γ_H and hence γ_w is primitive in $\pi_1(\Gamma_H, *)$. Therefore w is primitive in H, yielding a contradiction with the choice of H.

Thus $|Crit(w)| = 1$, as required. □

We can now prove Theorem 1.1 from the Introduction:

Theorem 4.2. *Let $r \ge 2$ be an integer and let $F_r = F(A)$, where $A = \{a_1, \dots, a_r\}$, be the free group of rank r.*

1. *There exists a subset $Y_r \subseteq F_r$ such that Y_r is exponentially generic in F_r and that for every $w \in Y_r$ we have $\pi(w) = r$ and $Crit(w) = \{F_r\}$.*
2. *There exists a subset $Q_r \subseteq U_r$ such that Q_r is exponentially generic in U_r and that for every $w \in Q_r$ we have $\pi(w) = r$ and $Crit(w) = \{F_r\}$.*
3. *Let $W_n \in F(A)$ be obtained by a simple non-backtracking random walk of length n. Then, with probability tending to 1 exponentially fast as $n \to \infty$, the word W_n has the property that $\pi(W_n) = r$ and $Crit(W_n) = \{F_r\}$.*

Proof. Choose λ, μ as in the assumptions of Theorem 4.1 and put $Q_r = P'(\lambda, \mu, r)$. Then Q_r is exponentially generic in U_r by Proposition 3.7. Then Q_r satisfies the requirements of part (2) by Theorem 4.1.

Now put $Y_r = Q_r^\circ$. Then Y_r is exponentially generic in F_r by Proposition-Definition 2.3. Every element w of Y_r is conjugate in F_r to some element w' of Q_r in F_r, that is $w = gw'g^{-1}$ for some $g \in F_r$. Then $\pi(w) = \pi(w')$ and $Crit(w) = gCrit(w')g^{-1} = \{gF_rg^{-1}\} = \{F_r\}$. Thus the requirements of (1) hold for Y_r.

Note that the simple non-backtracking random walk W_n of length n on $F(A)$ induces the uniform probability distribution on the n-sphere in $F(A)$. Therefore (3) directly follows from (1) in view of part 3 of Proposition 2.2.

□

References

[1] G. Arzhantseva and A. Olshanskii, *Genericity of the class of groups in which subgroups with a lesser number of generators are free,* (Russian) Mat. Zametki **59** (1996), no. 4, 489–496

[2] G. Arzhantseva, *On groups in which subgroups with a fixed number of generators are free,*(Russian) Fundam. Prikl. mat. **3** (1997), no. 3, 675–683

[3] G. Arzhantseva, *Generic properties of finitely presented groups and Howson's theorem,* Comm. Algebra **26** (1998), no. 11, 3783–3792

[4] C. H. Cashen and C. Hoffmann, *Short, highly imprimitive words yield hyperbolic one-relator groups*, preprint, 2020, arXiv:2006.15923

[5] F. Bassino, I. Kapovich, M. Lohrey, A. Miasnikov, C. Nicaud, A. Nikolaev, I. Rivin, V. Shpilrain, A. Ushakov, P. Weil, *Complexity and randomness in group theory – GAGTA book 1*, De Gruyter, Berlin, 2020, ISBN: 978-3-11-066702-8

[6] M. Gromov, *Asymptotic invariants of infinite groups*, in: Geometric Group Theory, Vol. 2, Sussex, 1991, Cambridge Univ. Press, Cambridge, 1993, pp. 1–295

[7] N. Gupta, and I. Kapovich, *The primitivity index function for a free group, and untangling closed curves on hyperbolic surfaces. With an appendix by Khalid Bou-Rabee*, Math. Proc. Cambridge Philos. Soc. **166** (2019), no. 1, 83–121

[8] L. Hanany and D. Puder, *Word Measures on Symmetric Groups,* preprint, September 2020, arXiv:2009.00897

[9] I. Kapovich, *Musings on generic-case complexity*, Elementary theory of groups and group rings, and related topics, 135–148, De Gruyter Proc. Math., De Gruyter, Berlin, 2020

[10] I. Kapovich and A. Myasnikov, *Stallings foldings and subgroups of free groups*, J. Algebra **248** (2002), no. 2, 608–668

[11] I. Kapovich and P. Schupp, *Genericity, the Arzhantseva-Ol'shanskii method and the isomorphism problem for one-relator groups,* Math. Ann. **331** (2005), no. 1, 1–19

[12] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, *Generic-case complexity, decision problems in group theory, and random walks.* J. Algebra **264** (2003), no. 2, 665–694

[13] I. Kapovich, P. Schupp, and V. Shpilrain, *Generic properties of Whitehead's algorithm and isomorphism rigidity of random one-relator groups.* Pacific J. Math. **223** (2006), no. 1, 113–140

[14] A. Klimakov, *Primitivity rank of elements of free algebras of Schreier varieties*, J. Algebra Appl. **15** (2016), no. 2, 1650036

[15] L. Louder and H. Wilton, *Negative immersions for one-relator groups*, Duke Mathematical Journal, to appear; arXiv:1803.02671

[16] L. Louder and H. Wilton, *Uniform negative immersions and the coherence of one-relator groups*, preprint, 2021, arXiv:2107.08911

[17] R. Lyndon and P. E. Schupp, *Combinatorial group theory.* Reprint of the 1977 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2001; ISBN: 3-540-41158-5

[18] J. Maher, and J. Tiozzo, *Random walks on weakly hyperbolic groups.* J. Reine Angew. Math. **742** (2018), 187–239

[19] A. Yu. Ol'shanskii, *Almost every group is hyperbolic*, Internat. J. Algebra Comput. **2** (1992), 1–17

[20] D. Puder, *Primitive words, free factors and measure preservation*. Israel J. Math. **201** (2014), no. 1, 25–73
[21] D. Puder, *Expansion of random graphs: new proofs, new results. Invent. Math. 201 (2015), no. 3, 845?908*
[22] D. Puder and O. Parzanchevski, *Measure preserving words are primitive.* J. Amer. Math. Soc. **28** (2015), no. 1, 63–97
[23] M. Sapir and I. Spakulová, *Almost all one-relator groups with at least three generators are residually finite*, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 2, 331–343
[24] J. R. Stallings, *Topology of finite graphs*, Invent. Math. **71** (1983), no. 3, 551–565
[25] J. H. C. Whitehead, *On equivalent sets of elements in a free group*, Ann. of Math. (2) **37** (1936), no. 4, 782–800

Department of Mathematics and Statistics, Hunter College of CUNY
695 Park Ave, New York, NY 10065
http://math.hunter.cuny.edu/ilyakapo/,

E-mail address: ik535@hunter.cuny.edu