SIEVE METHODS IN GROUP THEORY III: $\mathrm{Aut}(F_n)$

ALEXANDER LUBOTZKY AND CHEN MEIRI

Abstract. Let $\pi : \mathrm{Aut}(F_n) \to \mathrm{Aut}(\mathbb{Z}^n)$ be the epimorphism induced by the isomorphism $\mathbb{Z}^n \cong F_n/F_n'$ and define $\mathcal{T}_n := \ker \pi$. We prove that the subset of $\mathcal{T}_n$ consists of all non-iwip and all non-hyperbolic elements is exponentially small.

1. Introduction

Let Γ be a finitely generated group. A subset $\Sigma \subseteq \Gamma$ is called *admissible* if it is symmetric (i.e. $\Sigma = \Sigma^{-1}$) and the Cayley graph $\mathrm{Cay}(\Gamma, \Sigma)$ is not bi-partite. Fix an admissible generating subset Σ of Γ. If $Z \subseteq \Gamma$ then the asymptotic behavior of the probability $\mathrm{Prob}_\Sigma(w_k \in Z)$ that the k^{th}-step of a random walk on $\mathrm{Cay}(\Gamma, \Sigma)$ belongs to Z can be used to 'measure' the density of Z (the random walk begins at the identity). In fact,

$$\mathrm{Prob}_\Sigma(W_k \in Z) := \frac{|\{(s_1, \ldots, s_k) \in \Sigma^k \mid s_1 \cdots s_k \in Z\}|}{|\Sigma|^k}$$

We say that Z is *exponentially small with respect to* Σ if there exist constants $c, \alpha > 0$ such that $\mathrm{Prob}_\Sigma(w_k \in Z) \leq ce^{-\alpha k}$ for all $k \in \mathbb{N}$. The set Z is called *exponentially small* if it is exponentially small with respect to all admissible generating subsets.

One of the first applications of the large sieve method in group theory was a result of Rivin [Ri1] and Kowlaski [Ko]. They proved that the set of non-pseudo-Anosov elements in the Mapping Class Group, MCG for short, is exponentially small (see also [Ma]). Their proof uses the homomorphism form the MCG to the symplectic group which is induced by the action on the homology of the surface. Hence, the proof tells us nothing about the Torelli group which is the kernel of this homomorphism. Kowlaski asked [Ko, page 135] if the same result also holds for the Torelli subgroup. An affirmative answer to this question was given in [MS] and in [LuMe2]. The main idea in both proofs was to use the action of the Torelli group on the homologies of double covers of the surface in order to construct similar homomorphisms from the Torelli group to symplectic groups.

There is a lot of similarity between the MCG and the automorphism group $\mathrm{Aut}(F_n)$ of a non-abelian free group F_n of rank n. In particular, there are two possible natural analogue notions to pseudo-Anosov elements: iwip elements or hyperbolic elements (see Section 4 for definitions and [KM] for a discussion on the

Key words and phrases. Sieve; Property-τ; iwip; hyperbolic;.

analogies). Let $\pi : \mathrm{Aut}(F_n) \to \mathrm{Aut}(\mathbb{Z}^n)$ be the epimorphism induced by the isomorphism $\mathbb{Z}^n \cong F_n/F_n'$. The subgroup $\mathcal{T}_n := \ker \pi$ is an analog of the Torelli group and it is finitely generated for $n \geq 3$ by a result of Magnus, while for $n = 2$ it is just the group of inner automorphisms $\mathrm{Inn}(F_2)$.

The analogy between MCG (respectively the Torelli group) and $\mathrm{Aut}(F_n)$ (resp. $\mathcal{T}_n$) suggests that the subset of $\mathrm{Aut}(F_n)$ (resp. of $\mathcal{T}_n$) consisting of all non-iwip and all non-hyperbolic elements is exponentially small. Rivin and Kapovich proved that this in indeed the case for $\mathrm{Aut}(F_n)$ [Ri2]. In this note we show that the same result also holds for $\mathcal{T}_n$. The idea of the proof is similar to the one we used for the Torelli group case: we investigate the actions of $\mathcal{T}_n$ on the abelizations of finite index subgroups of F_n. For this we use a Theorem of Grunewald and the first author which analyzes these action [GL1]. In fact, the situation for the automorphism group case is somewhat less 'symmetric' then the Torelli group case (see footnote 3) and we have to consider also the action on subgroups of index three (and not just the action on subgroups of index two which are the analog of double covers). Thus, unlike the case of the MCG for which all the representations studied (in [LuMe2] or [MS]) were naturally defined over $\mathbb{Z}$, we have to consider here representations onto a subgroup H of $\mathrm{GL}_{n-1}(\mathbb{Z}[\xi])$ where ξ is a non-trivial cubic root of unity. This brings some new challenges. For example, along the way we have to prove (see Proposition 2.4 below) that the set

$$\{g \in H \mid \exists m \geq 1 \text{ such that the characteristic polynomial of } g^m \text{ belongs to } \mathbb{Z}[t]\}$$

is exponentially small. This is proved in Section 2. In Section 3, we describe the Grunewald-Lubotzky theorem in the form needed here, while in Section 4, we discuss iwip and hyperbolic elements and prove the main result of this paper- Theorem 4.5.

2. Characteristic polynomials

For a number field K and an element $g \in \mathrm{GL}_n(K)$ let $f_g := \det(t\,\mathrm{I}_d - g)$ denote the characteristic polynomial of g and let R_g denotes the set of roots of f_g. Let ξ be a non-trivial third root of unity.

Fix a subgroup Γ of $\mathrm{GL}_n(\mathbb{Z}[\xi])$ which is commensurable to $\mathrm{SL}_n(\mathbb{Z}[\xi])$. The goal of this section is to show that that set

$$\{g \in \Gamma \mid \exists m \geq 1 \text{ such that } \ f_{g^m} \in \mathbb{Z}[t]\}$$

is exponentially small.

Let us recall and set up the notations of the process of "restriction of scalars". We can view $\mathbb{Z}[\xi]$ as a free $\mathbb{Z}$-module of rank 2 with basis $1, \xi$. If $b \in \mathbb{Z}[\xi]$ then the map $x \mapsto bx$ is a $\mathbb{Z}$-homomorphism of $\mathbb{Z}[\xi]$. Thus, we have an embedding $\psi : \mathbb{Z}[\xi] \hookrightarrow \mathrm{M}_{2\times 2}(\mathbb{Z})$ (the embedding depends on the chosen basis of $\mathbb{Z}[\xi]$). The image of $\mathbb{Z}$ under this embedding is the set of scalar matrices. Moreover, an element $x \in \mathbb{Z}[\xi]$ belongs to $\mathbb{Z}$ if and only if the $(2,1)$-coordinate of $\psi(x)$ equals to zero. We can view $\mathrm{M}_{2n\times 2n}(\mathbb{Z})$ as the ring of matrices of size $n \times n$ with entries in $\mathrm{M}_{2\times 2}(\mathbb{Z})$.

Thus, ψ induces the restriction of scalars embedding $\varphi : \Gamma \hookrightarrow \mathrm{GL}_{2n}(\mathbb{Z})$.[1] Explicitly, if $g \in \Gamma$ then $\varphi(g)_{2(i-1)+k,2(j-1)+l} = \psi(g_{i,j})_{k.l}$ for every $1 \leq i,j \leq n$ and every $1 \leq k,l \leq 2$. In particular, the trace of an element $g \in \Gamma$ belongs to $\mathbb{Z}$ if and only if $\sum_{i=1}^{n} \varphi(g)_{2(i-1)+1,2(i-1)+2} = 0$. Let $\mathrm{G}(\mathbb{C})$ be the Zariski-closure of $\varphi(\Gamma)$ in $\mathrm{GL}_{2n}(\mathbb{C})$. The connected component $\mathrm{G}^\circ(\mathbb{C})$ of $\mathrm{G}(\mathbb{C})$ is isomorphic to $\mathrm{SL}_n(\mathbb{C}) \times \mathrm{SL}_n(\mathbb{C})$ and in particular it is semisimple.

Lemma 2.1. *The subset* $Z := \{g \in \Gamma \mid \mathrm{trace}(g) \in \mathbb{Z}\}$ *is exponentially small in* Γ.

Proof. The set $\varphi(Z)$ is contained in the subvariety

$$V(\mathbb{C}) := \{A \in \mathrm{G}(\mathbb{C}) \mid \sum_{i=1}^{n} A_{2(i-1)+1,2(i-1)+2} = 0\}$$

where $A_{i,j}$ is the (i,j)-coordinate of A. It is not hard to see that $V(\mathbb{C})$ does not contain any coset of $\mathrm{G}^\circ(\mathbb{C})$. Proposition 2.2 below completes the proof. □

Proposition 2.2 (see Proposition 5.3 of [LuMe1])**.** *Let* Γ *be a finitely generated subgroup of* $\mathrm{GL}_n(\mathbb{Q})$ *such that connected component* $\mathrm{G}^\circ(\mathbb{C})$ *of its Zariski-closure is semisimple. Assume that* $V(\mathbb{C})$ *is a variety defined over* $\mathbb{Z}$ *and that* $V(\mathbb{C})$ *does not contain any coset of* $\mathrm{G}^\circ(\mathbb{C})$*. Then,* $V(\mathbb{C}) \cap \Gamma$ *is exponentially small in* Γ.

Another consequence of Proposition 2.2 is:

Lemma 2.3. *The subset*

$$W := \{g \in \Gamma \mid \text{ There exists } m \geq 1 \text{ such that } f_{\varphi(g^m)} \text{ has multiply roots } \}$$

is exponentially small in Γ.

Proof. Let $g \in \Gamma$ and assume that the characteristic polynomial of some positive power of $\varphi(g)$ has multiply roots. Let $m \geq 1$ be the minimal positive integer for which $f_{\varphi(g)^m}$ has multiply roots. Then, there is a root x of $f_{\varphi(g)}$ and a primitive m-root of unity ζ such that ζx is also a root of $f_{\varphi(g)}$. Thus, ζ belong to the normal closure $K_{\varphi(g)}$ of $\mathbb{Q}(R_{\varphi(g)})$ (recall that $R_{\varphi(g)}$ is the set of roots of $f_{\varphi(g)}$). However, $[K_{\varphi(g)} : Q] \leq (2n)!$ and there are only finitely many roots of unity which belong to an algebraic extension of $\mathbb{Q}$ of bounded degree. So, m is bounded by some constant c_n which depends only on n. In particular, if the characteristic polynomial of some positive power of $\varphi(g)$ has multiply roots then $f_{\varphi(g)^{c_n!}}$ has multiply roots. A polynomial has multiply roots if and only if its discriminant is equal to zero. Define $W(\mathbb{C}) := \{A \in \mathrm{G}(\mathbb{C}) \mid \mathrm{disc}(f_{A^{c_n!}}) = 0\}$. It is not hard to verify that the variety $W(\mathbb{C})$ does not contain any cost of $\mathrm{G}^\circ(\mathbb{C})$. Proposition 2.2 completes the proof. □

We are ready to prove the main proposition of this section:

[1] There exists $h \in \mathrm{GL}_{2n}(Q(\xi))$ and an automorphism α of the algebraic closure of $\mathbb{Q}$ such that $\alpha(\xi) = \xi^{-1}$ and $h\varphi(g)h^{-1} = \mathrm{diag}(g, \alpha(g))$ for every $g \in \Gamma$ (where $\alpha(g)_{i,j} := \alpha(g_{i,j})$).

Proposition 2.4. *The set*

$$T := \{g \in \Gamma \mid \exists m \geq 1 \text{ such that } f_{g^m} \in \mathbb{Z}[t]\}$$

is exponentially small in Γ.

Proof. In light of Lemmas 2.1 and 2.3 it is enough to show that $T \subseteq Z \cup W$. For every $g \in \Gamma$ the following holds:

1. $R_g \subseteq R_{\varphi(g)}$.
2. If $\alpha \in \mathrm{Aut}(\tilde{Q})$ then $\alpha(R_g) \subseteq R_{\varphi(g)}$ ($\tilde{Q}$ is the algebraic closure of $\mathbb{Q}$).[2]
3. $f_g \in \mathbb{Z}[t]$ if an only if $\alpha(R_g) = R_g$ for every $\alpha \in \mathrm{Aut}(\tilde{Q})$.

Assume that $g \notin Z \cup W$. Then as $g \notin Z$, Condition 3 shows that $\alpha(R_g) \neq R_g$ for some $\alpha \in \mathrm{Aut}(\tilde{Q})$. In turn, conditions 1 and 2 together with the fact that $g \notin W$ imply that $\alpha(R_{g^m}) \neq R_{g^m}$ for every $m \geq 1$. The other direction of condition 3 then shows that $f_{g^m} \notin \mathbb{Z}[t]$ for every $m \geq 1$. □

3. Grunewald-Lubotzky Theorem

Fix $n \geq 3$ and a basis $x_1, \ldots, x_n$ of F_n. For $s \geq 2$, let K_s be the kernel of the homomorphism form F_n to $\mathbb{Z}/s\mathbb{Z}$ which sends x_n to 1 and $x_1, \ldots, x_{n-1}$ to 0. Denote $y_{k,i} := x_n^{-i} x_k x_n^i$ for $0 \leq i \leq s-1$ and $1 \leq k \leq n-1$. Then, the set

$$\{y_{k,i} \mid 0 \leq i \leq s-1 \ \wedge \ 1 \leq k \leq n-1\} \cup \{x_n^s\}$$

is a free basis of K_s.

There is a natural homomorphism $\alpha : K_s/K_s' \to F_n/F_n'$. Since F_n/K_s is abelian every $\varphi \in \mathcal{T}_n$ preserves K_s. Thus, φ also acts as an automorphism on K_s/K_s' and as the identity on F_n/F_n'. These actions commute with α, i.e., with a little abuse of notation we have $\varphi \circ \alpha = \alpha \circ \varphi$. In particular, φ preserves $\ker \alpha$. Denote

$$L_s := \langle y_{k,i} y_{k,i+1}^{-1} \mid 0 \leq i \leq s-2 \ \wedge \ 1 \leq k \leq n-1 \rangle.$$

Then, L_s is a free factor of K_s and $\ker \alpha = L_s K_s'/K_s'$.

The abelian group K_s/K_s' has a structure of a $\mathbb{Z}[\xi_s]$-module where ξ_s be a s^{th}-root of unity. For $k \in K_s$, $\xi_s(kK_s') = x_n^{-1} k x_n K_s'$. The subgroup $L_s K_s'/K_s'$ is in fact a free $\mathbb{Z}[\xi_s]$-submodule with a basis

$$D_s := \{d_k \mid 1 \leq k \leq n-1\}$$

where $d_k := y_{k,0} y_{k,1}^{-1} K_s'$.

Every $\varphi \in \mathcal{T}_n$ acts as an automorphism on $L_s K_s'/K_s'$ and preserves its structure as a $\mathbb{Z}[\xi_s]$-module. The group of $\mathbb{Z}[\xi_s]$-automorphisms of $L_s K_s'/K_s'$ is isomorphic to $\mathrm{GL}_{n-1}(\mathbb{Z}[\xi_s])$ where the isomorphism is depend on the basis chosen for $L_s K_s'/K_s'$.

Thus, there exists a homomorphism $\rho_s : \mathcal{T}_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[\xi_s])$ with respect to the above basis D_s.

Theorem 3.1 (Grunewald-Lubotzky [GL1])**.** *Fix $s \geq 2$ and let $\rho_s : \mathcal{T}_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[\xi_s])$ be the above homomorphism. Then $\rho(\mathcal{T}_n)$ is commensurable with $\mathrm{SL}_{n-1}(\mathbb{Z}[\xi_s])$.*

[2] In fact, if $\alpha \in \mathrm{Aut}(\tilde{Q})$ and $\alpha(\xi) \neq \xi$ then $R_g \cup \alpha(R_g) = R_{\varphi(g)}$ while if $\alpha(\xi) = \xi$ then $R_g = R_{\alpha(g)}$.

For $s = 2$ the above theorem in similar to Proposition 3 of [LuMe2]. However, we shall see in the next section that unlike in the Torelli group case where the analog of ρ_2 suffices, in the $\mathcal{T}_n$ case we also have to consider ρ_3.

4. Iwip and hyperbolic elements

We start by recalling the definitions of iwip and hyperbolic elements. A more detailed discussion about these elements and the analogy to pseudo-Anosov elements in the mapping class group can be found in [KM]. An element $g \in \mathrm{Aut}(F_n)$ is called *reducible* if there are non-trivial proper subgroups $H_1, \ldots, H_k < F_n$ such that $H_1 * \cdots * H_k$ is a free factor of F_n and $g(H_i)$ is conjugate to H_{i+1} for every $1 \leq i \leq k$ where the addition in the subscript is modulo k. An element $g \in \mathrm{Aut}(F_n)$ is called *irreducible with irreducible powers*, or *iwip* for short, if for every $m \geq 1$ the automorphism g^m is not reducible. Hence, if $g \in \mathrm{Aut}(F_n)$ is not iwip then there are $m \geq 1$ and a non-trivial proper free factor H such that $g^m(H)$ is conjugate to H. Rivin [Ri1] proved that the set of non-iwip elements of $\mathrm{Aut}(F_n)$ is exponentially small.

An element $g \in \mathrm{Aut}(F_n)$ is called *hyperbolic* if for every $m \in \mathbb{N}^+$, the element g^m does not fix any conjugacy class of a non-trivial element. Rivin and Kapovich [Ri2] proved that the set of non-hyperbolic elements of $\mathrm{Aut}(F_n)$ is exponentially small.

Note that both properties, iwip and hyperbolic, are invariant by multiplication by inner automorphisms, so can be thought (and usually are thought) as properties of elements of $\mathrm{Out}(F_n) = \mathrm{Aut}(F_n)/\mathrm{Inn}(F_n)$. As $\mathcal{T}_2 = \mathrm{Inn}(F_2)$, there is no interest in studying these properties in the case $n = 2$ and we therefore assume that $n \geq 3$.

The proofs of the above results use the homomorphism $\pi : \mathrm{Aut}(F_n) \to \mathrm{Aut}(\mathbb{Z}^n)$ so they give us no information on the subgroup $\mathcal{T}_n := \ker \pi$. However, these results for $\mathcal{T}_n$ can be obtained by looking at covers.

Proposition 4.1. *There are homomorphisms $\rho_1, \ldots, \rho_{2^n-1} : \mathcal{T}_n \to \mathrm{GL}_{n-1}(\mathbb{Z})$ and $\psi_1, \ldots, \psi_{3^n-1} : \mathcal{T}_n \to \mathrm{GL}_{n-1}(\mathbb{Z}[\xi])$ where ξ is a non-trivial third root of unity such that:*

1. *For every $1 \leq i \leq 2^n - 1$, $\rho_i(\mathcal{T}_n)$ is of finite index in $\mathrm{GL}_{n-1}(\mathbb{Z})$.*
2. *For every $1 \leq i \leq 3^n - 1$, $\psi_i(\mathcal{T}_n)$ is commensurable with $\mathrm{SL}_{n-1}(\mathbb{Z}[\xi])$.*
3. *If $\varphi \in \mathcal{T}_n$ is not iwip then there are $m \geq 1$, $1 \leq i \leq 2^n - 1$ and $1 \leq j \leq 3^n - 1$ such that the characteristic polynomial of $\rho_i(\varphi^m)$ is reducible or the characteristic polynomial of $\psi_j(\varphi^m)$ belongs to $\mathbb{Z}[t]$.*

Proof. We use the notation of the previous section. Assume that $\varphi \in \mathcal{T}_n$ is not iwip. Then there is a free basis $x_1, \ldots, x_n$ of F_n and two natural numbers $1 \leq l < n$ and $m \geq 1$ such that φ^m preserve the F_n-conjugacy class of $H := \langle x_1, \ldots, x_l \rangle$.[3] Recall that for $s \geq 2$ we defined K_s to be the kernel of the homomorphism form F_n to

[3]The fact that φ^m preserves $\langle x_1, \ldots, x_l \rangle$ does not imply that it also preserves $\langle x_{l+1}, \ldots, x_n \rangle$ so unlike the Torelli group case in [LuMe2] we cannot assume that $l < n - 1$. This is the reason why in the current paper we have to consider triple covers and not only double covers.

$\mathbb{Z}/s\mathbb{Z}$ which sends x_n to 1 and $x_1, \dots, x_{n-1}$ to 0. Thus, K_s is a subgroup of index s in F_n so the F_n-conjugacy class of H splits into at most s K_s-conjugacy classes. Hence, φ^{6m} preserves the K_2-conjugacy class and the K_3-conjugacy class of H.

From now on let $s = 2$ or 3 and recall that $y_{k,i} := x_n^{-i} x_k x_n^i$ and that ξ_s is a non-trivial s-root of unity. Since $\varphi \in \mathcal{T}_n$ and F_n/K_s is abelian, $\varphi(x_n)x_n^{-1} \in K_s$ and

$$\varphi(y_{k,1})K_s' = x_n^{-1}\varphi(y_{k,0})x_n K_s'.$$

Since φ^{6m} preserves the K_s-conjugacy class of H, for every $1 \le k \le l$ there exists a word w_k such that

$$\varphi^{6m}(y_{k,0})K_s' = w_k(y_{1,0}, \dots, y_{l,0})K_s'.$$

Thus,

$$\varphi^{6m}(y_{k,1})K_s' = w_k(y_{1,1}, \dots, y_{l,1})K_s'$$

and

$$\varphi^{6m}(y_{k,0}y_{k,1}^{-1})K_s' = w_k(y_{1,0}y_{1,1}^{-1}, \dots, y_{l,0}y_{l,1}^{-1})K_s'. \tag{1}$$

Recall that we defined $d_k := y_{k,0}y_{k,1}^{-1}K_s'$. We also showed that K_s/K_s' is a $\mathbb{Z}[\xi_s]$-module and that $d_0, \dots, d_{n-1}$ freely generates a free $\mathbb{Z}[\xi_s]$-submodule L_sK_s'/K_s' of K_s/K_s'. Equation 1 shows that φ^{6m} preserves the $\mathbb{Z}$-submodule generated by $d_1, \dots, d_l$. By the definition of ρ_s, the image $\rho_s(\varphi^{6m}) \in \mathrm{GL}_{n-1}(\mathbb{Z}[\xi_s])$ represents the action of φ^{6m} on L_sK_s'/K_s'. This implies that at least one of the following statements holds:

- $l < n-1$ and the characteristic polynomial of $\rho_2(\varphi^{6m})$ is reducible.
- $l = n-1$ and $\rho_3(\varphi^{6m})$ belongs to $\mathrm{GL}_{n-1}(\mathbb{Z})$. In particular, the characteristic polynomial of $\rho_3(\varphi^{6m})$ belongs to $\mathbb{Z}[t]$.[4]

There are only $s^n - 1$ normal subgroups of F_n of index s. The homomorphism ρ_s depends on the subgroup K_s and on the free basis $d_1, \dots, d_{n-1}$ of L_sK_s'/K_s'. However, the characteristic polynomial of $\rho_s(\varphi^{6m})$ does not depend on the choice of the basis so it is enough to take for each subgroup of index s just one homomorphism. □

In order to get a similar result for non-hyperbolic elements we will need the following theorem:

Theorem 4.2 (Bestvina-Handel [BH])**.** *If $\varphi \in \mathrm{Aut}(F_n)$ is iwip but not hyperbolic then there is $m \ge 1$ such that φ^m is induced by an automorphism of a compact surface M with one boundary component S.*

Proposition 4.3. *There are homomorphisms $\rho_1, \dots, \rho_{2^n-1} : \mathcal{T}_n \to \mathrm{GL}_{n-1}(\mathbb{Z})$ such that:*

1. *For every $1 \le i \le 2^n - 1$, $\rho_i(\mathcal{T}_n)$ is of finite index in $\mathrm{GL}_{n-1}(\mathbb{Z})$.*
2. *If $\varphi \in \mathcal{T}_n$ is iwip but not hyperbolic then there are $m \ge 1$ and $1 \le i \le 2^n - 1$ such that the characteristic polynomial of $\rho_i(\varphi^m)$ is reducible.*

[4]For every $\psi \in \mathcal{T}_n$, $\rho_2(\psi) \in \mathrm{GL}_{n-1}(\mathbb{Z})$ so we do not gain any new information on $\rho_2(\varphi^{6m})$ if $l = n-1$.

Proof. We use the notation of the previous section. Let $\varphi \in \mathcal{T}_n$ be iwip but not hyperbolic. Theorem 4.2 implies that for some $m \geq 1$, the automorphism φ^m is induced by an automorphism of a compact surface M with one boundary component S. Thus, φ^m sends the homotopic class of S to itself or to its inverse, so φ^{2m} sends the homotopic class of S to itself. We divide the proof into two cases.

First case: M is orientable. In that case n is even and there exists a free basis $x_1, \ldots, x_n$ of F_n such that $\varphi^{2m} \in \mathcal{T}_n$ preserves the F_n-conjugacy class of $[x_1, x_2] \cdots [x_{n-1}, x_n]$. Then, $\varphi^{4m} \in \mathcal{T}_n$ preserves K_2-conjugacy class of $[x_1, x_2] \cdots [x_{n-1}, x_n]$. In particular as $x_1, \ldots, x_{n-2} \in K_2$ and $d_{n-1} = [x_{n-1}, x_n]K_2'$, $\rho_2(\varphi^{4m})(d_{n-1}) = d_{n-1}$. Thus, the characteristic polynomial of $\rho_2(\varphi^{4m})$ is reducible.

Second case: M is not orientable. There exists a free basis $x_1, \ldots, x_n$ of F_n such that $\varphi^{2m} \in \mathcal{T}_n$ preserves the F_n-conjugacy class of of $x_1^2 \cdots x_n^2$. Then, $\varphi^{4m} \in \mathcal{T}_n$ preserves the K_2-conjugacy class of $x_1^2 \cdots x_n^2$. It also preserves the K_2-conjugacy class of $x_n^{-1}(x_1^2 \cdots x_n^2)x_n$. This implies that $\rho_2(\varphi^{4m})(d^2) = d^2$ where $d := d_1 \cdots d_{n-1}$, so the characteristic polynomial of $\rho_2(\varphi^{4m})$ is reducible.

As in the proof of Proposition 4.1 the irreducibility of $\rho_2(\varphi^{4m})$ depends only on the subgroup K_2 and not on the specific basis of F_n. Thus, the number of required homomorphisms follows from the fact that the are $2^n - 1$ subgroups of index 2. □

By using the large sieve method, Rivin proved:

Proposition 4.4 (Rivin, [Ri1])**.** *Fix $n \geq 2$ and let Γ be a subgroup of finite index in $\mathrm{GL}_n(\mathbb{Z})$. For every $g \in \Gamma$ let f_g be the characteristic polynomial of g. Then, the set*

$$\{g \in \Gamma \mid \exists m \geq 1 \text{ such that } f_{g^m} \text{is reducible}\}$$

is exponentially small.

We can now conclude:

Theorem 4.5. *Let $n \geq 3$ and denote $\mathcal{T}_n := \ker(\mathrm{Aut}(F_n) \to \mathrm{Aut}(\mathbb{Z}_n))$. Then the set Z consisting the elements of $\mathcal{T}_n$ which are either non-iwip or non-hyperbolic is exponentially small.*

Proof. This follows from Propositions 4.1 and 4.3, using Propositions 2.4 and 4.4. □

References

[BH] M. Bestvina and M. Handel, *Train tracks and automorphisms of free groups.* Ann. of Math. (2) 135 (1992), no. 1, 1-51.

[GL1] F. Grunewald and A. Lubotzky, *Linear representations of the automorphism group of a free group.* Geom. Funct. Anal. 18 (2009), no. 5, 1564-1608.

[KM] I. Kapovich and M. Lustig, *Ping-pong and outer space.* J. Topol. Anal. 2 (2010), no. 2, 173-201.

[Ko] E. Kowalski, *The Large Sieve and Its Applications*, Arithmetic geometry, random walks and discrete groups. Cambridge Tracts in Mathematics, 175. Cambridge University Press, Cambridge, 2008. xxii+293 pp.

[Ma] J. Maher, *Random walks on the mapping class group*, arXiv:math/0604433.

[MS] J. Malestein and J. Souto, *On genericity of pseudo-Anosovs in the Torelli group.* arXiv:1102.0601.

[LuMe1] A. Lubotzky and C. Meiri, *Sieve methods in group theory I: Powers in Linear groups.* preprint.

[LuMe2] A. Lubotzky, C. Meiri, *Sieve methods in group theory II: The Mapping Class Group.* arXiv:1104.2450.

[Ri1] I. Rivin, *Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms*, Duke Math. J. 142 (2008), no. 2, 353–379.

[Ri2] I. Rivin, *Zariski density and genericity.* Int. Math. Res. Not. IMRN 2010, no. 19, 3649–3657.

Einstein Institute of Mathematics, Hebrew University, Jerusalem 90914, Israel
E-mail address: alexlub@math.huji.ac.il, chen.meiri@mail.huji.ac.il