SIEVE METHODS IN GROUP THEORY II: THE MAPPING CLASS GROUP

ALEXANDER LUBOTZKY AND CHEN MEIRI

Abstract. We prove that the set of non-pseudo-Anosov elements in the Torelli group is exponentially small. This answers a question of Kowalski [Ko].

1. Introduction

Let S be an orientable closed surface of genus $g \geq 1$ and denote its mapping class group by $\mathrm{MCG}(S)$. Thurston divided the elements of the $\mathrm{MCG}(S)$ into three types: pseudo-Anosov (PA for short), reducible and periodic (see Theorem 4 below). He conjectured that 'most' of the elements of $\mathrm{MCG}(S)$ are PA. This was proved by Maher [Ma]. A stronger result was shown by Rivin [Ri1] (and reproved by Kowalski [Ko] in a more conceptual form). They proved that the set of non-PA elements is exponentially small. Let us define this notion:

Let Γ be a finitely generated group and fix a symmetric generating set Σ of Γ which satisfies an odd relation. Random walks on the Cayley graph $\mathrm{Cay}(\Gamma, \Sigma)$ can be used to 'measure' subsets $Z \subseteq \Gamma$ by estimating the probability, $\mathrm{prob}_{\Sigma,k}(Z)$, that the k^{th}-step of a random walk belongs to Z for larger and larger values of k's. We say that Z is *exponentially small with respect to* Σ if there exist constants $c, \alpha > 0$ such that $\mathrm{prob}_{\Sigma,k}(Z) \leq ce^{-\alpha k}$ for all $k \in \mathbb{N}$. The set Z is called *exponentially small* if it is exponentially small with respect to all symmetric generating sets Σ which satisfies an odd relation (so the Cayley graph is not bi-partite graph).

Rivin's result states:

Theorem 1. ([Ri1], *see also* [Ko]). *The set of non-PA elements of* $\mathrm{MCG}(S)$ *is exponentially small.*

The proof of this result uses the epimorphism $\pi : \mathrm{MCG}(S) \to \mathrm{Sp}(2g, \mathbb{Z})$ (which is induced by the action of $\mathrm{MCG}(S)$ on the homology of S). It is shown in [BC] that if $\gamma \in \mathrm{MCG}(S)$ is not PA then the characteristic polynomial $f(x)$ of $\pi(\gamma)$ satisfies one of the following possibilities:

a. $f(x)$ is reducible in $\mathbb{Q}[x]$.
b. $f(x)$ has a root which is a root of unity.

Key words and phrases. sieve methods; Pseudo-Anosov elements.

c. There is $d \geq 2$ and polynomial $g(x)$ such that $f(x) = g(x^d)$

Thus, it is enough to show that the set of elements of $\mathrm{Sp}(2g, \mathbb{Z})$ which satisfy at least one of the above three conditions is exponentially small. This is not a hard task for conditions (b) and (c) so we only focus on condition (a). The proof that the set of elements which satisfy condition (a) is exponentially small uses the 'large sieve method' (implicitly in [Ri1] and explicitly in [Ko]). For our purpose, this method can be summarized in the following theorem which follows from Theorem B of [LM]

Theorem 2. *Let Γ be a finitely generated group and let $\mathcal{P}$ be a set of all but finitely many primes . Let $(N_p)_{p\in\mathcal{P}}$ be a series of finite index normal subgroups of Γ. Assume that there is a constant $d \in \mathbb{N}^+$ such that:*

1. *Γ has property-τ with respect to the series of normal subgroup $(N_p \cap N_q)_{p,q\in\mathcal{P}}$.*
2. *$|\Gamma_p| \leq p^d$ for every $p \in \mathcal{P}$ where $\Gamma_p := \Gamma/N_p$.*
3. *The natural map $\Gamma_{p,q} \to \Gamma_p \times \Gamma_q$ is an isomorphism for every distinct $p, q \in \mathcal{P}$ where $\Gamma_{p,q} := \Gamma/(N_p \cap N_q)$.*

Then a subset $Z \subseteq \Gamma$ is exponentially small if there is $c > 0$ such that:

4. *$\frac{|Z_p|}{|\Gamma_p|} \leq 1 - c$ for every $p \in \mathcal{P}$ where $Z_p := ZN_p/N_p$.*

Theorem 2 can be used to show that the set $Z \subseteq \mathrm{Sp}(2g, \mathbb{Z})$ consists of matrices with reducible characteristic polynomials is exponentially small. Indeed, the symplectic group $\mathrm{Sp}(2g, \mathbb{Z})$ has property-τ with respect to the family $\{N_q \mid q \text{ is a square free positive integer}\}$ where N_q is the kernel of the modulo-q homomorphism $\mathrm{Sp}(2g, \mathbb{Z}) \to \mathrm{PSp}(2g, \mathbb{Z}/qZ))$ (in fact, the group $\mathrm{Sp}(2g, \mathbb{Z})$ even has property (T) for $g \geq 2$). Condition 2 holds for $d = 4g^2$ and condition 3 is well known. Condition 4 is due to Chavdarov [Ch] who proved that there is a constant $c \in (0, 1)$ such that for every prime p the proportion of the elements in $\mathrm{Sp}(2g, \mathbb{Z}/p\mathbb{Z})$ with reducible characteristic polynomial is at most c.

The proof sketched above gives no information on the Torelli subgroup $\mathcal{T}(S) := \ker \pi$. The group $\mathcal{T}(S)$ is trivial for $g = 1$ and infinitely generated for $g = 2$. On the other hand, $\mathcal{T}(S)$ is finitely generated group for $g \geq 3$ so from now on we assume $g \geq 3$. In the early days it was not even known if $\mathcal{T}(S)$ contains PA elements. However, it does and Maher result even showed that 'most' of the elements in a ball of radius n are PA. Kowalski [Ko, page 135] asked if the stronger result is valid also for $\mathcal{T}(S)$. In this paper we prove that this is indeed the case:

Theorem 3. *The set of non-PA elements of $\mathcal{T}(S)$ is exponentially small.*

Our proof also uses the sieve method but instead of π we look at the actions of $\mathcal{T}(S)$ on the homologies of the $2^{2g}-1$ 2-sheeted covers of S (called prym representations in [Lo], see also [GL1] and [GL2]). These covers give

$2^{2g}-1$ different homomorphisms $\pi_1, \ldots, \pi_{2^{2g}-1}$ of $\mathcal{T}(S)$ into $\mathrm{Sp}(2g-2,\mathbb{Z})$. We show that if $\gamma \in \mathcal{T}(S)$ is not PA then there is $1 \le i \le 2^{2g}-1$ such that the characteristic polynomial of $\pi_i(\gamma)$ is reducible. We also show (following [Lo] and [GL2]) that $\pi_i(\mathcal{T}(S))$ is a finite index subgroup of $\mathrm{Sp}(2g-2,\mathbb{Z})$ and hence also has property-τ with respect to congruence subgroups. We can therefore use the sieve method in a similar manner to the use for the mapping class group case.

After this work was announced in [Lu2] and a draft was written we learnt that Justin Malestein and Juan Souto also proved Theorem 6 [MS]. The main idea is similar in both proofs, but some details are done differently.

2. The Torelli group.

2.1. **The mapping class group and the Torelli subgroup.** Let S be an orientable connected compact surface of genus $g \ge 2$, S is homeomorphic to a connected sum of g tori. For $1 \le k \le g-1$, let c_k be the curve separating the left k tori for the right $g-k$ ones, as shown in Figure 1. The first homology group $\mathrm{H}_1(S,\mathbb{Z})$ is isomorphic to $\mathbb{Z}^{2g}$. If c is a closed curve of S then $\bar{c}$ denotes the homology class of it. The elements $\bar{a}_1, \bar{b}_1, \ldots, \bar{a}_g, \bar{b}_g$ form a basis of $\mathrm{H}_1(S,\mathbb{Z})$ where $a_1, b_1, \ldots, a_g, b_g$ are the curves shown in Figure 1.

If d_1, d_2 are simple closed curves on S with finite intersection then their *intersection number* $i(d_1,d_2)$ is the sum of the indices of the intersection points of d_1 and d_2, where an intersection point is of index $+1$ when the orientation of the intersection agrees with the orientation of S, and -1 otherwise. The intersection number induces a symplectic form $(\cdot,\cdot)_S$ on $\mathrm{H}_1(S,\mathbb{Z})$ in the following way: Given two homology classes we choose representatives d_1, d_2 with finite intersection and define $(\bar{d}_1, \bar{d}_2)_S := i(d_1,d_2)$. In particular, $(\bar{a}_i, \bar{b}_i)_S = \delta_{ij}$, $(\bar{a}_i, \bar{a}_j)_S = 0$ and $(\bar{b}_i, \bar{b}_j)_S = 0$ for all the integers $1 \le i, j \le g$, i.e. $\bar{a}_1, \bar{b}_1, \ldots, \bar{a}_g, \bar{b}_g$ is a sympletic basis.

The *mapping class group* $\mathrm{MCG}(S)$ of S is the group of isotopy classes of orientation-preserving homeomorphisms of S. We will denote an isotopy classes with representative ψ by $[\psi]$. The group $\mathrm{MCG}(S)$ acts on $\mathrm{H}_1(S,\mathbb{Z})$ and preserves its symplectic form. Hence, this action induces a homomorphism

$$\gamma : \mathrm{MCG}(S) \to \mathrm{Sp}(\mathrm{H}_1(S,\mathbb{Z})).$$

$\mathcal{T}(S) := \ker(\gamma)$ is called the *Torelli group* of S.

While the action of $\mathrm{MCG}(S)$ on $\mathrm{H}_1(S,\mathbb{Z})$ can be used to investigate its elements, it does not tell us much about the Torelli group elements. To overcome this problem we will investigate the action of the Torelli group on the homology of the double covers of S.

2.2. **Pseudo-Anosov elements.** We start this section with the Nielsen-Thurston classification of the elements of the mapping class group . An element $\Psi \in \Gamma_g$ is called *pseudo-Anosov* (PA for short) if there is a pair of

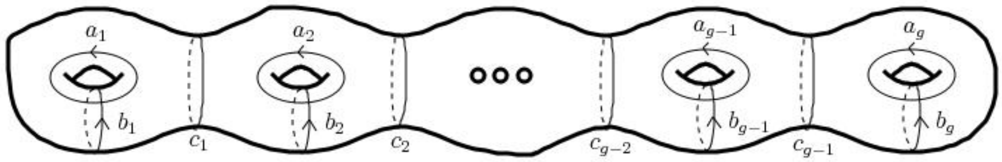

FIGURE 1. A surface of genus g.

transverse measured foliations (F^u, μ_u) and (F^s, μ_s) on S, a number $\lambda > 1$, and a $\psi \in \Psi$ so that $\psi \cdot (F^u, \mu_u) = (F^u, \lambda\mu_u)$ and $\psi \cdot (F^s, \mu_s) = (F^s, \lambda^{-1}\mu_s)$ (see [FM]). For our purpose, we do not need the details of this definition and we can use the following theorem:

Theorem 4 (see [FM], Theorem 12.1)**.** *An element $\Psi \in \mathrm{MCG}(S)$ is pseudo-Anosov if none of the following two possibilities holds:*

1. $\Psi^n = [\mathrm{id}]$ *for some* $n \in \mathbb{N}^+$.
2. *There is a finite non empty disjoint collection of non homotopic non trivial circles C_i in S and a $\psi \in \Psi$ such that $\psi(\mathcal{C}) = \mathcal{C}$, where $\mathcal{C}$ is the union of the circles C_i (C_i is non trivial if is not contractible to a point).*

We call Ψ periodic in case (1) *and reducible in case* (2)*.*

It is known that the Torelli group is torsion free. Hence, in order to show that an elements $\Psi \in \mathcal{T}(S)$ is pseudo-Anosov we will have to show that it is not reducible. In fact, we will use a result of Ivanov ([Iv1], Corollary 1.8) which implies:

Proposition 1. *Let $\Psi \in \mathcal{T}(S)$. If Ψ is not pseudo-Anosov then there is a non-trivial circle C and $\psi \in \Psi$ such that $\Psi(C) = C$.*

A circle C on S is *non-separating* if $S \setminus C$ is connected. If C and C' are non separating circles then there is a homeomorphism which sends C to C'. Hence, if C is a non-separating circle then there is a homeomorphism which sends C to a_1.

A circle C of S is *separating* if $S \setminus C$ is not connected. If C is a non trivial separating circle then it follows from the classification theorem of compact surfaces that there is $1 \leq k \leq g-2$ and a homeomorphism which sends C to the curve c_k shown in Figure 1 (in fact, by symmetry we can assume that $k \leq \frac{g-1}{2}$).

Summing all this we get the following:

Lemma 1. *Let $\Psi \in \mathcal{T}(S)$. If Ψ is not psuedo-Anosov then there is $\psi \in \Psi$ and an orientation preserving homeomorphism ν of S such that one of the following holds:*

1. $\psi(\nu(a_1)) = \nu(a_1)$ *or* $\psi(\nu(a_1)) = \nu(a_1)^{-1}$.
2. $\psi(\nu(c_k)) = \nu(c_k)$ *or* $\psi(\nu(c_k)) = \nu(c_k)^{-1}$ *for some* $1 \le k \le g-2$.

2.3. **The action of a psuedo-Anosov element on the homology of a double cover.** Let M be the bordered surface obtained from S after cutting along the curve b_g (Figure 2). So, S is a quotient space of M under the identification of $\dot{b}_g$ and $\hat{b}_g$. We take two copies $M^\diamond$,M^* of M and glue them together by identifying $\dot{b}_g^*$ with $\hat{b}_g^\diamond$ and $\hat{b}_g^*$ with $\dot{b}_g^\diamond$ (Figure 3). The resulting surfaces $\tilde{S}$ together with the natural map $\varphi : \tilde{S} \to S$ is a double cover of S of genus $2g-1$.

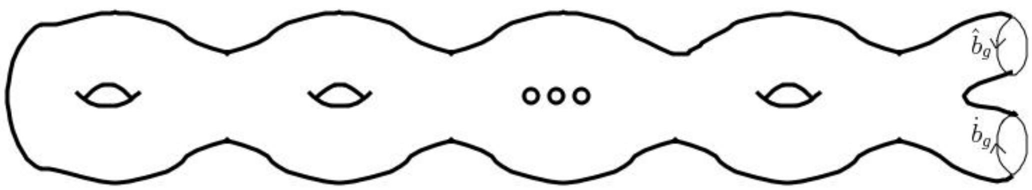

FIGURE 2. The surface after cutting along b_g.

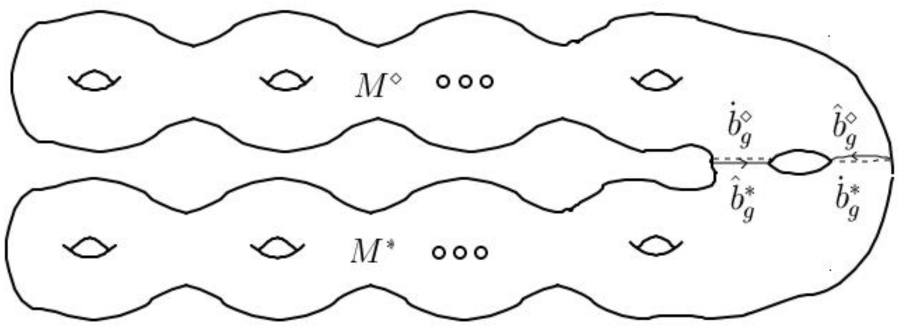

FIGURE 3. The double cover.

Let $\mathcal{H}$ be the kernel of the homomorphism $\mathrm{H}_1(\tilde{S},\mathbb{Z}) \to \mathrm{H}_1(S,\mathbb{Z})$ induced by φ. The group $\mathcal{H}$ is isomorphic to $\mathbb{Z}^{2g-2}$ with $z_1, z_{-1}, \ldots, z_{g-1}, z_{1-g}$ as a free basis where $z_i := \bar{a}_i^* - \bar{a}_i^\diamond$ and $z_{-i} := \bar{b}_i^* - \bar{b}_i^\diamond$ for $1 \le i \le g-1$.

The symplectic form $(\cdot,\cdot)_{\tilde{S}}$ of $\mathrm{H}_1(\tilde{S},\mathbb{Z})$ induces a related symplectic form $(\cdot,\cdot)_{\mathcal{H}} := \frac{1}{2}(\cdot,\cdot)_{\tilde{S}}$ on $\mathcal{H}$. The form $(\cdot,\cdot)_{\mathcal{H}}$ satisfies:

$$(z_i, z_j)_{\mathcal{H}} := \begin{cases} 1 & \text{if} \quad i = -j \text{ and } 0 < i \\ -1 & \text{if} \quad i = -j \text{ and } i < 0 \\ 0 & \text{otherwise} \end{cases}$$

Note that the identity map on S has two lifts to $\tilde{S}$. One is the identity and the other one is ξ which for every $q \in S$ substitutes the two lifts of q.

Choose a point $p \in S$ and a lift $\tilde{p}$ of it to $\tilde{S}$. For every $\Psi \in \mathcal{T}(S)$ we choose a representative $\psi \in \Psi$ such that $\psi(p) = p$. Since $(\tilde{S}, \varphi)$ is an abelian cover of S and $\mathcal{T}(S)$ acts trivially on $\mathrm{H}_1(S, \mathbb{Z})$ we can lift ψ to $\tilde{S}$ in two ways, one which fixes $\tilde{p}$ and one which switches $\tilde{p}$ with the other lift of p. Let $\tilde{\psi}$ be the first lift (the second one is $\xi \circ \tilde{\psi}$). This defines a map $\lambda : \mathcal{T}(S) \to \mathrm{MCG}(\tilde{S})$ which sends every $\Psi \in \mathcal{T}(S)$ to the isotopic class of $\tilde{\psi}$. If $\Psi \in \mathcal{T}(S)$ then $\lambda(\Psi)$ acts on $\mathrm{H}_1(\tilde{S}, \mathbb{Z})$ and leaves $\mathcal{H}$ invariant. It also preserves $(\cdot, \cdot)_{\tilde{S}}$ and $(\cdot, \cdot)_{\mathcal{H}}$. This define a map from $\mathcal{T}(S)$ to $\mathrm{Sp}(\mathcal{H})$. However, this map may depend on the choice of representative ψ of Ψ and may fail to be a homomorphism. But let us now compose λ with π, the homomorphism from isotopy classes of $\mathrm{MCG}(\tilde{S})$ which leaves $\mathcal{H}$ invariant and preserves $(\cdot, \cdot)_{\mathcal{H}}$ into $\mathrm{PSp}(\mathcal{H})$. We define:

$$\rho := \pi \circ \lambda : \mathcal{T}(S) \to \mathrm{PSp}(\mathcal{H}).$$

Proposition 2. *The map ρ is a homomorphism.*

Proof. Since π is a homomorphism is is suffices to show that $\rho(\Psi)$ does not depend on the representative ψ which has been chosen for Ψ.

Let $\Psi \in \mathcal{T}(S)$ and let $\psi_0, \psi_1 \in \Psi$. Let $\tilde{\psi}_0$ and $\tilde{\psi}_1$ be the lifts of ψ_0 and ψ_1 which preserve the point $\tilde{p}$. There is an isotopy $(\psi_t)_{t\in[0,1]}$ between ψ_0 and ψ_1. This isotopy can be lifted to isotopy $(\hat{\psi}_t)_{t\in[0,1]}$ in $\tilde{S}$ such that $\hat{\psi}_0 = \tilde{\psi}_0$. Note that $\hat{\psi}_1$ is a lift of ψ_1 but it does not have to preserve $\tilde{p}$. If $\hat{\psi}_1(\tilde{p}) = \tilde{p}$ then $\hat{\psi}_1 = \tilde{\psi}_1$ which means that $\tilde{\psi}_0$ and $\tilde{\psi}_1$ are isotopic so $\pi([\psi_0]) = \pi([\psi_1])$. On the other hand, if $\hat{\psi}_1(\tilde{p}) \neq \tilde{p}$ then $\hat{\psi}_1 = \xi \circ \tilde{\psi}_1$ when ξ is the non-identity lift to $\tilde{S}$ of the identity on S and $\pi([\psi_0]) = \pi([\xi \circ \psi_1]) = \pi([\xi])\pi([\psi_1]) = \pi([\psi_1])$. $\square$

The goal of the next proposition is to show that the image of ρ is of finite index in $\mathrm{PSp}(2g-2, \mathbb{Z})$. The proof of this proposition is by analyzing certain *Dehn twists* so we briefly recall their definition (for more details see [FM], 2.2 and 7.1).

Let t be a simple closed curve of an oriented surface S and let N be a regular neighborhood of it homoeomorphic to an annulus (the homoeomorphism is required to preserve orientation), which we consider parameterized as

$$\{(r, \theta) \mid 1 \leq r \leq 2 \quad \wedge \quad 0 \leq \theta < 2\pi\}$$

where t is identified with $\{(\frac{3}{2}, \theta) \mid 0 \leq \theta < 2\pi)\}$.

A *Dehn twist* D_t along t is the homeomorphism given by identity outside N and by the map $(r, \theta) \mapsto (r, \theta + 2\pi r)$ on N. The isotopic class of this homeomorphism does not depend on the neighborhood N. The action of D_t induced on $\mathrm{H}_1(S, \mathbb{Z})$ is given by $h \mapsto h + (h, \bar{t})_S \bar{t}$. In particular if $\bar{t} = 0$ then $[D_t] \in \mathcal{T}(S)$.

The following Proposition is a consequence of the more general results in [Lo]. For completeness we give the proof of our concrete case.

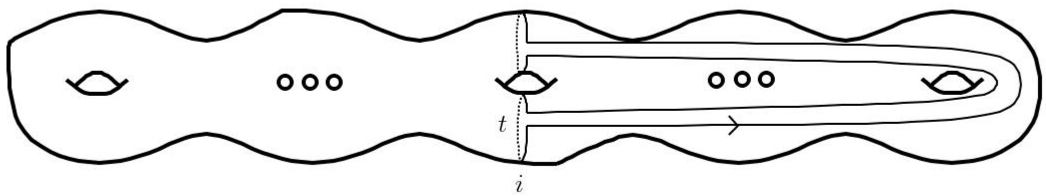

FIGURE 4.

Proposition 3. *The image of* ρ *is a finite index subgroup of* $\mathrm{PSp}(\mathcal{H})$.

Proof. For $i, j \in \{\pm 1, \ldots, \pm(g-1)\}$ with $i \neq \pm j$ we define:

$$\begin{array}{cc} T_i : \mathcal{H} \to \mathcal{H} & T_{i,j} : \mathcal{H} \to \mathcal{H} \\ h \mapsto h + (h, z_{-i})_{\mathcal{H}} z_{-i} & h \mapsto h + (h, z_{-i})_{\mathcal{H}} z_{-j} + (h, z_{-j})_{\mathcal{H}} z_{-i} \end{array}$$

The T_i's and $T_{i,j}$'s are called *elementary symplectic transformations* of $\mathcal{H}$ with respect to the basis $z_1, z_{-1}, \ldots, z_{g-1}, z_{1-g}$ and they generate $\mathrm{Sp}(\mathcal{H})$ [HO]. Let E be the set of elementary symplectic transformations with respect to the above basis. Tits proved that for every $k \in \mathbb{N}^+$ the set $E^k := \{T^k \mid T \in E\}$ generates a finite index subgroup of $\mathrm{Sp}(2g-2, \mathbb{Z})$ ([Tit]). Let $\bar{T}_i \in \mathrm{PSp}(2g-2, \mathbb{Z})$ and $\bar{T}_{i,j} \in \mathrm{PSp}(2g-2, \mathbb{Z})$ be the images of T_i and $T_{i,j}$. In order to prove the Proposition it suffices to show that $\mathrm{Im}\rho$ contains $\bar{E}^4$ where $\bar{E}^4 := \{\bar{T} \mid T \in E^4\}$.

Fix $1 \leq i \leq g-1$. We start by showing that $\bar{T}_i^4 \in \mathrm{Im}\rho$. Let t be the simple closed path of S drawn in Figure 4. Then $[D_t] \in \mathcal{T}(S)$ since $\bar{t} = 0$. The curve t has two disjoint lifts t_1,t_2 to $\tilde{S}$ as shown in figure 5. Thus, $\rho([D_t]) = \pi([D_{t_1}]) \circ \pi([D_{t_2}])$ (since the two lifts are disjoint, the isotopic classes of their Dehn twists commute, so the order of the multiplication is not important). Since $(\cdot,\cdot)_{\mathcal{H}} = \frac{1}{2}(\cdot,\cdot)_{\tilde{S}}$ and $\bar{t}_1 = -\bar{t}_2 = z_{-i}$ then $\pi[D_{t_1}] = \pi[D_{t_2}] = \bar{T}_i^2$ and $\rho([D_t]) = \bar{T}_i^4$.

Next, we show that $\bar{T}_{i,j}^4 \in \mathrm{Im}\rho$ where $1 \leq i \neq j \leq g-1$. Let r be the closed simple path of S drawn in Figure 6. Then $[D_r] \in \mathcal{T}(S)$ since $\bar{r} = 0$. The curve r has two disjoint lifts r_1,r_2 to $\tilde{S}$ as shown in figure 7. Thus, $\rho([D_r]) = \pi([D_{r_1}]) \circ \pi([D_{r_2}])$ and $\bar{r}_1 = -\bar{r}_2 = \bar{z}_{-j} - \bar{z}_{-i}$. Therefore, $\rho([D_r]) = \bar{T}_i^4 \circ \bar{T}_j^4 \circ \bar{T}_{i,j}^{-4}$. Thus, also $\bar{T}_{i,j}^4 \in \mathrm{Im}\,\rho$ since $\bar{T}_i^4, \bar{T}_j^4 \in \mathrm{Im}\,\rho$.

This handle the case of positive i and j. For the general case we can change coordinates and argue as follows:

Fix $\Psi_1, \Psi_2 \in \mathcal{T}(S)$ such that $\rho(\Psi_1) = \bar{T}_i^4$ and $\rho(\Psi_2) = \bar{T}_{i,j}^4$ for $1 \leq i \neq j \leq g-1$. Let $\Delta_i \in \mathrm{MCG}(S)$ be the isotopic class of the composition $D_{b_i} \circ D_{a_i} \circ D_{b_i}$ of Dehn twists. By the formula given in the previous paragraph for the action of a Dehn twist on the first homology we see that:

$$\Delta_i(\bar{a}_i) = \bar{b}_i, \quad \Delta_i(\bar{b}_i) = -\bar{a}_i, \quad \Delta_i(\bar{a}_j) = \bar{a}_j, \quad \Delta_i(\bar{b}_j) = \bar{b}_j.$$

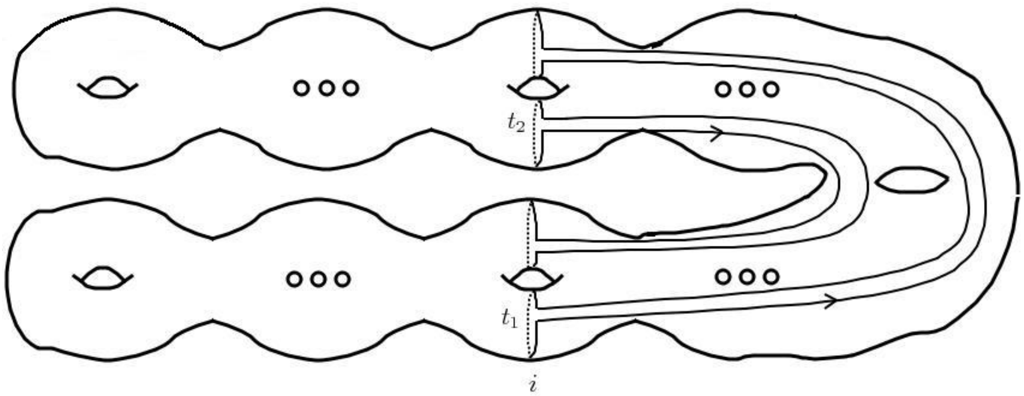

FIGURE 5.

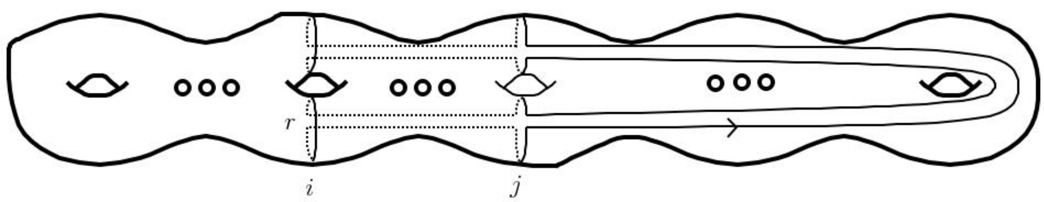

FIGURE 6.

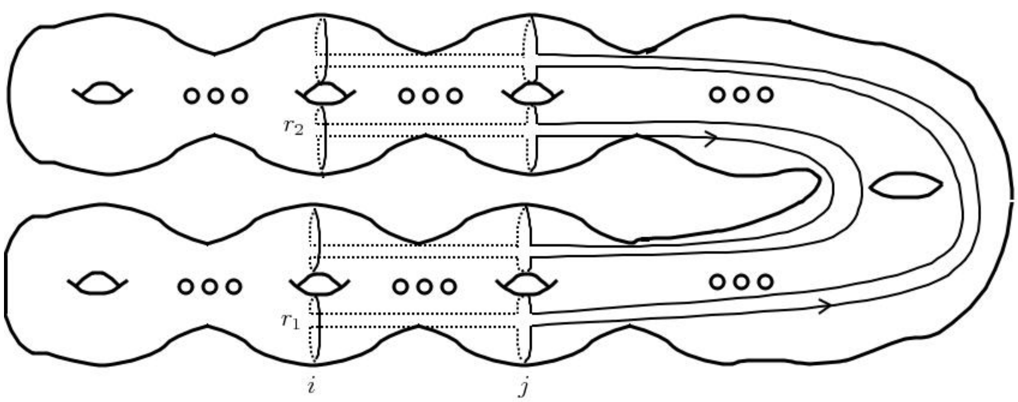

FIGURE 7.

Hence:

$$\begin{array}{cc} \rho(\Delta_i\Psi_1\Delta_i^{-1}) = \bar{T}^4_{-i} & \rho(\Delta_i^{-1}\Psi_2\Delta_i) = \bar{T}^4_{-i,j} \\ \rho(\Delta_j^{-1}\Psi_2\Delta_j) = \bar{T}^4_{i,-j} & \rho(\Delta_i^{-1}\Delta_j^{-1}\Psi_2\Delta_j\Delta_i) = \bar{T}^4_{-i,-j} \end{array}.$$

Thus, if $\bar{T}_i^4, \bar{T}_{i,j}^4 \in \mathrm{Im}\rho$ then so are $\bar{T}_{\pm i}^4, \bar{T}_{\pm i,\pm j}^4 \in \mathrm{Im}\rho$. □

An element of $\mathrm{PSp}(2g-2,\mathbb{Z})$ has two lifts to an elements of $\mathrm{Sp}(2g-2,\mathbb{Z})$. However, the characteristic polynomials of these lifts are all reducible or all irreducible. Thus, we can talk about the reducibility of an element of $\mathrm{PSp}(2g-2,\mathbb{Z})$. We are ready to prove the main proposition of this section.

Proposition 4. *There is a finite number of homomorphisms*

$$\rho_1, \ldots, \rho_n : \mathcal{T}(S) \to \mathrm{PSp}(2g-2,\mathbb{Z})$$

with the following properties:

1. *The homomorphism ρ_i is onto a finite index subgroup of* $\mathrm{PSp}(2g-2,\mathbb{Z})$ *for every $1 \le i \le n$.*
2. *If $\Psi \in \mathcal{T}(S)$ is not pseudo-Anosov then there exist $1 \le i \le n$ such that the characteristic polynomial of $\rho_i(\Psi)$ is reducible.*

Proof. Let $\Psi \in \mathcal{T}(S)$ be a non pseudo-Anosov element.

First assume that there exist $\psi \in \Psi$ satisfying $\psi(a_1) = a_1^{\pm 1}$ or $\psi(c_k) = c_k^{\pm 1}$ for some $1 \le k \le g-2$. In the first case $\rho(\Psi)$ preserves $\langle z_1 \rangle$ while in the second case, it preserves $\langle z_1, z_{-1}, \ldots, z_k, z_k \rangle$ (ψ leaves the two components of $S \setminus c_k$ invariant since it acts trivially on the homology). Thus, if we choose an isomorphism $\delta : \mathrm{PSp}(\mathcal{H}) \to \mathrm{PSp}(2g-2,\mathbb{Z})$ then the characteristic polynomial of $\delta \circ \rho(\Psi)$ is reducible.

Now for a general Ψ, Lemma 1 shows that there is an orientation preserving homeomorphism ν of S such that (1) or (2) of this lemma are satisfied. We can use the above construction of the double cover with respect to $\nu(a_1), \nu(b_1), \ldots, \nu(a_g), \nu(b_g)$ instead of $a_1, b_1, \ldots, a_g, b_g$ to get the desired homomorphism.

This implies that for every $\Psi \in \mathcal{T}(S)$ which is not pseudo-Anosov there are a double cover $(\tilde{S}, \varphi)$ of S, an orientation preserving homeomorphism ν of S and a homomorphism $\rho_{\tilde{S},\nu} : \mathcal{T}(S) \to \mathrm{PSp}(2g-2,\mathbb{Z})$ such that the characteristic polynomial of $\rho_{\tilde{S},\nu}(\Psi)$ is reducible. However, the dependence of $\rho_{\tilde{S},\nu}$ on ν just follows from the choice of basis for $\ker(\mathrm{H}_1(\tilde{S},\mathbb{Z}) \to \mathrm{H}_1(S,\mathbb{Z}))$.

Hence, fix once and for all a basis $B_{\tilde{S}}$ of $\ker(\mathrm{H}_1(\tilde{S},\mathbb{Z}) \to \mathrm{H}_1(S,\mathbb{Z}))$ ($B_{\tilde{S}}$ does not depend on ν or Ψ only on $\tilde{S}$) and define the homomorphism $\rho_{\tilde{S}} : \mathcal{T}(S) \to \mathrm{PSp}(2g-2,\mathbb{Z})$ with respect to this basis. Then, $\rho_{\tilde{S}}(\Psi)$ and $\rho_{\tilde{S},\nu}(\Psi)$ are conjugate so the characteristic polynomial of $\rho_{\tilde{S}}(\Psi)$ is also reducible. This finish the proof since S only has $2^{2g}-1$ double covers. □

3. Random walks and large sieve techniques

We start this section with a formal model for random walks. Let Γ be a group. A finite symmetric subset Σ of Γ is called *admissible* if it generates Γ and satisfies an odd relation, e.g. if it contains the identity (symmetric means $\Sigma = \Sigma^{-1}$). Fix an admissible subset Σ of Γ and endow it with the uniform probability measure. A *walk* w on Γ with respect to Σ is a function $w:\mathbb{N}^+\to\Sigma$. The k^{th}-step of w is $w_k := w(1)\cdots w(k)$ (in particular, w_0 is the identity). The probability measure on Σ induces a product probability measure on the set of Σ-walks $\Sigma^{\mathbb{N}^+}$. For a subset Z of Γ we denote the probability that the k^{th}-step of a walk belongs to Z by $\text{prob}(w_k\in Z)$. The set Z is called *exponentially small with respect to* Σ if there are constants $c,\alpha>0$ such that $\text{prob}(w_k\in Z)\le ce^{-\alpha k}$ for every $k\in\mathbb{N}$. A set is *exponentially small* if it exponentially small with respect to every admissible subset of Γ.

The following theorem follows immediately from Theorem 2 of [LM]:

Theorem 5. *Let Γ be a finitely generated group and let $\mathcal{P}$ the set of all but finitely many primes. Let $(N_p)_{p\in\mathcal{P}}$ be a series of finite index normal subgroups of Γ. Assume that there is a constant $d\in\mathbb{N}^+$ such that:*

1. *Γ has property-τ with respect to the series of normal subgroup $(N_p\cap N_q)_{p,q\in\mathcal{P}}$.*
2. *$|\Gamma_p|\le p^d$ for every $p\in\mathcal{P}$ where $\Gamma_p:=\Gamma/N_p$.*
3. *The natural map $\Gamma_{p,q}\to\Gamma_p\times\Gamma_q$ is an isomorphism for every distinct $p,q\in\mathcal{P}$ where $\Gamma_{p,q}:=\Gamma/(N_p\cap N_q)$.*

Then a subset $Z\subseteq\Gamma$ is exponentially small if there is $c>0$ such that:

4. *$\frac{|Z_p|}{|\Gamma_p|}\le 1-c$ for every $p\in\mathcal{P}$ where $Z_p:=ZN_p/N_p$.*

See Section 2 of [LM] or [Lu1] for the definition of property-τ. We are ready to prove our main theorem:

Theorem 6. *Let S be an orientable connected compact surface of genus $g\ge 3$ and denote its Torelli subgroup by $\mathcal{T}(S)$. The set $Z\subseteq\mathcal{T}(S)$ consisting of non-pseudo-Anosov elements is exponentially small.*

Proof. Let $\rho_1,\ldots,\rho_n:\mathcal{T}(S)\to\text{PSp}(2g-2,\mathbb{Z})$ be the homomorphisms of Proposition 4. For every $1\le i\le n$, define $Z_i:=\rho_i^{-1}(R)$ where $R\subseteq\text{PSp}(2g-2,\mathbb{Z})$ consisting of the elements with reducible characteristic polynomial. We have $Z\subseteq\cup_{1\le i\le n}Z_i$ so it is enough to prove that for such an i the set Z_i is exponentially small. Fix $1\le i\le n$.

For every prime p define $\psi_p:=\pi_p\circ\rho_i$ and $N_p:=\ker\psi_p$ where π_p is the modulo-p map $\text{PSp}(2g-2,\mathbb{Z})\to\text{PSp}(2g-2,\mathbb{Z}/p\mathbb{Z})$. The image of ρ_i in $P\,\text{Sp}(2g-2,\mathbb{Z})$ is of finite index. This and the fact that $\text{PSp}(2g-2,\mathbb{Z}/p\mathbb{Z})$ is simple for $p\ge 3$ implies that for large enough prime p the image of ψ_p is $\text{PSp}(2g-2,\mathbb{Z}/p\mathbb{Z})$. Let $\mathcal{P}$ be the set of large enough primes. We have to check that the four conditions of Theorem 5 are satisfied.

Condition 1 follows from the fact that $\text{PSp}(2g-2,\mathbb{Z})$ has property-τ with respect to the family of congruence subgroups and the fact that property-τ is inherited by finite index subgroups (see for example [Lu1]). Condition 2 is readily true for $d=(2g-2)^2$. Condition 3 follows from the fact that for distinct primes $p, q \geq 3$ the groups $\mathrm{PSp}(2g-2, \mathbb{Z}/p\mathbb{Z})$ and $\mathrm{PSp}(2g-2, \mathbb{Z}/q\mathbb{Z})$ are simple and non-isomorphic. Finally condition 4 was proved by Chavdarov [Ch] (see also [Ri1]). □

Remark. The method of proof actually applies to many other subgroups of $\mathrm{MCG}(S)$ besides the Torelli subgroup. In fact, by combining strong approximation [We] and the result of Salehi-Golsefidy-Varju about property-τ [SGV], the proof applies to all subgroups Γ of $\mathcal{T}(S)$ such that for every $1 \leq i \leq n$ the group $\rho_i(\Gamma)$ is Zariski-dense subgroup of $\mathrm{PSp}(2g-2, \mathbb{Z})$ where the notations are as in Proposition 4. In particular, the result applies to all finite index subgroup of $\mathcal{T}(S)$.

Another interesting class of subgroups are the Johnson subgroups. For every $k \in \mathbb{N}^+$ let $J(k)$ be the kernel of the action of $\mathrm{MCG}(S)$ on $\pi_1(S)/\gamma_i(\pi_1(S))$ where $\pi_1(S)$ is the fundamental group of S and $\gamma_i(\pi_1(S))$ is the i^{th}-subgroup in the lower central series of $\pi_1(S)$. The Torelli group is just $J(2)$ and for every $k \geq 2$ the group $J(2)/J(k)$ is nilpotent. The group $\mathrm{PSp}(2g-2, \mathbb{Z})$ has property-T for $g \geq 3$ so if H is a finite index subgroup of $\mathrm{PSp}(2g-2, \mathbb{Z})$ and $L \lhd H$ is co-nilpotent then L is of finite index in H. Thus, for every $k \geq 2$ and every $1 \leq i \leq n$ the group $\rho_i(J(k))$ is a finite index subgroup of $\mathrm{PSp}(2g-2, \mathbb{Z})$ and in particular Zariski-dense.

For $k \geq 3$ the group $J(k)$ is unlikely to be finitely generated. However the previous discussion shows that there is a finite set $R(k) \subseteq J(k)$ such that if $L(k)$ is a finitely generated subgroup of $J(k)$ which contains $R(k)$ then for every $1 \leq i \leq n$ the group $\rho_i(L(k))$ is a Zariski-dense subgroup of $\mathrm{PSp}(2g-2, \mathbb{Z})$. Thus, the set of non-pseudo-Anosov elements of $L(k)$ is exponentially small.

This shows that in some sense Theorem 6 is true for "sufficiently large" finitely generated subgroups of $\mathcal{T}(S)$, e.g. subgroups which contains $R(k)$. The use here of the term "sufficiently large" should be compared to the one in [Ma] where the term "sufficiently large" subgroup refer to a subgroup which contains a pair of pseudo-Anosov elements with distinct fixed points in the space of projective measured laminations.

References

[BC] S. A. Bleiler and A. J. Casson, *Automorphisms of surfaces after Nielsen and Thurston.* London Mathematical Society Student Texts, 9. Cambridge University Press, Cambridge, 1988. iv+105 pp.

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

[Ch] N. I. Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy.* Thesis (Ph.D.)Princeton University. 1995. 56 pp, ProQuest LLC, Thesis More links

[FM] Benson Farb and Dan Margalit. A primer on mapping class groups. preprint. www.math.utah.edu/ margalit/primer/.

[GL1] F. Grunewald and A. Lubotzky,*Linear representations of the automorphism group of a free group*. Geom. Funct. Anal. 18 (2009), no. 5, 15641608.

[GL2] F. Grunewald and A. Lubotzky,*Arithmetic quotients of the mapping class group.* In preperation.

[HO] A.J. Hahn and O.T O'Meara, *The classical groups and KK-theory.* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 291. Springer-Verlag, Berlin, 1989. xvi+576 pp.

[Iv1] Nikolai V. Ivanov. Subgroups of Teichmuller modular groups, volume 115 of Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, 1992.

[Ko] Emmanuel Kowalski. The Large Sieve And Its Applications. Arithmetic geometry, random walks and discrete groups. Cambridge Tracts in Mathematics, 175. Cambridge University Press, Cambridge, 2008.

[Lo] Eduard Looijenga. Prym representations of mapping class groups. Geom. Dedicata 64 (1997), no. 1, 69–83.

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

[Lu1] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, with an appendix by Jonathan D. Rogawski. Reprint of the 1994 edition. Modern Birkhuser Classics. Birkhuser Verlag, Basel, 2010. iii+192 pp.

[Lu2] A. Lubotzky, *Expanders in pure and applied mathematics*, Bull. AMS, to appear. arXiv:1105.2389v1.

[Ma] J. Maher, *Random walks on the mapping class group.* Duke Math. J. 156 (2011), no. 3, 429–468.

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

[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.

[SGV] A. Salehi-Golsefidy and P. Varju. *Expansion in perfect groups.* Preprint.

[Tit] Jacques Tits. Systèmes générateurs de groupes de congruence. (French) C. R. Acad. Sci. Paris Se'r. A-B 283 (1976), no. 9, Ai, A693–A695.

[We] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups.* Ann. of Math. (2) 120 (1984), no. 2, 271–315.

Einstein Institute of Mathematics, Hebrew University, Jerusalem 90914, Israel

E-mail address: alexlub@math.huji.ac.il, chen.meiri@mail.huji.ac.il