Rank one phenomena for mapping class groups

Benson Farb[*], Alexander Lubotzky[†] and Yair Minsky[‡]

March 6, 2000

1 Introduction

Let Σ_g be a closed, orientable, connected surface of genus $g \geq 1$. The *mapping class group* $\mathrm{Mod}(\Sigma_g)$ is the group $\mathrm{Homeo}^+(\Sigma_g)/\mathrm{Homeo}_0(\Sigma_g)$ of isotopy classes of orientation-preserving homeomorphisms of Σ_g. It has been a recurring theme to compare the group $\mathrm{Mod}(\Sigma_g)$ and its action on the Teichmüller space $\mathcal{T}(\Sigma_g)$ to lattices in simple Lie groups and their actions on the associated symmetric spaces.

Indeed, the groups $\mathrm{Mod}(\Sigma_g)$ share many of the properties of (arithmetic) lattices in semisimple Lie groups. For example they satisfy the Tits alternative, they have finite virtual cohomological dimension, they are residually finite, and each of their solvable subgroups is polycyclic.

A well-known dichotomy among the lattices in simple Lie groups is between lattices in rank one groups and higher-rank lattices, i.e. those lattices in simple Lie groups of $\mathbf{R}$-rank at least two. It is somewhat mysterious whether $\mathrm{Mod}(\Sigma_g)$ is similar to the former or the latter. Some higher rank behavior of $\mathrm{Mod}(\Sigma_g)$ is indicated by the cusp structure of moduli space, by the fact that $\mathrm{Mod}(\Sigma_g)$ has Serre's property (FA) [CV], and by Ivanov's version (see, e.g. [Iv2]) for $\mathrm{Mod}(\Sigma_g)$ of Tits's Theorem on automorphism groups of higher rank buildings.

In this note we add two more properties to the list (see, e.g. [Iv1, Iv2, Iv3] and the references therein) of properties which exhibits similarities of $\mathrm{Mod}(\Sigma_g)$ with lattices in rank one groups: every infinite order element of $\mathrm{Mod}(\Sigma_g)$ has linear growth in the word metric, and $\mathrm{Mod}(\Sigma_g)$ is not bound-

[*]Supported in part by NSF grant DMS 9704640 and by a Sloan Foundation fellowship.
[†]Supported in part by the US-Israel BSF grant.
[‡]Supported in part by NSF grant DMS 9971596

edly generated. In addition, we present a restriction on low-dimensional representations of $\mathrm{Mod}(\Sigma_g)$ which has a higher rank flavor.

Dehn twists have linear growth. In Section 2 we prove that Dehn twists have linear growth with respect to the word metric on the mapping class group of an oriented surface of finite type (Theorem 1.1). This answers a question of Ivanov in [Iv1]. A proof in the case of punctured surfaces was given by Mosher [Mo] using his techniques for constructing an automatic structure on the mapping class group.

This result implies in particular that the embedding of the mapping class group as an orbit in Teichmüller space is not a Lipschitz equivalence (Theorem 2.1). This should be viewed in comparison with the opposite conclusion for higher-rank lattices, by Lubotzky-Mozes-Raghunathan [LMR1].

Theorem 1.1 *Let $\Sigma_{g,m}$ be an oriented surface of genus g and m punctures. Fix a finite generating set for $Mod(\Sigma_{g,m})$ and let $||\cdot||$ denote minimal word length with respect to these generators. Then every Dehn twist t has linear growth in $Mod(\Sigma_{g,m})$, i.e. there exists a constant $c > 0$ so that*

$$||t^n|| \geq c|n|$$

for all n.

Equivalently, one can say that t has *positive translation distance* in the sense of Gersten and Short [GS], that is

$$d(t) = \liminf_{n\to\infty} \frac{||t^n||}{n} > 0.$$

More generally, by previously known results we can conclude the following.

Theorem 1.2 *Every element of infinite order in $Mod(\Sigma_{g,m})$ has linear growth.*

Theorem 1.2 should be compared with [LMR1], which shows that non-cocompact, irreducible lattices in higher rank contain elements with logarithmic growth (so-called *U-elements*). This does not happen for lattices in rank one groups (see [LMR1, LMR2]).

The bounded generation property. Recall that a group Γ is *boundedly generated* if there is a finite set of elements $\{a_1, \ldots, a_n\}$ of Γ so that every element $g \in \Gamma$ can be written

$$g = a_1^{m_1} \cdots a_n^{m_n}$$

for some $m_1, \ldots, m_n \in \mathbf{Z}$. In other words, Γ is the (set-theoretic) product of a finite number of cyclic groups. It was shown by Tawgen [Ta] to hold for most (and conjecturally for all) non-cocompact lattices in higher rank simple Lie groups. On the other hand, word-hyperbolic groups are not boundedly generated (see §3.5), and therefore neither are cocompact lattices in rank one groups. It also seems likely that non-cocompact lattices in rank one groups are not boundedly generated.

Theorem 1.3 *For $g \geq 1$, the group Mod(Σ_g) is not boundedly generated.*

In fact we prove a stronger result:

Theorem 1.4 *For every $g \geq 1$ and every prime p, the group Mod(Σ_g) has a finite index subgroup H whose pro-p completion $H_{\hat{p}}$ is not a p-adic analytic group.*

If a group is boundedly generated then so is every finite-index subgroup. Also, the pro-p completion of a boundedly generated group is p-adic analytic. Thus Theorem 1.4 implies Theorem 1.3.

Recall that a pro-finite group is *boundedly generated* if it is the set-theoretic product of finitely many pro-cyclic groups. It is known ([Lu, PR]) that arithmetic groups have the congruence subgroup property if and only if their profinite completion is boundedly generated. This property is known to hold for all non-cocompact, higher-rank lattices and for most cocompact ones. An analogue of the congruence subgroup property for $\mathrm{Mod}(\Sigma_g)$ has been conjectured by Ivanov [Iv1]. On the other hand, Theorem 1.4 has the following consequence.

Corollary 1.5 *The pro-finite completion of Mod(Σ_g) is not boundedly generated as a profinite group*

It should be stressed, however, that Corollary 1.5 does not contradict Ivanov's conjecture, as the equivalence between the congruence subgroup property and bounded generation of the profinite completion is valid only for arithmetic groups.

Low-dimensional representations of Mod(Σ_g). It is a well-known open question whether the mapping class group $\mathrm{Mod}(\Sigma_g), g > 1$ has a faithful linear representation $\psi : \mathrm{Mod}(\Sigma_g) \to \mathrm{GL}(n, \mathbf{C})$ for some $n \geq 2$. In Section 4 we show that such representations, even for finite index subgroups of $\mathrm{Mod}(\Sigma_g)$, do not exist for $n < 2\sqrt{g-1}$.

Theorem 1.6 *Let H be any finite index subgroup of Mod$(\Sigma_g), g \geq 2$. Then there is no faithful representation $\psi : H \to GL(n, \mathbf{C})$ for $n < 2\sqrt{g-1}$.*

2 Growth of Dehn twists

To show that a power T_α^n of a Dehn twist cannot be expressed as a product of a smaller than linear number of generators, we need a way to measure the "twistiness" of any element of $\mathrm{Mod}(\Sigma)$ around α, in such a way that T_α^n twists n times and any generator twists a bounded amount. Note that this cannot be made group-theoretically precise, since $\mathrm{Mod}(\Sigma)$ does not admit a non-trivial homomorphism to $\mathbf{Z}$ (see, e.g. [Ha])

In the rest of the section we will assume that Σ is hyperbolic of finite volume. This rules out $\Sigma_{0,n}$ for $n \leq 3$, for which $\mathrm{Mod}(S)$ is trivial or finite, and the torus $\Sigma_{1,0}$, for which $\mathrm{Mod}(\Sigma) = \mathrm{SL}(2, \mathbf{Z})$ and the theorem is known. (At any rate since $\mathrm{SL}(2, \mathbf{Z})$ is also $\mathrm{Mod}(\Sigma_{1,1})$ and $\mathrm{Mod}(\Sigma_{0,4})$ this case is covered).

2.1 The annulus complex and relative twists

Let $Y = S^1 \times [0,1]$ be an oriented annulus and let $\mathcal{A}(Y)$ denote the set of arcs joining $S^1 \times \{0\}$ to $S^1 \times \{1\}$, up to homotopy with endpoints fixed. If a and b in $\mathcal{A}(Y)$ do not share any endpoints then we can define their algebraic intersection number $a \cdot b$. (The arcs inherit an orientation from any fixed orientation on $[0,1]$, and if this orientation is reversed then the senses of the intersections are unchanged.) We also define $a \cdot a = 0$.

A lift of any $a \in \mathcal{A}(Y)$ to $\widetilde{Y} = \mathbf{R} \times [0,1]$ has endpoints $(a_0, 0)$ and $(a_1, 1)$, well-defined up to translation (of both) by $\mathbf{Z}$. We can immediately check that, with appropriate choice of orientation of Y,

$$a \cdot b = \lfloor b_1 - a_1 \rfloor - \lfloor b_0 - a_0 \rfloor$$

(where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x). It then follows that

$$a \cdot c = a \cdot b + b \cdot c + \Delta \tag{1}$$

where $\Delta \in \{0, 1, -1\}$, for any $a, b, c \in \mathcal{A}(Y)$ such that the intersection numbers are defined.

Now to any essential simple closed curve α in Σ we can associate a closed annulus $Y = Y_\alpha$ as follows: Let g_α be an isometry of $\mathbf{H}^2$ representing the conjugacy class of α, and let $Y = (\overline{\mathbf{H}}^2 \setminus Fix(g_\alpha))/\langle g_\alpha \rangle$, where $\overline{\mathbf{H}}^2$ is the standard closed-disk compactification of $\mathbf{H}^2$. For any simple curve β in Σ we can consider its lift to $int(Y)$. If β is not homotopic to α then its endpoints are distinct from those of α and hence each component of its lift extends to a properly embedded arc in Y.

Let $\mathbf{lift}_\alpha(\beta)$ denote the subset of components that connect the two boundaries of Y, viewed as a subset of $\mathcal{A}(Y)$. This set is always finite, and nonempty if β crosses α at least once.

The set of all arcs that arise in this way have mutually disjoint endpoints since any two elements of $\pi_1(S)$ acting on $\mathbf{H}^2$ with asymptotic axes must be the same up to finite powers. Thus the intersection numbers are well-defined among all these lifts. Let us now define, for α, β and γ simple closed curves in Σ, a subset of $\mathbf{Z}$:

$$\tau_\alpha(\beta,\gamma) \equiv \{b \cdot c : b \in \mathbf{lift}_\alpha(\beta), c \in \mathbf{lift}_\alpha(\gamma)\}.$$

(If β or γ is disjoint from α then this is the empty set). Since the components of $\mathbf{lift}_\alpha(\beta)$ are mutually disjoint (and similarly for $\mathbf{lift}_\alpha(\gamma)$), we obtain from (1) that $\operatorname{diam}(\tau_\alpha(\beta,\gamma)) \leq 2$.

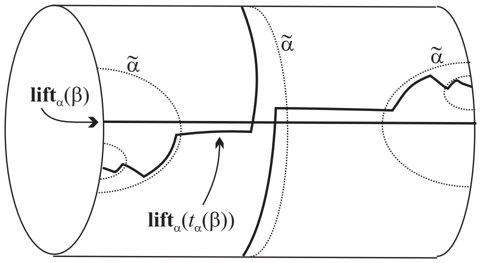

Figure 1: The effect of a Dehn twist on the lift to the annulus

Let $t = T_\alpha$ be a (leftward) Dehn twist on α. The effect of t^n for $n > 0$ on β, lifted to the components of $\mathbf{lift}_\alpha(\beta)$, is to twist each component n times around the annulus, and shift the endpoints a little up on $S^1 \times \{1\}$ and a little down on $S^1 \times \{0\}$ (if $n < 0$ then up and down are interchanged). The shift of endpoints comes from the intersections of $\mathbf{lift}_\alpha(\beta)$ with the non-closed components of the lift of α to Y (see Figure 1). It follows directly that

$$\tau_\alpha(\beta, t^n(\beta)) \subset \{n, n+1\} \tag{2}$$

Furthermore, we have the following properties. If β and γ intersect α, then their intersection number bounds their relative twisting:

$$\max |\tau_\alpha(\beta,\gamma)| \leq i(\beta,\gamma) + 1 \tag{3}$$

(Here $i(\cdot,\cdot)$ denotes unoriented geometric intersection number, and by $|A|$ for $A \subset \mathbf{R}$ we mean $\{|a| : a \in A\}$.)

To see this, note first that if $i(\beta, \gamma) = 0$ then $\tau_\alpha(\beta, \gamma) = \{0\}$ so we may assume $i(\beta, \gamma) \geq 1$. Let b and c be components of $\mathbf{lift}_\alpha(\beta)$ and $\mathbf{lift}_\alpha(\gamma)$, respectively. We may assume that b and c intersect exactly $k = |b \cdot c|$ times in the annulus. If $k = 2$ there is nothing to prove, so assume $k > 2$. Let $b_1, \ldots, b_{k-1}$ be successive segments of b bounded by points of $b \cap c$, and let $c_1, \ldots, c_{k-1}$ be the corresponding segments of c, so that $A_i = b_i * c_i$ is a simple closed curve homotopic to the core of Y, and A_i and A_j are distinct for $i < j$. If A_i and A_j map to the same curve in Σ then the region they bound is identified to make a torus covering Σ, contradicting the assumption that Σ is hyperbolic. Thus all the b_i have distinct projections to Σ, and in particular there are at least $k-1$ intersection points of β with γ. This proves inequality (3).

Finally, for β, γ and δ crossing α we have:

$$\max \tau_\alpha(\beta, \delta) \leq \max \tau_\alpha(\beta, \gamma) + \max \tau_\alpha(\gamma, \delta) + 2 \tag{4}$$

and similarly

$$\min \tau_\alpha(\beta, \delta) \geq \min \tau_\alpha(\beta, \gamma) + \min \tau_\alpha(\gamma, \delta) - 2. \tag{5}$$

These follow immediately from applying equation (1) to the components of $\mathbf{lift}_\alpha(\beta)$, $\mathbf{lift}_\alpha(\gamma)$, and $\mathbf{lift}_\alpha(\delta)$.

2.2 Proof of Theorem 1.1

Let t be a Dehn twist on α. Without loss of generality assume that t is a leftward twist, so that (2) holds.

A set M of simple closed curves *binds* Σ if every nontrivial, nonperipheral curve in Σ intersects some element of M. Let us choose a particular binding set P as follows: extend α to a pants decomposition of Σ (a maximal collection of disjoint non-homotopic essential curves), and then for each pants curve β add a curve β' which crosses β once or twice, and misses the other pants curves. Let α' be the curve in P that crosses α.

Now for any set M of simple closed curves in Σ, define

$$\tau(M) = \bigcup_{\mu \in M} \tau_\alpha(\alpha', \mu).$$

In particular, $\tau(P) = \{0\}$. Note that $\tau(M)$ is always nonempty when M binds Σ.

Let X be some fixed finite generating set for $\mathrm{Mod}(\Sigma)$. Assume without loss of generality that $n > 0$, and suppose we can write t^n as a word $w =$

$g_1 \circ \cdots \circ g_m$, with each $g_i \in X$. Let w_j denote the subword $g_1 \circ \cdots \circ g_j$, and let $P_j = w_j(P)$. We will prove that

$$\max \tau(P_{j+1}) \leq \max \tau(P_j) + K \tag{6}$$

for a fixed K.

Define

$$B = \max\{i(\beta, \gamma) : \beta \in P, \gamma \in g(P), g \in X\}$$

which is finite since the maximum is over a finite set. Since $w_{j+1}(P) = w_j(g_{j+1}(P))$ for any j, and intersection number is $\mathrm{Mod}(\Sigma)$-invariant, we have for each j, for all $\beta \in P_j$ and $\gamma \in P_{j+1}$, that

$$i(\beta, \gamma) \leq B.$$

Inequality (3) then implies that, for any $\beta \in P_j$ and $\gamma \in P_{j+1}$ which cross α, $\max |\tau_\alpha(\beta, \gamma)| \leq B + 1$. Then applying (4), we find that

$$\max \tau_\alpha(\alpha', \gamma) \leq \max \tau_\alpha(\alpha', \beta) + B + 3.$$

This establishes (6). Now, since we know (using (2)) that $\tau(w(P)) = \tau_\alpha(\alpha', t^n(\alpha')) \subset \{n, n+1\}$, it follows that the length m of w is at least $n/(B+3)$. This concludes the proof.

Note that the constants can be made explicit if the set of generators X is adapted nicely to P – for example if they are Dehn twists on the components of P.

2.3 Corollaries

Theorem 1.2, that every infinite order element of $\mathrm{Mod}(\Sigma)$ has linear growth, is now easy to put together from known results. The case of simultaneous Dehn twists around a collection of disjoint curves is done in the same way as for a single curve, computing the twisting numbers separately for each component. The case of an element h which is pseudo-Anosov or is reducible and has a power which is pseudo-Anosov on some subsurface is already known – the argument uses the exponential growth of lengths of curves under h (see Mosher [Mo]). By Thurston's classification of elements of $\mathrm{Mod}(\Sigma)$ [FLP], these are all possible cases.

The second corollary of Theorem 1.1 is the following statement for the Teichmüller space $\mathcal{T}(\Sigma)$ of Σ, on which $\mathrm{Mod}(\Sigma)$ acts properly discontinuously. Fixing a basepoint $x_0 \in \mathcal{T}(\Sigma)$, we may embed $\mathrm{Mod}(\Sigma)$ in $\mathcal{T}(\Sigma)$ as an orbit, i.e. $g \mapsto g(x_0)$. Endowing $\mathcal{T}(\Sigma)$ with the Teichmüller metric $d_{\mathcal{T}}$, we induce a metric on $\mathrm{Mod}(\Sigma)$ by inclusion. We then have

Theorem 2.1 *The word metric on $Mod(\Sigma)$ and the metric induced by inclusion as an orbit in $\mathcal{T}(\Sigma)$ are not Lipschitz equivalent.*

Here Lipschitz equivalent means distances in the two metrics are within bounded ratio.

To obtain this result one just needs to know that the translation distance of a Dehn twist in Teichmüller space,

$$\inf_{x \in \mathcal{T}(\Sigma)} d_{\mathcal{T}}(x, t(x)),$$

is zero, and furthermore

$$d_{\mathcal{T}}(x, t^n(x)) = O(\log |n|)$$

for any $x \in \mathcal{T}(\Sigma)$. In fact Marden-Masur show [MM] that each x is contained in a totally geodesic copy of the hyperbolic plane (a Teichmüller disk) invariant by t, on which t acts as a parabolic isometry.

The situation is similar for non-cocompact lattices in rank-one Lie groups. For example a parabolic element in a non-cocompact lattice in $SO(n,1) = Isom(\mathbf{H}^n)$ has linear growth in the word metric but logarithmic growth in the left-invariant metric on $SO(n,1)$.

By contrast, the situation in a higher-rank semisimple linear Lie group G is the opposite. Lubotzky-Mozes-Raghunathan have shown [LMR1] that for an irreducible lattice Γ in G the word metric and the metric induced from G *are* Lipschitz-equivalent. For example, a unipotent element of $\mathrm{SL}(3, \mathbf{Z})$ has logarithmic growth both in $\mathrm{SL}(3, \mathbf{R})$ *and* in the word metric of $\mathrm{SL}(3, \mathbf{Z})$.

As a concrete example, the matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has linear growth as an element of $\mathrm{SL}(2, \mathbf{Z})$, but as a matrix in $\mathrm{SL}(3, \mathbf{Z})$ via the "upper left hand corner" embedding $\mathrm{SL}(2, \mathbf{Z}) \to \mathrm{SL}(3, \mathbf{Z})$ it has logarithmic growth.

3 Pro-p groups and mapping class groups

3.1 Some pro-p preliminaries

Let us briefly recall some definitions from the theory of pro-p groups. Further details and proofs may be found in [DDMS].

A *profinite group* G is a compact, Hausdorff topological group which is (topologically) isomorphic to an inverse limit of finite groups. Let p be a fixed prime. The profinite group G is a *pro-p* group if it is topologically isomorphic to an inverse limit of finite p-groups.

The *pro-p* completion $H_{\hat{p}}$ of a group H is defined as the inverse limit

$$H_{\hat{p}} = \lim H/N$$

where the limit is taken over all normal subgroups whose index is a power of p. For example, the p-adic numbers $\mathbf{Q}_p$ are the pro-p completion of $\mathbf{Q}$.

A profinite group G is *finitely generated* (as a profinite group) if it contains a finite subset $S \subset G$ so that the topological closure of the group generated by S equals all of G.

A profinite group is *p-adic analytic* if it has the structure of a Lie group over $\mathbf{Q}_p$. In particular every such group has a well-defined *dimension*.

A p-adic analytic profinite group always contains a pro-p subgroup of finite index. See [DDMS] for various characterizations of p-adic analyticity of pro-p groups. A typical example of a compact p-adic analytic group is any closed subgroup of $\mathrm{SL}(n, \mathbf{Z}_p)$; in fact this ends up being all examples (see [DDMS]). In particular, closed subgroups of compact, p-adic analytic groups are analytic. It is also known that an analytic pro-p group is finitely generated (as a pro-p group).

3.2 Analyticity and extensions

In many cases, if the pro-p completion $G_{\hat{p}}$ of a group G is taken, then the closure of a subgroup N in $G_{\hat{p}}$ is very small with respect to $N_{\hat{p}}$ (the pro-p completion of N). In other words, the pro-p topology of G induces on N a topology which is much weaker than the pro-p topology of N. The following lemma asserts (when N is f.g. normal in a discrete G) that, after passing to a finite index subgroup L, "most of" $N_{\hat{p}}$ is preserved.

Lemma 3.1 *Let*

$$1 \to N \to G \to H \to 1$$

be an exact sequence of discrete groups. Assume that N is finitely generated. Then G has a finite index subgroup L containing N, so that the closure $\overline{N}$ of N in the pro-p completion of L is mapped onto $N_{\hat{p}}/Z(N_{\hat{p}})$, the pro-p completion of N modulo its center.

Proof. G acts on N by conjugation. This defines a homomorphism $\rho : G \to \mathrm{Aut}(N)$. We also have the natural homomorphism $\psi : \mathrm{Aut}(N) \to \mathrm{Aut}(N_{\hat{p}})$. Since N is finitely generated, the group $N_{\hat{p}}$ is finitely generated as a pro-p group. As such, it is known (see Theorem 5.6 of [DDMS]) that $\mathrm{Aut}(N_{\hat{p}})$ is a virtually pro-p group, that is, $\mathrm{Aut}(N_{\hat{p}})$ has a normal open pro-p subgroup. In fact

$$K = \mathrm{Ker}(\mathrm{Aut}(N_{\hat{p}}) \to \mathrm{Aut}(N_{\hat{p}}/[N_{\hat{p}}, N_{\hat{p}}]N_{\hat{p}}^{p}))$$

is a normal pro-p subgroup of finite index in $\mathrm{Aut}(N_{\hat{p}})$.

Let $L = (\psi \circ \rho)^{-1}(K)$. Then L has finite index in G. Moreover, L contains N since N acts trivially on $N_{\hat{p}}/[N_{\hat{p}}, N_{\hat{p}}]N_{\hat{p}}^{p}$. So we have a map $\psi \circ \rho$ from L into the pro-p group K. Now if $j : L \to L_{\hat{p}}$ is the canonical map from L into its pro-p completion, then we have a map $\pi : L_{\hat{p}} \to K$ so that

$$\pi \circ j = (\psi \circ \rho)|_L$$

Let $\overline{N}$ be the closure of $j(N)$ in $L_{\hat{p}}$. Then

$$\pi(\overline{N}) = \overline{\psi \circ \rho(N)}$$

and it is easy to see that $\overline{\psi \circ \rho(N)}$ is just equal to the group of inner automorphisms of $N_{\hat{p}}$, that is:

$$\pi(\overline{N}) = \overline{\psi \circ \rho(N)} = N_{\hat{p}}/Z(N_{\hat{p}})$$

Thus $\overline{N}$, which is a quotient of $N_{\hat{p}}$, is also mapped onto $N_{\hat{p}}/Z(N_{\hat{p}})$ and the lemma is proven. $\diamond$

We will need the following elementary lemma about nilpotent groups.

Lemma 3.2 *If Γ is a finitely generated, torsion-free nilpotent group of class k, then the dimension of $\Gamma_{\hat{p}}$ is at least k.*

Proof. The lemma follows easily by induction on k. $\diamond$

Let us recall that a finitely generated group N is called *residually torsion-free nilpotent* if, for every $g \in N$, there exists a torsion-free nilpotent group N_0 and a homomorphism $\phi : N \to N_0$ with $\phi(g) \neq 0$.

Lemma 3.3 *Let N be a finitely generated residually torsion-free nilpotent group which is not nilpotent. Then for every prime p, the groups $N_{\hat{p}}$ and $N_{\hat{p}}/Z(N_{\hat{p}})$ are not p-adic analytic groups.*

Proof. Assume $N_{\hat{p}}/Z(N_{\hat{p}})$ is a p-adic analytic group of dimension r. Let M be any finitely generated torsion-free nilpotent group which is a quotient of N. By our assumptions on N, there are infinitely many such groups M of arbitrarily high nilpotency class, for otherwise N itself would be nilpotent. Let M be such a quotient of N of class at least $r+2$. Hence $M/Z(M)$ is of class at least $r+1$. By Lemma 3.3 applied to $M/Z(M)$, we have that the dimension of $(M/Z(M))_{\hat{p}}$ is at least $r+1$. But this group is a quotient of $N_{\hat{p}}/Z(N_{\hat{p}})$, which is of dimension r, a contradiction.

Hence $N_{\hat{p}}/Z(N_{\hat{p}})$ is not p-adic analytic. Since quotient groups of p-adic analytic groups are p-adic analytic ([DDMS], Theorem 10.7), it follows that $N_{\hat{p}}$ is not p-adic analytic. $\diamond$

Combining Lemma 3.1 and Lemma 3.3 gives the following.

Corollary 3.4 *Let*

$$1 \to N \to G \to H \to 1$$

be an exact sequence of discrete groups. Assume that N is finitely generated, residually torsion-free nilpotent, but not nilpotent. Then G has a finite index subgroup L containing N so that $L_{\hat{p}}$ is not p-adic analytic.

Proof. By Lemma 3.1, G has such a subgroup L for which $\overline{N}$, the closure of N in $L_{\hat{p}}$, is mapped onto $N_{\hat{p}}/Z(N_{\hat{p}})$. By Lemma 3.3, the group $N_{\hat{p}}/Z(N_{\hat{p}})$ is not p-adic analytic. Thus $\overline{N}$ and $L_{\hat{p}}$ are not p-adic analytic since subgroups and quotient groups of analytic pro-p groups are analytic ([DDMS], Theorem 10.7). $\diamond$

3.3 Proof of Theorem 1.4

We can now prove Theorem 1.4. First, for $g = 1$, the group $\mathrm{Mod}(\Sigma_g)$ is isomorphic to $\mathrm{SL}(2, \mathbf{Z})$, which has a finite index nonabelian free subgroup, and so its pro-p completion is not p-adic analytic and thus not boundedly generated.

We now consider the case $g > 2$. An old theorem of Dehn states that, for all $g \geq 1$, the group $\mathrm{Mod}(\Sigma_g)$ is isomorphic to $\mathrm{Out}^+(\pi_g)$, where π_g is the fundamental group of Σ_g, $\mathrm{Out}(\pi_g)$ is the group of outer automorphisms of π_g, and $\mathrm{Out}^+(\pi_g)$ is a subgroup of index two in $\mathrm{Out}(\pi_g)$

The natural action of $\mathrm{Homeo}(\Sigma_g)$ on $H_1(\Sigma_g, \mathbf{Z})$ clearly descends to an action of $\mathrm{Mod}(\Sigma_g)$. This action preserves the pairing on $H_1(\Sigma_g, \mathbf{Z}) = \mathbf{Z}^{2g}$ given by intersection number, so leaves the standard symplectic form on $H_1(\Sigma_g, \mathbf{Z})$ invariant, giving the well-known exact sequence:

$$1 \to T(g) \to \mathrm{Mod}(\Sigma_g) \to \mathrm{Sp}(2g, \mathbf{Z}) \to 1$$

The kernel $T(g)$ is called the *Torelli group* of genus g. The group $T(g)$ has the following properties:

1. It is finitely generated when $g \geq 3$ (see [J]).

2. It is residually torsion-free nilpotent for $g \geq 2$ (see [BL]).

3. It is not nilpotent. While this seems to be well-known, and is for example implicit in [Hai], here is a short argument which actually proves the stronger result that $T(g)$ contains a nonabelian free group:

   Consider essential, separating, simple closed curves α, β in Σ_g with $i(\alpha, \beta) = 2$. Then α and β fill out a 4-holed sphere, and the Dehn twists T_α and T_β lie in the subgroup corresponding to the mapping class group of this subsurface (preserving the holes). We claim that they generate a free group.

   To see this, note that the torus covers the sphere with 4 branch points, and the Dehn twists on α and β in the sphere lift to squares of Dehn twists on the torus. That is, they correspond to the matrices

   $$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \quad \text{in } \mathrm{PSL}(2, Z)$$

   These generate a free group, as one can easily see by looking at an appropriate fundamental domain in $\mathbf{H}^2$ and applying the standard Schottky argument.

Applying Corollary 3.4 to the exact sequence above now gives the conclusion of Theorem 1.4 for $g \geq 3$.

For $g = 2$ the above proof breaks down since the Torelli group $T(2)$ is not finitely generated. In fact it was shown by Mess [Me] that $T(2)$ is an infinitely generated free group. We can still modify the arguments above to cover the case $g = 2$ as well. We sketch here a proof of how to do this.

For each prime p, let π_p denote the composition

$$\mathrm{Mod}(\Sigma_g) \to \mathrm{Sp}(2g, \mathbf{Z}) \to \mathrm{Sp}(2g, \mathbf{Z}/p\mathbf{Z})$$

and let $L = \ker(\pi_p)$. Consider $L_{\hat{p}}$. Let $\overline{N}$ be the closure of the Torelli group in $L_{\hat{p}}$. If $\overline{N}$ is not finitely generated we are done, i.e. $L_{\hat{p}}$ cannot be p-adic analytic since every closed subgroup of an analytic group is finitely generated. So suppose that $\overline{N}$ is finitely generated. We will show that $\overline{N}$ has quotients of arbitrarily large dimension, so that $\overline{N}$ (hence $L_{\hat{p}}$) is not p-adic analytic.

To this end, consider the image of $\overline{N}$ in $\mathrm{Out}((\Gamma_1/\Gamma_i)_{\hat{p}})$, where Γ_i is defined inductively as follows: $\Gamma_1 = \pi_1(\Sigma_g)$ and $\Gamma_{i+1} = [\Gamma_1, \Gamma_i]$ for $i > 1$. Consider the pro-p completion $(\Gamma_1/\Gamma_i)_{\hat{p}}$. As Γ_i is characteristic in Γ_1, there is a homomorphism

$$\mathrm{Out}(\Gamma_1) \to \mathrm{Out}(\Gamma_1/\Gamma_i) \to \mathrm{Out}((\Gamma_1/\Gamma_i)_{\hat{p}})$$

which induces a homomorphism ψ from L to a pro-p subgroup of $\mathrm{Out}((\Gamma_1/\Gamma_i)_{\hat{p}})$. As the image of ψ is contained in a pro-p group, we have that ψ can be extended to $L_{\hat{p}}$. One can then check, á la the analysis in Andreadakis [An], that the image of $\overline{N}$ in $\mathrm{Out}((\Gamma_1/\Gamma_i)_{\hat{p}})$ is a nilpotent analytic group whose dimension is growing to infinity with i (since N is not nilpotent). This proves that $\overline{N}$ is not finite dimensional, i.e. is not analytic.

$\diamond$

3.4 Automorphism groups of free groups

Let $\mathrm{Aut}(F_n)$ (resp. $\mathrm{Out}(F_n)$) denote the automorphism group (resp. outer automorphism group) of the free group F_n of rank n. The same technique as was used to prove Theorem 1.4 and Theorem 1.3 applies to $\mathrm{Aut}(F_n)$ and $\mathrm{Out}(F_n)$.

Theorem 3.5 *For every $n \geq 2$ and every prime p, the group Aut(F_n) has a finite index subgroup L whose pro-p completion $L_{\hat{p}}$ is not p-adic analytic; similarly for Out(F_n). In particular neither Aut(F_n) nor Out(F_n) is boundedly generated.*

Remark. The latter result for $\mathrm{Aut}(F_n)$ was proved by Sury [Su].

Proof. We describe the proof for $\mathrm{Out}(F_n)$. For $n \geq 3$ the proof is exactly the same as the case $\mathrm{Mod}(\Sigma_g) = \mathrm{Out}(\pi_1(\Sigma_g))$. The corresponding Torelli subgroup

$$T = \ker(\mathrm{Out}(F_n) \to \mathrm{SL}(n, \mathbf{Z}))$$

is indeed finitely generated and residually torsion-free nilpotent (see [BL] and the references therein). Further, T is not nilpotent. One can do this explicitly (as in the case for the Torelli subgroup of $\mathrm{Mod}(\Sigma_g)$ above), or for $n \geq 4$ as follows: if T were nilpotent then one could deduce from [Lu2] (which holds for $n \geq 4$) that $\mathrm{Out}(F_n)$ is linear, which contradicts [FP]. Applying Corollary 3.4 now finishes the proof.

For $n = 2$, the group $\mathrm{Out}(F_n)$ is isomorphic to $\mathrm{GL}(2, \mathbf{Z})$, which has a nonabelian free subgroup of finite index, hence its pro-p completion is not analytic. In particular it is not boundedly generated. $\diamond$

3.5 Word-hyperbolic groups are not boundedly generated

We would like to record the following.

Proposition 3.6 *A non-elementary word-hyperbolic group is not boundedly generated.*

Proof. Gromov has shown that every non-elementary word-hyperbolic group G has an infinite torsion quotient H. If G were boundedly generated then so would H be. But it is clear that a boundedly generated torsion group must be finite. $\diamond$

4 Low-dimensional representations of $\mathbf{Mod}(\Sigma_g)$

In this section we prove Theorem 1.6.

Let $\mathcal{C} = \{C_1, \ldots, C_{2g}\}$ be a collection of essential, homotopically distinct, simple closed curves such that $i(C_i, C_{g+i}) = i(C_{g+i}, C_i) = 1$ for each $1 \leq i \leq g$ and $i(C_i, C_j) = 0$ otherwise.

For any simple closed curve α, let T_α denote the Dehn twist about α. Then $i(\alpha, \beta) = 0$ if and only if T_α commutes with T_β. In fact (see, e.g. [Iv2], Theorem 7.5C), powers $T_\alpha^m, T_\beta^n, m, n \in \mathbf{Z}^+$ commute if and only if $i(\alpha, \beta) = 0$

Now let any finite index subgroup H of $\mathrm{Mod}(\Sigma_g)$ be given. As H has finite index, there exists $l > 0$ so that $Y_{C_i}^l \in H$ for all $1 \leq i \leq 2g$.

For any subset $S \subset \mathcal{C}$ we denote by T_S^l the subgroup of $\mathrm{Mod}(\Sigma_g)$ generated by $\{T_C^l : C \in S\}$. Let

$$\mathcal{S} = \{S \subset \mathcal{C} : T_S^l < H \text{ is abelian}\} = \{S \subset \mathcal{C} : \text{if } \alpha, \beta \in S \text{ then } i(\alpha, \beta) = 0\}$$

Now let
$$N = \max_{S \in \mathcal{S}} \dim(\overline{\psi(T_S^l)})$$

where $\overline{H}$ denotes the Zariski closure of the subgroup H in $\mathrm{GL}(n, \mathbf{C})$ and dim denotes the dimension of an algebraic group. Let $B = \{C_{i_1}, \ldots, C_{i_r}\}$ be an element of $\mathcal{S}$ which both realizes this maximum and such that r is minimal over all elements of $\mathcal{S}$ realizing this maximum.

We claim that $r \leq N$. As $\overline{\psi(T_B^l)}$ is abelian, it is enough to show that, for an abelian algebraic group $A = \overline{< a_1, \ldots, a_r >}$ where the set $\{a_i\}$ is minimal as above, that $r \leq \dim(A)$. To see this, one proceeds by induction on r, the case $r = 1$ being clear. By the minimality assumption, $A_2 = \overline{< a_1, \ldots, a_{r-1} >}$ has dimension at most $N-1$, for otherwise we could throw away a_r. As the product of algebraic groups is algebraic (see, e.g. [Sp], p.31), the Zariski closure of a product is the product of Zariski closures. Hence $\{a_1, \ldots, a_{r-1}\}$ is minimal for A_2, so by induction $r - 1 \leq N - 1$. Hence $r \leq N$.

Since in an algebraic group the centralizer of a single element is clearly algebraic, and the intersection of algebraic groups is algebraic, we see that the Zariski closure of a finitely-generated abelian group is also abelian. In particular $\overline{\psi(T_B^l)}$ is an abelian algebraic subgroup of $\mathrm{GL}(n, \mathbf{C})$. By an old result of Schur [Sc] any such subgroup of $\mathrm{SL}(n, \mathbf{C})$ has dimension at most $\lfloor n^2/4 \rfloor \leq n^2/4$. But any maximal abelian subgroup of $\mathrm{GL}(n, \mathbf{C})$ is of the form ZA, where A is such a subgroup on $\mathrm{SL}(n, \mathbf{C})$ and Z denotes the center of $\mathrm{GL}(n, C)$. Hence any abelian algebraic subgroup of $\mathrm{GL}(n, \mathbf{C})$, in particular $\overline{\psi(T_B^l)}$, has dimension at most $n^2/4 + 1$.

We now clearly have

$$r \leq N \leq n^2/4 + 1$$

so the hypothesis $n < 2\sqrt{g-1}$ gives

$$g > n^2/4 + 1 \geq r$$

Hence there are curves $\alpha_1, \alpha_2 \in \mathcal{C}$ so that :

(a) $i(\alpha_i, \gamma) = 0$ for $i = 1, 2$ and for each $\gamma \in B$.

(b) $i(\alpha_1, \alpha_2) = 1$.

Recall that powers $T_\alpha^m, T_\beta^n, m, n \in \mathbf{Z}^+$ commute if and only if $i(\alpha, \beta) = 0$. By (a), each T_{α_i} commutes with T_B^l. By the maximality property of B, for $i = 1, 2$ the abelian algebraic group $\overline{\psi(T_B^l \cup T_{\alpha_i})}$ has dimension N, and so must contain $\overline{\psi(T_B^l)}$ as a finite-index subgroup. In particular there exist positive integers m_1, m_2 so that

$$\psi(T_{\alpha_i})^{m_i} \in \overline{\psi(T_B^l)} \text{ for } i = 1, 2$$

Hence $\psi(T_{\alpha_1}^{m_1})$ and $\psi(T_{\alpha_2}^{m_2})$ commute. But by (b) we have that no power of T_{α_1} commutes with any power of T_{α_2}. Hence it must be that ψ is not faithful. $\diamond$

References

[An] S. Andreadakis, On the automorphisms of free groups and free nilpotent groups, *Proc. London Math. Soc.* (3) 15, 1965, 239–268.

[Bi] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies, No. 82, Princeton Univ. Press, 1975.

[BL] H. Bass and A. Lubotzky, Linear-central filtrations on groups, *Contemporary Math.*, Vol. 169 (1994), p. 45-98.

[CV] M. Culler and K. Vogtmann, A group-theoretic criterion for property FA, *Proc. Amer. Math. Soc.* 124 (1996), no. 3, p.677-683.

[DDMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, *Analytic Pro-p Groups*, LMS Lecture Notes 157, Cambridge Univ. Press, 1991.

[FLP] A. Fathi, F. Laudenbach, and V. Poenaru, *Travaux de Thurston sur les surfaces*, vol. 66-67, Asterisque, 1979.

[FP] E. Formanek and C. Procesi, The automorphism group of a free group is not linear, *J. Algebra* 149 (1992), no. 2, 494-499.

[GS] S. M. Gersten and H. B. Short, *Rational subgroups of biautomatic groups.*, Ann. of Math. **134** (1991), 125–158.

[Hai] R. Hain, Infinitesimal presentations of the Torelli groups, *J. Amer. Math. Soc.* 10 (1997), no. 3, 597-651.

[Ha] J. Harer, The second homology group of the mapping class group of an orientable surface, *Invent. Math.*, Vol.72 (1983), p.221-239.

[Iv1] N. Ivanov, Ten problems on the mapping class group, preprint, available at http://www.math.msu.edu/ ivanov.

[Iv2] N. Ivanov, Mapping class groups, preprint, available at http://www.math.msu.edu/ ivanov.

[Iv3] N. Ivanov, Subgroups of Teichmuller Modular Groups, AMS Translations of Mathematical Monographs, Vol. 115, 1992

[J] D. Johnson, The structure of the Torelli group, I. A finite set of generators for $\mathcal{I}$, *Ann. of Math.* (2) 118 (1983), no. 3, 423-442.

[LMR1] A. Lubotzky, S. Mozes, and M. S. Raghunathan, *Cyclic subgroups of exponential growth and metrics on discrete groups*, C. R. Acad. Sci. Paris t. 317, Série I. (1993), 735–770.

[LMR2] A. Lubotzky, S. Mozes, and M. S. Raghunathan, The word and Riemannian metrics on lattices of semisimple groups, *Publ. Math. IHES*, to appear.

[Lu] A. Lubotzky, Subgroup growth and congruence subgroups, *Inventiones Math.*, Vol.119 (1995), p.267-295.

[Lu2] A. Lubotzky, A group-theoretic characterization of linear groups, *J. Algebra* 113 (1988), no. 1, 207–214.

[Me] G. Mess,The Torelli groups for genus 2 and 3 surfaces, *Topology* 31 (1992), no. 4, 775-790.

[MM] A. Marden and H. A. Masur, *A foliation of Teichmüller space by twist invariant disks*, Math. Scand. **36** (1975), 211–228.

[Mo] L. Mosher, *Mapping class groups are automatic*, Ann. of Math. **142** (1995), 303–384.

[Po] J. Powell, Two theorems on the mapping class group of a surface, *Proc. AMS*, Vol.68, No.3 (1978), p.347-350.

[PR] V. Platanov and A. Rapinchuck, Abstract properties of S-arithmetic subgroups and the congruence subgroup problem, *Izvestiya Ross. Acad. Sci. Ser. Math.* 56 (1992), 483-508.

[Sc] I. Schur, Zur Theorie der vertauschbaren Matrizen, *J. Reine Angew. Math.*, No. 130, p.66-76 (1905).

[Sp] T.A. Springer, *Linear Algebraic Groups*, Progress in Math., Vol. 9, Birkhäuser, 1981.

[Su] B. Sury, Bounded generation does not imply finite presentation, *Comm. Algebra* 25 (1997), no. 5, 1673–1683.

[Ta] O. Tavgen, Bounded generation of Chevalley groups over rings of algebraic S-integers, *Math USSR Izvestiya* 36 (1991), p.101-128.

Benson Farb:
Dept. of Mathematics, University of Chicago
5734 University Ave.
Chicago, Il 60637
E-mail: farb@math.uchicago.edu

Alex Lubotzky:
Department of Mathematics
Hebrew University
Jerusalem, Israel
E-mail: alexlub@math.huji.ac.il

Yair Minsky:
Department of Mathematics
SUNY Stony Brook
Stony Brook, NY 11794
E-mail: yair@math.suysb.edu