Thin groups and superstrong approximation
MSRI Publications
Volume **61**, 2013

Generic phenomena in groups: some answers and many questions

IGOR RIVIN

To the memory of Bill Thurston, with gratitude

We give a survey of some known results and of the many open questions in the study of generic phenomena in geometrically interesting groups.

1. Introduction

In this paper we will discuss a number of loosely related questions, which emanate from Thurston's geometrization program for three-dimensional manifolds, and the general Thurston "yoga" that most everything is hyperbolic. We venture quite far afield from three-dimensional geometry and topology — to the geometry of higher-rank symmetric spaces, to number theory, and probability theory, and to the theory of finite groups. In Section 2 we describe the underpinnings from the theory of three-dimensional manifolds as envisaged by W. Thurston. In Section 3 we will describe one natural approach to describing randomness in groups. In Section 5 we describe an approach to actually producing random matrices in lattices in semisimple Lie groups using the philosophy in Section 3. In Section 6 we describe a different approach to randomness, and the questions it raises.

MSC2010: primary 20G25, 20H25, 20P05, 05C81, 20G30, 20F28, 57M50, 20E05, 60F05; secondary 60B15, 60G50, 57M07, 37E30, 20H10, 37A50, 15A36, 11F06.

Keywords: groups, lattices, mapping class group, modular group, random matrix products, three-dimensional manifolds, surfaces, genericity, Zariski-density.

2. Thurston geometry

In so far as this paper is concerned, history begins with Bill Thurston's geometrization program of three-dimensional manifolds. We will begin with the fibered version. The setup is as follows: we have a surface M (a two-dimensional manifold, homeomorphic to a compact surface with a finite number of punctures) and a homeomorphism $\phi : M \to M$. Given this information we construct the *mapping torus* $T_\phi(M)$ of ϕ, by first constructing the product $\Pi = M \times [0, 1]$, and then defining $T_\phi(M)$ to be the quotient space of Π by the equivalence relation which is trivial outside $M \times \{0, 1\}$, where $(x, 0) \sim (\phi(x), 1)$.

One of Thurston's early achievements was the complete understanding of geometric structures on such fibered manifolds. To state the next results we will need to give a very short introduction to the *mapping class group* $\mathrm{Mod}(M)$, which is the group of homeomorphisms of our surface modulo the normal subgroup of homeomorphisms isotopic to the identity — for a longer introduction, see the recently published (but already standard) reference [Farb and Margalit 2011].

In low genus, the mapping class group is easy to understand. For $M \simeq \mathbb{S}^2$, $|\mathrm{Mod}(M)| = 2$; every automorphism of the sphere is isotopic to either the identity map or the antipodal map.

The next easiest case is that of the torus: $M \simeq \mathbb{T}^2$. Then, $\mathrm{Mod}(M) \simeq \mathrm{GL}(2, \mathbb{Z})$. Looking at this case in more detail, we note that the elements of $\mathrm{GL}(2, \mathbb{Z})$ fall into three classes: elliptic (those with a fixed point in the upper halfplane), parabolic (those with a single fixed point p/q on the real axis in $\mathbb{C}$) and the rest (these are hyperbolic, and have two quadratic irrational fixed points on the real axis). Elliptic elements are *periodic*. Parabolic elements leave the (p, q) curve on the torus invariant (they correspond to a *Dehn twist* about this curve). Hyperbolic elements leave no curve invariant. Further, one of their fixed points is attracting, while the other one is repelling. These two fixed points correspond to two orthogonal curves of *irrational slope* on the torus.

In the case where M is the torus with one puncture, Nielsen had proved that $\mathrm{Mod}(M)$ is the same as for $M \simeq \mathbb{T}^2$. After that, things were rather mysterious, until Thurston discovered his classification of surface homeomorphisms, which parallels closely the toral characterization. Thurston's result is that every surface homeomorphism falls into three classes: it is either periodic, or leaves invariant a *multicurve* γ (a collection of simple closed curves on M) — in this case the map is allowed to permute the components of γ, or *pseudo-Anosov*, in which case the map has a pair of orthogonal measured foliations, one of which is expanded by ϕ and the other is contracted. This is a highly nontrivial result which is the beginning of the modern two-dimensional geometry, topology, and dynamics. For a discussion in considerably more depth, see the standard references [Thurston 1988; Poénaru et al. 1979; Casson and Bleiler 1988; Farb and Margalit 2011].

The next theorem ties the above discussion into Thurston's geometrization program for 3-dimensional manifolds (the special case of fibered manifolds was probably the first case of geometrization finished — see J. P. Otal's excellent exposition [2001].) For an in-depth discussion of the various geometries of three-dimensional manifolds, see [Scott 1983].

Theorem 2.1 (Thurston's geometrization theorem for fibered manifolds). *Let $T_\phi(M)$ be as above. We have the following possibilities for the geometry of M.*

(1) *If $M \simeq \mathbb{S}^2$, then $T_\phi(M)$ is modeled on $\mathbb{S}^2 \times \mathbb{R}$.*

(2) *If $M \simeq \mathbb{T}^2$, we have the following possibilities*:
   (a) *If ϕ is elliptic, $T_\phi(M)$ is modeled on $\mathbb{E}^3$.*
   (b) *If ϕ is parabolic, $T_\phi(M)$ is a nil-manifold.*
   (c) *If ϕ is hyperbolic, $T_\phi(M)$ is a solv-manifold.*

(3) *If M is a hyperbolic surface, then*:
   (a) *If ϕ is periodic, $T_\phi(M)$ is modeled on $\mathbb{H}^2 \times \mathbb{R}$.*
   (b) *If ϕ is reducible, $T_\phi(M)$ is a graph manifold.*
   (c) *If ϕ is pseudo-Anosov, $T_\phi(M)$ is hyperbolic.*

An attentive reader will note there are seven special cases, and six out of the eight three-manifold geometries make an appearance. Six out of the seven special cases of the theorem are easy, while the proof of the last case (c) occupies most of the book [Otal 2001]. Thurston's philosophy, moreover, is that "most" fibered (or otherwise) three-manifolds are hyperbolic — the first appearance of this phenomenon in Thurston's work is probably the Dehn surgery theorem [Thurston and Milnor 1979], which states that most Dehn fillings on a cusped hyperbolic manifold yield hyperbolic manifolds, and the last appears in [Dunfield and Thurston 2003; 2006], where it is conjectured that a random three manifold of fixed Heegard genus is hyperbolic. The actual statement that a random *fibered* manifold is hyperbolic seems to have not been published by Thurston, and the honor of first publication of an equivalent question goes to Benson Farb [2006]. We will discuss Farb's precise question below, but first, let's talk about what it means for some property P to be generic for some (possibly) infinite (but countable) set S.

3. An idealist approach to randomness

First, define a measure of size v on the elements of S. This should satisfy some simple axioms:

(1) $v(x) \geq 0$ for all $x \in S$.

(2) The set $S_k = \{x \in S \,|\, v(x) \leq k\}$ is finite for every k.

Now let P be a predicate on the elements of S — think of a predicate as just a function from S to $\{0, 1\}$. Let $\mathcal{P} \subset S$ be defined as $\mathcal{P} = \{x \in S \,|\, P(x) = 1\}$, and define $P_k = \{x \in \mathcal{P} \,|\, v(x) \leq k\}$. We say that the property P is *generic* for S with respect to the valuation v if

$$\lim_{k\to\infty} \frac{|P_k|}{|S_k|} = 1. \tag{1}$$

We say that P is *negligible* with respect to v if

$$\lim_{k\to\infty} \frac{|P_k|}{|S_k|} = 0. \tag{2}$$

Sometimes the above two definitions are not enough, and we say that P has asymptotic density p with respect to v if

$$\lim_{k\to\infty} \frac{|P_k|}{|S_k|} = p. \tag{3}$$

These definitions work well when they work. Here are some examples:

Example 3.1. The set S is the set $\mathbb{N}$ of natural numbers, and the predicate P is $P(x) =$ "x is prime". The valuation v is just the usual archimedean valuation on $\mathbb{N}$, and, as is well known, the set of primes is *negligible*. One can make a more precise statement (which is the content of the prime number theorem; see [Davenport 2000; Newman 1980]).

With definitions as above,

$$\frac{P_k}{S_k} = \Theta\left(\frac{1}{\log k}\right).$$

Example 3.2. Let S be the set of integer lattice points $(x, y) \in \mathbb{Z}^2$, let $\Omega \subset \mathbb{R}^2$ be a Jordan domain, and define the valuation on S as follows:

$$v(x) = \inf\{t \mid x \in t\Omega\}.$$

Further, define the predicate P by $P(x, y) =$ "x is relatively prime to y"; such points are called *visible*, since one can see them from the origin $(0, 0)$. Then, the asymptotic density of P is $1/\zeta(2) = 6/\pi^2$.

The proof of this for Ω being the unit square is classical, and can be found (for example) in [Hardy and Wright 2008] or in the less classical reference [Rivin 2001]. To get the general statement, we first note that the special linear group $\mathrm{SL}(2, \mathbb{Z})$ acts ergodically on the plane $\mathbb{R}^2$ (see [Zimmer 1984]). Now, define a measure μ_t by

$$\mu_t(\Omega) = \frac{1}{t^2} \text{ (the number of points such that } P(x, y) = 1 \text{ in } t\Omega.)$$

Each μ_t is clearly a measure, dominated by the Lebesgue measure, and invariant under the $\mathrm{SL}(2,\mathbb{Z})$ action on $\mathbb{R}^2$. By Helly's theorem [Lax 2002, Section 10.3] It follows that the set $\{mu_t\}$ has a convergent subsequence σ, and by $\mathrm{SL}(2,\mathbb{Z})$ invariance, the limit μ_σ is a constant multiple of the Lebesgue measure, and the constant can be evaluated for some specific Ω, such as the square (more details of the argument can be found in [Kapovich et al. 2007]). Notice that the constant does not depend on σ, so all the convergent subsequences of the set $\{\mu_t\}$ have the same limit, which must, therefore, be the unique limit point of the set.

Example 3.3. Consider the free group on two generators $F_2 = \langle a, b\rangle$. We define the valuation $v(x)$ to be the reduced word length of x. Define the predicate $P(x) =$ "the abelianization $a(x) \in \mathbb{Z}^2$ is a visible point". Then P does *not* have an asymptotic density (see [Kapovich et al. 2007] for a discussion). It does, however, have a an asymptotic *annular* density, defined as follows: Let $X \subset S$, where S, as usual, has a valuation satisfying our axioms. We define $S_k = \{x \in S \mid v(x) = k\}$, and similarly for X_k. Then, the k-th annular density of T is defined by

$$\rho_k(X) = \frac{1}{2}\left(\frac{X_{k-1}}{S_{k-1}} + \frac{X_k}{S_k}\right). \tag{4}$$

We define the *strict annular density* of X to be $\rho_A(X) = \lim_{k\to\infty} \rho_k(X)$, if the limit exists. The general result is this:

Theorem 3.4 [Kapovich et al. 2007]. *Let S be an $\mathrm{SL}(n,\mathbb{Z})$ invariant subset of $\mathbb{Z}^k$, and let $\tilde{S} = a^{-1}S$, where a, as before, is the abelianization map from the free group on k generators F_k to $\mathbb{Z}^k$. Then $\tilde{S}$ has a strict annular density whenever S has an asymptotic density. Moreover, the two densities are equal.*

The proof of Theorem 3.4 uses the ergodicity of the $\mathrm{SL}(n,\mathbb{Z})$ action on $\mathbb{R}^n$, as described in Example 3.2, and the central and local limit theorems of [Rivin 1999] (see also [Rivin 2010a; Sharp 2001]).

The examples above show that the cases where the groups are reasonably simple to describe, the idealistic valuation-based approach is quite successful. However, once the groups are more complicated, this approach often bogs down in at least some ways, the principal of which is that when one talks of negligibility, genericity, or density, one is making a statement about properties of *random* elements of the set S. However, this raises the question of how to generate such random elements (note that the generation method will often hold the keys to our ability to approach asymptotic statements.)

Example 3.5. Let $S = \mathrm{SL}(n,\mathbb{Z})$. There is a natural family of valuations on S — the archimedean valuations associated to the various Banach space norms on the space of $n \times n$ matrices $M^{n\times n}$. Since all these are known to be equivalent, we

might as well choose the Frobenius norm (the L^2 norm of a matrix $x \in \mathrm{SL}(n, \mathbb{Z})$ viewed as a vector in $\mathbb{Z}^{n\times n}$.). In other words, in our previous language,

$$v(x) = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2}.$$

Let $S_{\leq k}$ be the set of those x in S with $v(x) \leq k$. It is not at all obvious how to find the cardinality of $S_{\leq k}$, though this has been done (relatively recently) for $\mathrm{SL}(2, \mathbb{Z})$ (by Morris Newman [1988][1] and in general by W. Duke, Z. Rudnick, and P. Sarnak [1993], and by A. Eskin and C. McMullen [1993]. The result is that the number of points is asymptotic to a constant times k^{n^2-n} – the constant for $n = 2$ is 6. In any case, enumeration in and of itself is difficult, and enumerating subsets seems more difficult still. An example of this is the (simple to state) question of finding a *uniformly distributed random element* of bounded norm (see Section 5 for more).

Nevertheless, one can try to show some results on linear groups using the archimedean valuation as above, sometimes using the very deep results of A. Nevo and P. Sarnak [2010], which are a major advance on the results of [Duke et al. 1993].

Example 3.6 Rivin 2008; 2009. A generic element of $\mathrm{SL}(n, \mathbb{Z})$ has irreducible characteristic polynomial; furthermore, the Galois group of the characteristic polynomial is generically the full symmetric group. The generic element of $\mathrm{Sp}(n, \mathbb{Z})$ has irreducible characteristic polynomial.

Example 3.7. Let G be a lattice in a semisimple linear group $\mathfrak{G}$, pick a (non-central) element $h \in G$ and for an element $x \in G$ consider the group $H_x = \langle x, h\rangle$. Consider the predicate $P(x) =$ "H_x is Zariski-dense in $\mathfrak{G}$". In [Rivin 2010b] I showed that P is generic in G. Similarly, if $H = G \times G$, the property $P(x, y) =$ "H_x is Zariski-dense in $\mathfrak{G}$" is generic in $G \times G$. The results are based on strong approximation theory, as developed in [Matthews et al. 1984]; see also [Platonov and Rapinchuk 1994].

Question 3.8. How do we tell if a subgroup G of (say) $\mathrm{SL}(n, \mathbb{Z})$ given by its matrix generators is Zariski-dense?

There are two avenues by which to attack Question 3.8. The first is via strong approximation techniques: by [Matthews et al. 1984], almost all modular projections are surjective for any Zariski-dense subgroup G, and further, by [Weigel 1996], the group is Zariski-dense if *any* projection modulo some $p > 3$ is surjective. So, we need only check a finite number of possible bad projections,

[1] P. Sarnak remarks that this result follows immediately from Delsarte's solution of the circle problem in hyperbolic case, but Newman's argument is completely different.

which *is* bounded by [Rapinchuk 2012], but the bound is not what one would call practical, so this approach, while aesthetically pleasing, takes a lot of work to make work.

A completely different approach is the brute force attack: take the group, compute several elements, compute their (matrix) logarithm, and see if the resulting elements generate the Lie algebra of $\mathrm{SL}(n, \mathbb{C})$ as a vector space. This is a much more computationally promising approach, but it requires a lot of work to produce provable results (the logarithm can usually be computed only approximately, so one needs to find the measure of one's confidence in one's results, etc). The method is particularly effective when there are a lot of unipotent elements in the subgroup, since the logarithm of a unipotent integral matrix is a matrix with *rational* entries, so no approximation techniques are necessary (this was pointed out to me by A. Eskin, who, in turn, credits Forni, Matheus, and Zorich).

Added in proof. Since the first version of this paper was written, the author has discovered a third method (much superior to the other two), based on the following observation: if a subgroup of $\mathrm{SL}(n, \mathbb{Z})$ contains two noncommuting matrices of infinite order such that the Galois group of at least one of them is the full symmetric group, then the subgroup is Zariski-dense. Since, as shown in [Rivin 2008; 2009; 2010b], the probability that a random word of length N of a Zariski dense subgroup does *not* have the full Galois group has probability decreasing exponentially in N, and since testing for Galois group equaling S_n is both theoretically and practically fast, this is an excellent practical and theoretical method. The validity of this method is shown, and the result is extended to other algebraic groups, in [Prasad and Rapinchuk 2014, Theorem 9.10], and the general algorithmic aspects are discussed in an upcoming paper of the author.

Example 3.9 [Fuchs and Rivin $\geq$ 2012]. If G is a lattice in $\mathrm{SL}(2, \mathbb{C})$, and $H = G \times G$, then, for any $\alpha > 0$, the property

$$P(x, y) = \text{“the Hausdorff dimension of } \langle x, y \rangle \text{ is at least } \alpha\text{”}$$

is negligible in H.

The argument uses the ergodicity of the action of $\mathrm{SL}(2, \mathbb{Z})$ on the plane (which shows that the attractive and repelling fixed points of elements are equidistributed), and a ping-pong argument, together with bounds on the Hausdorff dimension as in [McMullen 1998].

One can also show (using an idea of Sarnak) that the same result holds in the parabolic setting:

Theorem 3.10. *Consider a pair of elements* one of which is parabolic. *The property*

$$P(x, y) = \text{“The Hausdorff dimension of the limit set of } \langle x, y\rangle \text{ is at least } \alpha\text{”}$$

is negligible for any $\alpha > \frac{1}{2}$.

It is a theorem of Beardon [1968] that any such group *does* have Hausdorff dimension at least $\frac{1}{2}$, so the constant $\frac{1}{2}$ in Theorem 3.10 is best possible.

It is hoped that the techniques used to attack Example 3.9 can be extended to attack Theorem 3.10.

Example 3.11 [Capdeboscq and Rivin $\geq$ 2012]. If G is a lattice in a semisimple Lie group $\mathfrak{G}$ of rank at least two, and $H = G \times G$, and if we define $P(x, y) = \langle x, y\rangle$ is profinitely dense, then $P(x, y)$ has asymptotic density bounded below.

The idea of the argument is as follows (in the case of $\mathrm{SL}(n, \mathbb{Z})$):

The first observation is that $\mathrm{SL}(n, \mathbb{Z}/NM\mathbb{Z}) = \mathrm{SL}(n, \mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}(n, \mathbb{Z}/M\mathbb{Z})$, for N, M relatively prime.

The second observation is that random elements (either in the random walk model or in the “archimedean height” model) are eventually equidistributed in modular projections, e.g modulo the product P of the first k primes (this is one of the results of [Rivin 2008]). By the first observation, the behaviors modulo different primes are independent, and so by [Kantor and Lubotzky 1990; Liebeck and Shalev 1995] the probability that the projections onto the first k primes are surjective is bounded below by

$$B_k = \prod_{i=1}^{k} (1 - C(n)/p^{n-1}),$$

where $C(n)$ is a rank-dependent constant (we are using the congruence subgroup property). Since the series

$$\sum_{i=1}^{\infty} \frac{1}{p^{n-1}}$$

converges for $n > 2$, it follows that the products B_k converge to some constant B.

Now, for any ϵ we can pick k in such a way that $|B_k - B| < \epsilon$, while

$$R_k = \sum_{i=k+1}^{\infty} \frac{C(n)}{p^{n-1}} < \epsilon.$$

By the union bound, the probability that some projection is not surjective is bounded above by $(1 - B_k) + R_k \leq B + 2\epsilon$. So, as long as $\epsilon \ll (1 - B)/2$, we get the probability that at least one projection does not surject is bounded

above by $(1-B)/2$. In reality, of course, if the walks get very very long, the true probability of profinite density is bounded below by B.

The observations above show that the modular projections are surjective for all *prime* moduli with positive probability. Then, using some group-theoretic arguments we can show that there is a positive probability of surjection for all moduli. The estimates on the probabilities are completely effective.

Since the first example of a profinitely dense (free) subgroup of $\mathrm{SL}(n,\mathbb{Z})$ was constructed by Steve Humphries in his beautiful paper [1988], we call the groups described in Example 3.11 *Humphries groups*. Now for the question:

Question 3.12. Suppose we are given a subgroup G of $\mathrm{SL}(n,\mathbb{Z})$ given by matrix generators. How hard it is to decide whether it is a Humphries group?

Question 3.12 is quite difficult. Notice that the full lattice $\mathrm{SL}(n,\mathbb{Z})$ is a Humphries group (by the definition above), so there is a natural dichotomy: Either a Humphries group G is the whole $\mathrm{SL}(n,\mathbb{Z})$ or, by the congruence subgroup property, it is infinite index, and further, by [Lubotzky 1999] (see [Weigel 1996] for a sharper result), G is Zariski-dense in $\mathrm{SL}(n,\mathbb{Z})$. This dichotomy is not really relevant from the algorithmic standpoint — we know from the work of Matthews, Vaserstein and Weisfeiler [Matthews et al. 1984] that for any Zariski-dense subgroup G only a finite number of projections is not surjective, and if we could bound the number, we could just check surjectivity for every possible exceptional modulus — such a check can be performed efficiently using, for example, the algorithm of Neumann and Praeger [1992]. Unfortunately, getting a bound using the generators is not so easy. The first advance came (after the author raised the question at an MSRI Hot Topics conference) very recently, in the work by A. Rapinchuk [2012], but the bounds there, while explicit, are not really computationally useful, as Rapinchuk prominently states in the paper.

On the other hand, the beginning of the discussion in the paragraph above begs the question:

Question 3.13. Given a collection of matrices in $\mathrm{SL}(n,\mathbb{Z})$ do they generate $\mathrm{SL}(n,\mathbb{Z})$?

One attempt is as follows: compute the fundamental domain of the span of the matrices on the homogeneous space of $\mathrm{SL}(n,\mathbb{R})$. If we are lucky, and that domain is finite-volume, we can answer the question (the author has conducted a number of experiments along these lines). No general attack seems to be available, and it is not even clear whether the question is decidable! Similar sounding questions (like the membership problem) are undecidable in $\mathrm{SL}(n,\mathbb{Z})$ for $n \geq 4$, but the techniques which show this seem unapplicable here. In special cases (which are central to the study of mirror symmetry; see [Singh and Venkataramana 2012;

Brav and Thomas 2012]) the question can be decided by a rather diverse set of approaches (arithmeticity is proved using T. N. Venkataramana's theorem that if a Zariski-dense subgroup has "opposing unipotents", then it is a lattice; nonarithmeticity use proved using ping-pong — a presentation is obtained for the group, and then it can be checked that for homological reasons the group cannot be a lattice).

4. Punctured (or not) torus

Consider the modular group $\mathrm{SL}(2,\mathbb{Z})$. Our first set of results will use ordering by Frobenius norm of the matrix.

Definition 4.1. The *Frobenius norm* of the matrix $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is

$$\|x\| = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

The first question is:

Question 4.2. How many elements $x \in \mathrm{SL}(2,\mathbb{Z})$ have $\|x\| \leq N$?

It is surprising that answer to this question was first written down by Morris Newman a quarter-century ago!

Theorem 4.3 [Newman 1988]. *The number $\mathcal{N}_k$ of elements $x \in \mathrm{SL}(2,\mathbb{Z})$ with $\|x\| \leq k$ is asymptotic to $6k^2$.*

Newman's proof begins by reparametrizing $\mathrm{SL}(2,\mathbb{Z})$, as follows. First define the variables

$$A = a + d, \quad B = b + c, \quad C = b - c, \quad D = a - d.$$

We see that $A^2 + B^2 + C^2 + D^2 = 2(a^2 + b^2 + c^2 + d^2)$. Further note that

$$4 = 4(ad - bc) = A^2 + C^2 - B^2 - D^2, \tag{5}$$

while

$$A = \mathrm{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{6}$$

Since the difference between A and D is $2d$, we know that

$$A \equiv D \mod 2, \tag{7}$$

and for the same reason

$$B \equiv C \mod 2. \tag{8}$$

Then Newman writes down a generating function for the number of matrices in $\mathrm{SL}(2,\mathbb{Z})$ with prescribed Frobenius norm in terms of the theta function

$$\theta(x) = \sum_{n=-\infty}^{\infty} x^{n^2}, \tag{9}$$

and uses classical estimates on the coefficients of products of theta functions to obtain the asymptotic result of Theorem 4.3. Since an exposition of this method would take us too far afield, let's use the parametrization above to count those elements with trace equal to 2 (which is to say, the parabolic elements). Equations (5) and (6) tell us that the number of such matrices with Frobenius norm bounded by k is exactly equal to the number of *Pythagorean triples* of norm bounded by k.

Now, as is well known, pythagorean triples (A, B, C) with $A^2 = B^2 + C^2$ are rationally parametrized by

$$A = u^2 + v^2, \quad B = u^2 - v^2, \quad C = 2uv. \tag{10}$$

With this parametrization, the 2-norm of (A, B, C) equals $\sqrt{2}(u^2 + v^2)$, so the number of pythagorean triples with L^2 norm bounded above by X equals the number of pairs (u, v) with L^2 norm bounded above by $2^{1/4}\sqrt{X}$, which, in turn, is asymptotic to $\sqrt{2}\pi X$. Note that the congruences (7) and (8) tell us that $2uv = a - d$. This overcounts by a factor of two (since (u, v) and $(-u, -v)$ give the same Pythagorean triple, but on the other hand, parabolic matrices are allowed to have trace equal to ± 2, so when the smoke clears, we have:

Fact 4.4. *The number of parabolic matrices in* $\mathrm{SL}(2,\mathbb{Z})$ *and Frobenius norm bounded above by* k *is asymptotic to* $\sqrt{2}\pi k$.

Observation 4.5. The characteristic polynomial of a matrix in $\mathrm{SL}(2,\mathbb{Z})$ factors over $\mathbb{Z}$ if and only if the matrix is parabolic (so has trace ± 2.)

Proof. If $M \in \mathrm{SL}(2,\mathbb{Z})$, the roots of the characteristic polynomial $\chi(M)$ are

$$\frac{\operatorname{tr} M \pm \sqrt{\operatorname{tr}^2 M - 4}}{2}. \tag{11}$$

For $\chi(M)$ to factor, $\operatorname{tr}^2 M - 4$ must be a perfect square, which obviously happens only when $|\operatorname{tr} M| = 2$. □

We thus have:

Theorem 4.6. *The probability of a matrix in* $\mathrm{SL}(2,\mathbb{Z})$ *of Frobenius norm at most* x *having* reducible *characteristic polynomial is asymptotic to* $3\sqrt{2}/(\pi x)$.

5. Looking for random integer matrices

Consider a simple question: Let v be an archimedean valuation in a lattice (below we will be discussing $\mathrm{SL}(n,\mathbb{Z})$, but the question is just as interesting for any other lattice in a noncompact Lie Group, not necessarily semisimple).

Question 5.1. Given k, how do we choose a random element x *uniformly* with $v(x) \leq k$?

Even for $\mathrm{SL}(2,\mathbb{Z})$, Question 5.1 seems not to have been studied, but here is an idea.

***A line of attack for* $\mathbf{SL(2,\mathbb{Z})}$.** To get an *approximately* uniform element, based on the fact that the homogeneous space of $\mathrm{SL}(2,\mathbb{R})$ is the hyperbolic plane $\mathbb{H}^2$: Take a basepoint in $\mathbb{H}^2$ (since we will be eventually interested in $\mathrm{SL}(2,\mathbb{Z})$, the Poincaré halfspace model is popular, and there the point $i = \sqrt{-1}$ is a popular choice of basepoint). Now, the matrices in $\mathrm{SL}(2,\mathbb{R})$ with Frobenius norm bounded by N translate i by hyperbolic distance at most some $f(N)$, so pick a disk D of radius $g(N)$ in $\mathbb{H}^2$, and pick a point x uniformly at random. x will lie in some fundamental domain of the $\mathrm{SL}(2,\mathbb{Z})$ action. The point x corresponds to a lattice $L \subset \mathbb{R}^2$, which can be *reduced* (using Legendre's algorithm — basically continued fractions); this corresponds to finding a matrix $m(x)$ in $\mathrm{SL}(2,\mathbb{Z})$ that maps the fundamental domain of x to the "standard" fundamental domain of the modular group $\mathrm{SL}(2,\mathbb{Z})$. The matrix $m(x)$ is our candidate for the uniformly random element of $\mathrm{SL}(2,\mathbb{Z})$ we seek. (That equidistribution on $\mathbb{H}^2$ leads to equidistribution on $\mathrm{SL}(2,\mathbb{R})$ is standard; see [Eskin and McMullen 1993], for example.)

There are two problems with this approach. Firstly, $m(x)$ might not satisfy the norm constraint. If that is the case, we throw it away, and try again — if $g(N)$ is not too big, this process will terminate reasonably quickly. The other problem is that the area in the disk D is only approximately equidistributed amongst fundamental domains (more precisely, the intersection of D with the union of the translates of the basic fundamental domain by matrices satisfying the norm inequality is only approximately equidistributed among these translates). There is a trade-off between the two problems: the larger disk we take, the more uniform the distribution is, but the less likely we are to get a point satisfying the norm inequality, so some care is required in designing this algorithm properly.

***A line of attack for* $\mathbf{SL(n,\mathbb{Z})}$ *and* $\mathbf{Sp(2n,\mathbb{Z})}$.** The method just described can be extended to higher dimensions, for at least the special linear and symplectic groups. The homogeneous space for $\mathrm{SL}(n,\mathbb{Z})$ (symmetric positive definite matrices with determinant 1,) and for $\mathrm{Sp}(2n,\mathbb{Z})$ (the Siegel halfspace) have been known for several decades, and sampling uniformly from the ball in that space is easy, using what Lie theorists call the KAK decomposition, and most other

people call the singular value decomposition. The Haar measure (induced by that on the Lie group) is easy to compute, and a random element in the ball of the homogeneous space is easy to sample.

What is *not* so easy is the lattice reduction step. Lattice reduction is a much studied problem, since the groundbreaking work of Lovasz (as embodied in the LLL algorithm); a good survey is [Nguyen 2011]. (Interestingly, the symplectic version of the problem had not been considered until quite recently; see [Gama et al. 2006]). The problem is that the complexity of *exact* lattice reduction is, at present, exponential (in the dimension n of the lattice). The LLL algorithms, and the various improvements run in polynomial time, but they don't necessarily get us to the canonical fundamental domain. They *do* get us near the canonical fundamental domain, which brings up a fundamental question:

Question 5.2. What are the statistical properties of the currently used lattice reduction algorithms?

In other words, if we run the algorithm we sketched not with a precise lattice reducer, but with an approximate one (like LLL), will the matrices we get be uniformly distributed in the ball in $\mathrm{SL}(n,\mathbb{Z})$ or $\mathrm{Sp}(2n,\mathbb{Z})$?

The basic principle of the method described works for lattices over number field, and not just over $\mathbb{Z}$. In fact, a version of lattice reduction for such is described in [Fieker and Stehlé 2010]. The version over $\mathrm{SL}(2,\mathbb{Z})$ can be easily made to work to generate a random matrix in an *arithmetic* Kleinian group — the continued fraction algorithm analogue is described in [Page 2012]. It would be interesting to analyze the *non*arithmetic case.

6. A nonidealist approach to randomness

A much more tractable, from the computational standpoint, approach to generating random elements of fairly arbitrary (finitely generated) groups is the following:

Take a symmetric generating set $S = \{g_1, \dots, g_k\}$ of our favorite group G (where "symmetric" means that the set is invariant under the map $x \mapsto x^{-1}$), and look at the set W_k words of length k in the elements of S. The statement that the group G is finitely generated means that

$$\bigcup_{k\geq 0} W_k = G.$$

Now, the trick is to use the definitions in Section 3, but apply them not to the group G itself but to the *free monoid* M_S on S, with

$$v(x) = \text{the word length of } x.$$

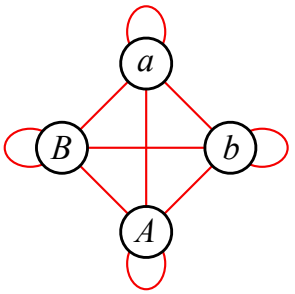

Figure 1. The recognizing automaton for the free monoid on two generators is the (very) complete graph: $bB = aA = 1$.

This approach has many advantages: it is trivial to produce a random element (just multiply elements at random), there are different techniques for proving results, and, in the linear group context this model is closely related to the study of random matrix products, which has a long history and a considerable record of success (a standard reference is [Bougerol and Lacroix 1985]). The (fairly obvious) disadvantage is that the structure of M_S has nothing to do with the structure of G, and it is very difficult to estimate the relationship between the number of occurrences of a given group element in a v-ball of some given radius R. Consequently, doing probability on M_S instead of G is has a certain air of capitulation to it. On the other hand, the free monoid model can be refined, as follows: Elements in the free monoid can be identified with walks in the *complete graph* $\mathcal{K}_k$ on $k = |S|$ vertices (we use the expression in a nonstandard way: every vertex of K_k is connected *to itself* in addition to all the other vertices; see Figure 1.[2])

However, it turns out that this is too broad a context to be able to demonstrate sharp results, and so much of the author's work (see [Rivin 2008, 2009; 2010b] so far has centered on a smaller set of automatic structures: namely, we consider only *undirected* graphs, which, in addition, have the *Perron–Frobenius* property: there is a unique eigenvalue of the adjacency matrix of maximal modulus. This has the immediate benefit of bringing the *free monoid* model closer to reproducing structures of actual interest. For example, Figure 2 shows the graph that generates reduced words (for two generator groups, the general case is similar):

[2]If we remove the requirement that a graph be the (very) complete graph, and, indeed, a directed, as opposed to undirected graph, we find ourselves in the world of *regular languages*, and it was a major discovery of Jim Cannon's, expanded upon by a number of people, including David Epstein and Bill Thurston (see the classic book [Epstein et al. 1992]) that such regular languages are a good way of describing a large class of groups, called *automatic groups*. For such groups, the length of a walk in the defining automaton is a very good valuation — in particular, it coincides with the distance in the Cayley graph from the identity element.

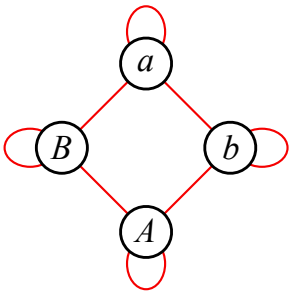

Figure 2. The recognizing automaton for the free group on two generators F_2: $bB = aA = 1$.

This brings up the relatively obvious question:

Question 6.1. Which groups have an automatic structure where the accepting automaton has the properties of being (1) undirected and (2) Perron–Frobenius?

Let's call the combination of properties 1 and 2 *property R*.

Conjecture 6.2. Every word hyperbolic group has property R, with respect to some generating set.

It is not clear that property R is generating-set invariant. While the answer to Question 6.1 is obvious of interest, and the only groups known to have property R are free groups, there is a "cheap" way to extend the techniques to a bigger class of groups, as described in the next section.

What if your group is not free? As a simple example of a nonfree group, we take the *modular group* $\mathcal{M} = \mathrm{SL}(2, \mathbb{Z})$. As is well known, this group is almost, but not quite free. More precisely,

$$\mathcal{M} = \langle S, T \mid S^2, T^3 \rangle = C_2 \star C_2,$$

where C_p is the cyclic group of order p and $\star$ denotes the free product. The obvious symmetric automaton which accepts $C_p \star C_q$ has $p + q - 2$ vertices, corresponding to $T, T^2, \ldots, T^{p-1}, S, \ldots, S^{q-1}$. Every vertex corresponding to T^i is connected to all vertices of the form S^j. This works wonderfully, except for the minor matter of not representing the identity element and the not-so-minor matter of being bipartite, hence not having property R. However, this can seemingly be fixed by making a new graph with $(p-1)(q-1)$ vertices (corresponding to the products $S^i T^j$) and $q - 1$ start states (corresponding to $T, \ldots, q - 1$. I believe that this technique will allow the methods used in [Rivin 2008; 2009; 2010b] to be extended to this class of groups.

7. A nonidealistic approach to SL(2, $\mathbb{Z}$)

Using the automata described in either of the Figures 1 or 2, we can study $\mathrm{SL}(2,\mathbb{Z})$ using the random walk approach described in Section 6. The idea is simple: consider an n-step walk on the recognizing graph G. Since the group $\mathrm{SL}(2,\mathbb{Z})$ is a bit too big for us (it is infinite, for one thing), let's do a quick warm-up, and consider the group $\mathcal{M}_p = \mathrm{SL}(2,\mathbb{Z}/p\mathbb{Z})$. How many elements of $\mathcal{M}_p$ have trace equal to 2? A matrix $M \in \mathcal{M}_p$ has trace 2 if it has the form

$$M = \begin{pmatrix} a & b \\ c & 2-a \end{pmatrix},$$

where $a(2-a) - bc = 1$, which we rewrite as

$$bc + (a-1)^2 = 0. \tag{12}$$

Now, if $a = 1$, Equation (12) has $2p-1$ solutions ($p-1$ solutions with b, but not c equal to 0, $p-1$ solutions with c, but not b, equal to zero, and $(0,0)$.) If $a \neq 1$, (12) has $p-1$ solutions of the form $(b, -(a-1)^2/b)$. This gives a total of $2p-1+(p-1)^2 = p^2$ matrices with trace equal to 2. On the other hand, the order of $\mathcal{M}_p$ is equal to $p(p^2-1)$, so for large p there is a probability of around $1/p$ that M picked uniformly from $\mathcal{M}_p$ picked uniformly at random has trace equal to 2.

What does this have to do with the problem at hand? Note that a matrix which has trace equal to 2 has trace equal to 2 for *every* prime p. This means that if the walks on our graph G are equidistributed in $\mathcal{M}_p$ for some p, the asymptotic probability that an element is parabolic is *at most* $1/p$. The key is this:

Theorem 7.1 [Rivin 2008]. *Let G be a graph with property R, with vertices labeled by generators $\gamma_1, \ldots, \gamma_v$ of a finite group Γ. Then, the walks of length k become equidistributed in Γ, exponentially quickly as a function of k*, unless *all of the γ_i are sent to the same complex number by some nontrivial one-dimensional irreducible representation of Γ.*

Since $\mathcal{M}_p$ has no irreducible one-dimensional representations, we see that the asymptotic probability is smaller than any $1/p$, and hence the asymptotic density is 0. In fact, using the fact that $\mathrm{SL}(2,\mathbb{Z})$, while not enjoying property T, does enjoy property τ for congruence representations (see [Lubotzky 2005]), we can show that the probability of being parabolic decreases *exponentially* in the length of the walk (see [Rivin 2009]).

For specific generating sets, explicit growth rates have been computed in [Takasawa 2001] and [Atalan and Korkmaz 2010]. In the first of these papers, $\mathrm{SL}(2,\mathbb{Z})$ is viewed as the mapping class group of the torus. In the second, the authors study the mapping class group of the four-punctured sphere, but the two

objects are, in fact, the same (though the generating sets are different). This follows from the fact that for any hyperbolic structure on the punctured torus there is the *elliptic involution*, the quotient by which is an orbifold of signature $(0; 2, 2, 2, \infty)$, while each quadruply punctured sphere admits an order four symmetry group (the Klein four-group) of involutions (this can be seen in many ways, one of which being that each complete finite-area structure on the four times punctured sphere can be realized uniquely as the induced metric on an ideal symplex in $\mathbb{H}^3$; see [Rivin 1994]), the quotient by which is the self-same orbifold. The reader wishing an algebraic proof of this fact can consult [Thompson 1995].

Polynomial versus exponential. The attentive and inquisitive reader may have noticed that in Section 4 we showed that for the matrices of norm bounded above by x, there was a probability of order $1/x$ of finding a parabolic, while this probability decreases *exponentially* fast for the graph walk model. The simplest way of explaining this is the following: the number of distinct elements of length k grows exponentially in k (the order of growth depends on the generating set), so the probability of being parabolic is decaying only polynomially in the size of the sample space.

The second simplest explanation (closely related to the first) is that at least in the simplest possible walk model, the expected norm of the products grows exponentially in the length of the walk (this follows from the classical theory of random matrix products; see [Bougerol and Lacroix 1985]).

The case of $\mathrm{SL}(2, \mathbb{Z})$ is particularly interesting (as it always is). A particularly popular generating set for $\mathrm{SL}(2, \mathbb{Z})$ is the set $\{L, U\}$ where $L = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $U = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Any matrix $M\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where we assume that $b > a > 0$, $d > c \geq 0$ (the other cases are similar), can be written as $M = U^{a_0} L^{a_1} \dots U^{a_r}$, where $b/d = [a_0, a_1, \dots, a_r]$. In this case, the word length of M in terms of the generators L, U is simply the sum of the continued fraction coefficients of b/d — the word length with respect to other generating sets is within a multiple (obtained by writing the "new" generators S, T as words in U, L and vice versa). It turns out that the sum of continued fraction coefficients is not so easy to analyze, though not for lack of trying. The first reference seems to be the paper of Andy Yao and Don Knuth [1975], which showed that the *average* value of the sum $S(p/q)$ of the continued fraction coefficients of p/q taken over all $0 < p < q$ satisfies

$$\frac{1}{q} \sum_{0<p<q} S(p, q) \asymp \frac{6}{\pi^2} (\log q)^2.$$

The $(\log q)^2$ growth is a little deceptive, since the distribution has "fat tails". Indeed, I. Vardi [1993] had shown that for any α satisfying $1 > \alpha > \frac{1}{2}$, we have

$$S(p/q) \leq (\log q)^{1+\alpha}, \quad p < q < n,$$

with at most $O_\epsilon(N^2(\log N)^{1/2-\alpha+\epsilon})$ exceptions.

Vardi's paper is mostly concerned with Dedekind sums, which can be interpreted as the *alternating* sum of continued fraction coefficients. The reader is referred to Vardi's very nice preprint [2009] for more on continued fractions and related mathematics.

8. Higher mapping class groups

The techniques which work for the torus at first appear to fail resoundingly for the mapping class group of more complicated surfaces, since the mapping class group in that setting is not linear. Luckily, there is a workaround: The *Torelli homomorphism* $\mathcal{T}$ is a homomorphism from the mapping class group $\mathcal{M}(S)$ of a (closed, for simplicity, and oriented) surface S of genus g to $\mathrm{Sp}(2g, \mathbb{Z})$. A mapping class ϕ is mapped by $\mathcal{T}$ to its action on the first homology group of S. This action preserves the intersection pairing, and so the image of $\mathcal{T}$ is contained in the symplectic group. In addition, the following fact is standard:

Fact 8.1 [Farb and Margalit 2011]. *The image of $\mathcal{T}$ is all of the symplectic group* $\mathrm{Sp}(2g, \mathbb{Z})$.

Except for the cases of the torus and the four-times punctured sphere, the map $\mathcal{T}$ has a nontrivial kernel, known as the *Torelli group* $\mathfrak{T}(S)$ of the surface S. The Torelli group contains pseudo-Anosov elements, so the Torelli homomorphism does lose a lot of information. Nonetheless, we have: .

Theorem 8.2 [Casson and Bleiler 1988]. *Suppose the characteristic polynomial $\chi(M)$ of a matrix $M = \mathcal{T}(\phi)$ has the following properties*:

(1) $\chi(M)$ *is irreducible.*

(2) $\chi(M)$ *is not cyclotomic.*

(3) $\chi(M)$ *is not of the form $f(x^k)$, for some $k > 1$.*

Then ϕ is pseudo-Anosov.

In view of Fact 8.1, the question of showing that a generic element of $\mathcal{M}(S)$ is pseudo-Anosov reduces to showing that a generic (in the sense of Section 6) element of the symplectic group $\mathrm{Sp}(2g, \mathbb{Z})$ satisfies the conditions of Theorem 8.2. This is a done by what is, philosophically (in a sense that was later made precise by E. Kowalski [2008]), a sieving argument. We show that the properties desired by Theorem 8.2 are enjoyed with a probability *independent of the prime p* by

elements of the quotient group $\mathrm{Sp}(2g, \mathbb{Z}/p\mathbb{Z})$. Since, by strong approximation (see [Platonov and Rapinchuk 1994], or, for a more elementary approach, in [Newman 1972]), the reductions modulo different primes are independendent, and the properties described in Theorem 8.2 are assymmetric, in the sense that, for example, in order to conclude that a polynomial is irreducible it is enough to find a *single* prime for which the reduction mod p is irreducible[3], brings us close to the end. The end is achieved thanks to the fundamental equidistribution result Theorem 7.1, together with property T for the groups we are studying for the groups we are interested in to assure exponential convergence [Rivin 2009].

The good news. The argument sketched above (see [Rivin 2008; 2009] for all the details) has many virtues.

Firstly, it is very general — just how general was outlined in [Lubotzky and Meiri 2012a]. In particular, it can be used to show that a generic element in the outer automorphism group of a free group is *irreducible with irreducible powers*, which is the analogue in that setting of being pseudo-Anosov (an element ψ of the automorphism group of a free group is *irreducible* if it does not preserve any splitting of the free group F as a free product $F = G \star H$; it is irreducible with irreducible powers (iwip) if all powers ψ^k are, likewise, irreducible). The importance of iwip automorphisms was first noted in the foundational paper of M. Bestvina and M. Handel [1992]. For automorphisms of free groups there is the analogue of the Torelli homomorphism, which sends an automorphism ψ of a free group F_n to its action on the abelianization $\mathbb{Z}^n$ of F_n. It is easy to show that the Torelli homomorphism $\mathfrak{T}$ is surjective onto the automorphism group of $\mathbb{Z}^n$ — $\mathrm{GL}(n, \mathbb{Z})$, and it is easy to see that an automorphism ψ is irreducible if (of course, *not* only if) the characteristic polynomial of $\mathfrak{T}(\psi)$ is irreducible. Initially, it seems a little frightening to check that ψ is iwip by checking the characteristic polynomials of $(\mathfrak{T}(\psi))^k$ for *every* k for irreducibility, but it turns out (see [Rivin 2008]) that it is enough to check that the Galois group of the characteristic polynomial $\chi(\mathfrak{T}(\psi))$ is the full symmetric group. This can be proved by combining the previous ideas with the idea (going back to van der Waerden) of characterizing Galois groups *via* the factorization patterns of polynomials modulo various primes. This result was later extended in [Jouve et al. 2013] to show that characteristic polynomials of matrices in lattices in semisimple Lie group usually have as big a Galois group as possible (which is to say, the Weyl group of the ambient Lie group).

[3] Note that the argument we used for $\mathrm{SL}(2, \mathbb{Z})$ is much simpler, since there only one (large) prime sufficed, and no strong approximation argument was necessary — it turns out that this kind of argument works for $\mathrm{SL}(n, \mathbb{Z})$ to show that the characteristic polynomial of a generic matrix is irreducible, since it can be shown that the set of irreducible polynomials is a relatively sparse set of subvarieties of the set of coefficients

The results are effective (and explicit) in that they give an exponential rate of convergence of the densities to 0.

The results can be extended without any work to finite index subgroups of $\mathrm{SL}(n,\mathbb{Z})$ and $\mathrm{Sp}(2g,\mathbb{Z})$, and their preimages in the mapping class groups, and, with some work, and much use of the results of [Breuillard et al. 2011], to *thin Zariski-dense subgroups* of such groups, and *their* preimages (these results are still effective, but considerably less explicit than for lattices. It can also be shown, using the results of [Rivin 2010b] that for a *generic* subgroup H of the mapping class group, a generic element of H is pseudo-Anosov.

Bad news. In the context of mapping class groups, our results are not useful for groups which have very small image under the Torelli homomorphism. In particular, the Torelli group itself is completely "orphaned" — Theorem 8.2 is vacuous for elements in the Torelli group. This is all the more galling, since more geometric approaches (see Section 9) show that a generic element of a subgroup of the mapping class group which contains at least two noncommuting pseudo-Anosov elements (below we will call such subgroups *nonelementary*) is pseudo-Anosov. The problem with these approaches is that the convergence rates are completely ineffective, and also they do not apply in the less-geometric situations like the automorphism group of a free group.

Better news. Recently, at least some of the news became less bad, since two groups — A. Lubotzky and C. Meiri [2012b] and J. Malestein and J. Souto [2013] — have extended the results sketched above to the Torelli group, using very similar methods. Lubotzky and Meiri have also extended their results to the Torelli subgroup of the automorphism group of the free group in [Lubotzky and Meiri 2012c]. (The results on the Torelli group make sense only when the genus of the surface in question is at least three — genericity is hard to define for infinitely generated groups).

The first idea of these results goes to the beautiful paper of E. Looijenga [1997], later developed in a more algebraic direction by F. Grunewald and A. Lubotzky [2009]:

Consider a surface S and a double cover $\tilde{S}$. Any homeomorphism the Torelli group lifts to a homeomorphism of $\tilde{S}$. In addition, the image of the lift of the Torelli group under the Torelli homomorphism of $\tilde{S}$ is of finite index in $P\,\mathrm{Sp}(2g-2,\mathbb{Z})$, where $P\,\mathrm{Sp}(\cdot,\mathbb{Z})$ denotes $\mathrm{Sp}(\cdot,\mathbb{Z})/\{\pm I\}$.

This gives us an indication that we might be able to use linear methods to study the Torelli group. The next ingredient goes back to N. V. Ivanov:

Theorem 8.3 [Ivanov 1992]. *Any non-pseudo-Anosov element of the Torelli subgroup of a surface S leaves invariant an essential simple curve γ on S.*

A much stronger result was shown by B. Farb, C. Leininger and D. Margalit:

Theorem 8.4 [Farb et al. 2008, Proposition 1.4]. *Let γ be a curve and f an element in the Torelli subgroup. Then $i(\gamma, f(\gamma)) \geq 4$ if γ is nonseparating, then $i(\gamma, f^j(\gamma)) \geq 2$, for $j = 1$ or $j = 2$, where $i(x, y)$ denotes the geometric intersection number of curves x and y.*

Finally, it is noted that γ can be used to construct a cover such that the element g in the corresponding $P\,\mathrm{Sp}(2g-2, \mathbb{Z})$ leaves invariant a line in $\mathbb{Z}2g-2$, from which the genericity of pseudo-Anosovs in the *whole* Torelli follows.

In fact, one can combine the above with the methods and results of [Rivin 2010b] it can be shown that a for a generic subgroup of Torelli, a generic element is pseudo-Anosov. However, the silver bullet would be the following:

Conjecture 8.5. For any nonelementary subgroup H of the mapping class group there is a cover $\tilde{S}$ to which H lifts, and such that the image of H under the Torelli homomorphism is not solvable, with the degree of the cover at most polynomial in the sums of the word-lengths of the generators of H.

It should be noted that we are *very* far from being able to resolve Conjecture 8.5. For example, while it is known that for every pseudo-Anosov mapping class ψ there exists *some* cover to which ψ lifts, and such that the ψ is not in the Torelli subgroup for that cover [Koberda 2012], it is *not* known that the image $\mathfrak{T}(\psi)$ is of infinite order! The degree of the cover is effective — the bounds in the paper follow essentially from the results of Edna Grossman [1974] — but, just as in her paper, they are easily doubly exponential in the word length of the element.

9. The geometric approach

Above we have alluded to the "geometric" approach to the mapping class, which uses the curve complex. This approach was used by Joseph Maher [2011] (where he also shows other remarkable results). Maher's results are very general, but not effective. A somewhat more conceptual approach was undertaken in a very nice paper by A. Malyutin, using the followin approach.

First, he uses the central limit theorem of M. Björklund and T. Hartnick [2011] (which is a vast generalization, at the cost of losing effectiveness completely of some of the results of [Rivin 1999]) to show this:

Theorem 9.1 [Malyutin 2011]. *Let G be a countable group and let $\Phi : G \mapsto \mathbb{R}^d$ is a nondegenerate $\mathbb{R}^d$-quasimorphism. Then, for each nondegenerate probability measure μ on G and for every bounded subset $Q \subset \mathbb{R}^d$, there is a constant $C = C(G, \Phi, \mu, Q)$ such that for any $k \in \mathbb{N}$ and $\boldsymbol{x} \in \mathbb{R}^d$ we have*

$$\mu^{*k}(\Phi^{-1}(\boldsymbol{x} + Q)) < Ck^{-d/2},$$

where μ^{*k} denotes the k-fold convolution of μ with itself.

Recall that a *quasimorphism* from a group G to $\mathbb{R}$ is a map $\phi : G \mapsto \mathbb{R}$ such that the following condition holds:

$$\sum_{h,g\in G} \left|\phi(gh) - \phi(g) - \phi(h)\right| < \infty. \tag{13}$$

An $\mathbb{R}^d$ quasimorphism is a map $\Phi : G \to \mathbb{R}^d$ which satisfies the inequality (13) (where $|\cdot|$ now denotes some Banach norm) — a map is an $\mathbb{R}^d$ quasimorphism if and only if its coordinates are garden-variety quasimorphisms. Such a Φ is called *nondegenerate* if its image is not contained in a proper hyperplane.

An immediate corollary of Theorem 9.1 is:

Corollary 9.2. *If a subset S of a countable group G has bounded image under a nondegenerate $\mathbb{R}^d$-quasimorphism $G \mapsto \mathbb{R}^d$, then for every nondegenerate probability measure μ on G there exists a constant $C = C(\mu)$, such that for each $k \in \mathbb{N}$ we have*

$$\mu^{*k}(S) < Ck^{-d/2}.$$

The other ingredient is the result of M. Bestvina and K. Fujiwara [2002], which states that if H is a nonelementary subgroup of the mapping class group of a surface, than there are infinitely many linearly independent quasimorphisms which all map the non-pseudo-Anosov mapping classes to 0.

The Bestvina–Fujiwara theorem and Corollary 9.2 together show that the probability of being non-pseudo-Anosov decreases faster than any polynomial (but does not quite show exponential decay). All constants in the argument are completely ineffective.

Acknowledgements

The author would like to thank Ilan Vardi, Alex Eskin, Inna Capdeboscq, Peter Sarnak, Tania Smirnova-Nagnibeda and Tobias Hartnick for enlightening conversations, and the editors for their patience.

References

[Atalan and Korkmaz 2010] F. Atalan and M. Korkmaz, "Number of pseudo-Anosov elements in the mapping class group of a four-holed sphere", *Turkish J. Math.* **34**:4 (2010), 585–592.

[Beardon 1968] A. F. Beardon, "The exponent of convergence of Poincaré series", *Proc. London Math. Soc.* (3) **18**:3 (1968), 461–483.

[Bestvina and Fujiwara 2002] M. Bestvina and K. Fujiwara, "Bounded cohomology of subgroups of mapping class groups", *Geom. Topol.* **6** (2002), 69–89.

[Bestvina and Handel 1992] M. Bestvina and M. Handel, "Train tracks and automorphisms of free groups", *Ann. of Math.* (2) **135**:1 (1992), 1–51.

[Björklund and Hartnick 2011] M. Björklund and T. Hartnick, "Biharmonic functions on groups and limit theorems for quasimorphisms along random walks", *Geom. Topol.* **15**:1 (2011), 123–143.

[Bougerol and Lacroix 1985] P. Bougerol and J. Lacroix, *Products of random matrices with applications to Schrödinger operators*, Progress in Probability and Statistics **8**, Birkhäuser, Boston, 1985.

[Brav and Thomas 2012] C. Brav and H. Thomas, "Thin monodromy in Sp(4)", preprint, 2012. arXiv 1210.0523

[Breuillard et al. 2011] E. Breuillard, B. Green, and T. Tao, "Approximate subgroups of linear groups", *Geom. Funct. Anal.* **21**:4 (2011), 774–819.

[Capdeboscq and Rivin $\geq$ 2012] I. Capdeboscq and I. Rivin, "The density of profinite density". In preparation.

[Casson and Bleiler 1988] A. J. Casson and S. A. Bleiler, *Automorphisms of surfaces after Nielsen and Thurston*, London Math. Soc. Student Texts **9**, Cambridge University Press, 1988.

[Davenport 2000] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics **74**, Springer, New York, 2000.

[Duke et al. 1993] W. Duke, Z. Rudnick, and P. Sarnak, "Density of integer points on affine homogeneous varieties", *Duke Math. J.* **71**:1 (1993), 143–179.

[Dunfield and Thurston 2003] N. M. Dunfield and W. P. Thurston, "The virtual Haken conjecture: Experiments and examples", *Geom. Topol.* **7** (2003), 399–441.

[Dunfield and Thurston 2006] N. M. Dunfield and W. P. Thurston, "Finite covers of random 3-manifolds", *Invent. Math.* **166**:3 (2006), 457–521.

[Epstein et al. 1992] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, *Word processing in groups*, Jones and Bartlett, Boston, 1992.

[Eskin and McMullen 1993] A. Eskin and C. McMullen, "Mixing, counting, and equidistribution in Lie groups", *Duke Math. J.* **71**:1 (1993), 181–209.

[Farb 2006] B. Farb, "Some problems on mapping class groups and moduli space", pp. 11–55 in *Problems on mapping class groups and related topics*, edited by B. Farb, Proc. Sympos. Pure Math. **74**, Amer. Math. Soc., Providence, RI, 2006.

[Farb and Margalit 2011] B. Farb and D. Margalit, *A primer on mapping class groups*, Princeton Mathematical Series **49**, Princeton University Press, 2011.

[Farb et al. 2008] B. Farb, C. J. Leininger, and D. Margalit, "The lower central series and pseudo-Anosov dilatations", *Amer. J. Math.* **130**:3 (2008), 799–827.

[Fieker and Stehlé 2010] C. Fieker and D. Stehlé, "Short bases of lattices over number fields", pp. 157–173 in *Algorithmic number theory* (Nancy, 2010), edited by G. Hanrot et al., Lecture Notes in Comput. Sci. **6197**, Springer, Berlin, 2010.

[Fuchs and Rivin $\geq$ 2012] E. Fuchs and I. Rivin, "How thin is thin?". In preparation.

[Gama et al. 2006] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen, "Symplectic lattice reduction and NTRU", pp. 233–253 in *Advances in cryptology—EUROCRYPT 2006* (St. Petersburg, 2006), edited by S. Vaudenay, Lecture Notes in Comput. Sci. **4004**, Springer, Berlin, 2006.

[Grossman 1974] E. K. Grossman, "On the residual finiteness of certain mapping class groups", *J. London Math. Soc.* (2) **9**:1 (1974), 160–164.

[Grunewald and Lubotzky 2009] F. Grunewald and A. Lubotzky, "Linear representations of the automorphism group of a free group", *Geom. Funct. Anal.* **18**:5 (2009), 1564–1608.

[Hardy and Wright 2008] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008.

[Humphries 1988] S. P. Humphries, "Free subgroups of $\mathrm{SL}(n, \mathbf{Z})$, $n > 2$, generated by transvections", *J. Algebra* **116**:1 (1988), 155–162.

[Ivanov 1992] N. V. Ivanov, *Subgroups of Teichmüller modular groups*, Translations of Mathematical Monographs **115**, Amer. Math. Soc., Providence, RI, 1992.

[Jouve et al. 2013] F. Jouve, E. Kowalski, and D. Zywina, "Splitting fields of characteristic polynomials of random elements in arithmetic groups", *Israel J. Math.* **193**:1 (2013), 263–307.

[Kantor and Lubotzky 1990] W. M. Kantor and A. Lubotzky, "The probability of generating a finite classical group", *Geom. Dedicata* **36**:1 (1990), 67–87.

[Kapovich et al. 2007] I. Kapovich, I. Rivin, P. Schupp, and V. Shpilrain, "Densities in free groups and $\mathbb{Z}^k$, visible points and test elements", *Math. Res. Lett.* **14**:2 (2007), 263–284.

[Koberda 2012] T. Koberda, "Asymptotic linearity of the mapping class group and a homological version of the Nielsen–Thurston classification", *Geom. Dedicata* **156** (2012), 13–30.

[Kowalski 2008] E. Kowalski, *The large sieve and its applications: Arithmetic geometry, random walks and discrete groups*, Cambridge Tracts in Mathematics **175**, Cambridge University Press, 2008.

[Lax 2002] P. D. Lax, *Functional analysis*, Wiley, New York, 2002.

[Liebeck and Shalev 1995] M. W. Liebeck and A. Shalev, "The probability of generating a finite simple group", *Geom. Dedicata* **56**:1 (1995), 103–113.

[Looijenga 1997] E. Looijenga, "Prym representations of mapping class groups", *Geom. Dedicata* **64**:1 (1997), 69–83.

[Lubotzky 1999] A. Lubotzky, "One for almost all: Generation of $\mathrm{SL}(n, p)$ by subsets of $\mathrm{SL}(n, \mathbf{Z})$", pp. 125–128 in *Algebra, K–theory, groups, and education* (New York, 1997), edited by T. Y. Lam and A. R. Magid, Contemp. Math. **243**, Amer. Math. Soc., Providence, RI, 1999.

[Lubotzky 2005] A. Lubotzky, "What is... property (τ)?", *Notices Amer. Math. Soc.* **52**:6 (2005), 626–627.

[Lubotzky and Meiri 2012a] A. Lubotzky and C. Meiri, "Sieve methods in group theory I: Powers in linear groups", *J. Amer. Math. Soc.* **25**:4 (2012), 1119–1148.

[Lubotzky and Meiri 2012b] A. Lubotzky and C. Meiri, "Sieve methods in group theory II: The mapping class group", *Geom. Dedicata* **159** (2012), 327–336.

[Lubotzky and Meiri 2012c] A. Lubotzky and C. Meiri, "Sieve methods in group theory, III: $\mathrm{Aut}(F_n)$", *Internat. J. Algebra Comput.* **22**:7 (2012), 1250062.

[Maher 2011] J. Maher, "Random walks on the mapping class group", *Duke Math. J.* **156**:3 (2011), 429–468.

[Malestein and Souto 2013] J. Malestein and J. Souto, "On genericity of pseudo-Anosovs in the Torelli group", *Int. Math. Res. Not.* **2013**:6 (2013), 1434–1449.

[Malyutin 2011] A. V. Malyutin, "Quasimorphisms, random walks, and transient subsets in countable groups", *Zap. Nauchn. Sem.* (*POMI*) **390** (2011), 210–236. Republished in *J. Math. Sci. New York* **181**:6 (2012), 871–885.

[Matthews et al. 1984] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler, "Congruence properties of Zariski-dense subgroups, I", *Proc. London Math. Soc.* (3) **48**:3 (1984), 514–532.

[McMullen 1998] C. T. McMullen, "Hausdorff dimension and conformal dynamics, III: Computation of dimension", *Amer. J. Math.* **120**:4 (1998), 691–721.

[Neumann and Praeger 1992] P. M. Neumann and C. E. Praeger, "A recognition algorithm for special linear groups", *Proc. London Math. Soc.* (3) **65**:3 (1992), 555–603.

[Nevo and Sarnak 2010] A. Nevo and P. Sarnak, "Prime and almost prime integral points on principal homogeneous spaces", *Acta Math.* **205**:2 (2010), 361–402.

[Newman 1972] M. Newman, *Integral matrices*, Pure and Applied Mathematics **45**, Academic Press, New York, 1972.

[Newman 1980] D. J. Newman, "Simple analytic proof of the prime number theorem", *Amer. Math. Monthly* **87**:9 (1980), 693–696.

[Newman 1988] M. Newman, "Counting modular matrices with specified Euclidean norm", *J. Combin. Theory Ser. A* **47**:1 (1988), 145–149.

[Nguyen 2011] P. Q. Nguyen, "Lattice reduction algorithms: Theory and practice", pp. 2–6 in *Advances in cryptology—EUROCRYPT 2011* (Tallinn, Estonia, 2011), edited by K. G. Paterson, Lecture Notes in Comput. Sci. **6632**, Springer, Berlin, 2011.

[Otal 2001] J.-P. Otal, *The hyperbolization theorem for fibered* 3*–manifolds*, SMF/AMS Texts and Monographs **7**, Amer. Math. Soc., Providence, RI, 2001.

[Page 2012] A. Page, "Computing arithmetic Kleinian groups", preprint, 2012. arXiv 1206.0087

[Platonov and Rapinchuk 1994] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics **139**, Academic Press, Boston, 1994.

[Poénaru et al. 1979] *Travaux de Thurston sur les surfaces*, Astérisque **66**, Société Mathématique de France, Paris, 1979.

[Prasad and Rapinchuk 2014] G. Prasad and A. S. Rapinchuk, "Generic elements in Zariski-dense subgroups and isospectral locally symmetric space", pp. 211–252 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge, New York, 2014.

[Rapinchuk 2012] A. S. Rapinchuk, "Strong approximation for algebraic groups", preprint, 2012. arXiv 1207.4425

[Rivin 1994] I. Rivin, "Intrinsic geometry of convex ideal polyhedra in hyperbolic 3-space", pp. 275–291 in *Analysis, algebra, and computers in mathematical research* (Luleå, 1992), edited by M. Gyllenberg, Lecture Notes in Pure and Appl. Math. **156**, Dekker, New York, 1994.

[Rivin 1999] I. Rivin, "Growth in free groups (and other stories)", preprint, 1999. arXiv math/9911076

[Rivin 2001] I. Rivin, "Simple curves on surfaces", *Geom. Dedicata* **87**:1-3 (2001), 345–360.

[Rivin 2008] I. Rivin, "Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms", *Duke Math. J.* **142**:2 (2008), 353–379.

[Rivin 2009] I. Rivin, "Walks on graphs and lattices—effective bounds and applications", *Forum Math.* **21**:4 (2009), 673–685.

[Rivin 2010a] I. Rivin, "Growth in free groups (and other stories)—twelve years later", *Illinois J. Math.* **54**:1 (2010), 327–370.

[Rivin 2010b] I. Rivin, "Zariski density and genericity", *Int. Math. Res. Not.* **2010**:19 (2010), 3649–3657.

[Scott 1983] P. Scott, "The geometries of 3–manifolds", *Bull. London Math. Soc.* **15**:5 (1983), 401–487.

[Sharp 2001] R. Sharp, "Local limit theorems for free groups", *Math. Ann.* **321**:4 (2001), 889–904.

[Singh and Venkataramana 2012] S. Singh and T. N. Venkataramana, "Arithmeticity of certain symplectic hypergeometric groups", preprint, 2012. To appear in *Duke Math. J.* arXiv 1208.6460

[Takasawa 2001] M. Takasawa, "Enumeration of mapping classes for the torus", *Geom. Dedicata* **85**:1-3 (2001), 11–19.

[Thompson 1995] J. G. Thompson, "4-punctured spheres", *J. Algebra* **171**:2 (1995), 587–605.

[Thurston 1988] W. P. Thurston, "On the geometry and dynamics of diffeomorphisms of surfaces", *Bull. Amer. Math. Soc.* (*N.S.*) **19**:2 (1988), 417–431.

[Thurston and Milnor 1979] W. P. Thurston and J. W. Milnor, "The geometry and topology of three-manifolds", Lecure notes, Princeton University, 1979, http://library.msri.org/books/gt3m/.

[Vardi 1993] I. Vardi, "Dedekind sums have a limiting distribution", *Int. Math. Res. Not.* **1993**:1 (1993), 1–12.

[Vardi 2009] I. Vardi, "Continued fractions from Euclid to the present day", preprint, 2009, http://www.chronomaitre.org/ContinuedFractions.pdf.

[Weigel 1996] T. Weigel, "On the profinite completion of arithmetic groups of split type", pp. 79–101 in *Lois d'algèbres et variétés algébriques* (Colmar, 1991), edited by M. Goze, Travaux en Cours **50**, Hermann, Paris, 1996.

[Yao and Knuth 1975] A. C. Yao and D. E. Knuth, "Analysis of the subtractive algorithm for greatest common divisors", *Proc. Nat. Acad. Sci. U.S.A.* **72**:12 (1975), 4720–4722.

[Zimmer 1984] R. J. Zimmer, *Ergodic theory and semisimple groups*, Monographs in Mathematics **81**, Birkhäuser, Basel, 1984.

rivin@temple.edu

Department of Mathematics, Temple University, Philadelphia, PA 19122, United States