THE UBIQUITY OF THIN GROUPS

ELENA FUCHS

Abstract. In this article, which is an elaboration of our talk at the MSRI workshop "Thin Groups and Super Strong Approximation," we discuss how one can approach the question of whether typical subgroups of $\mathrm{GL}_n(\mathbb{Z})$ are thin. We discuss interpretations of what typical should mean, motivated by recently solved arithmetic problems involving thin groups. We give an overview of what is known about the ubiquity of thin groups which come up in these problems and describe some known tools to detect whether a given subgroup of $\mathrm{GL}_n(\mathbb{Z})$ is thin.

1. Introduction

While studying number theoretic properties of arithmetic groups is fairly classical, the number theory connected to thin groups (see Definition 1.1 below) is a relatively new and still developing area of mathematics, and our understanding of the theory is much more narrow than that of its classical counterpart. Various new arithmetic methods (see [4], [10], and [28], for example) which apply to thin and arithmetic groups alike have already served to unify these two fields by showing that thin groups often exhibit rich properties similar to those of arithmetic groups. With this in mind, it is natural to try to further not only our understanding of the arithmetic of specific thin groups, but also of the question of how ubiquitous thin groups are in general. For example, given a subgroup of $\mathrm{GL}_n(\mathbb{Z})$, we have a limited arsenal of tools to determine whether the group is thin or not. Similarly, given an infinite family of groups which come up in a specific kind of arithmetic problem, we know little about whether the generic group in such a family is thin. In this article, we discuss both of these issues and what is currently known towards resolving them.

Throughout what follows, we focus for simplicity on subgroups of $\mathrm{GL}_n(\mathbb{Z})$, and so we give the following definition of a thin group.

Definition 1.1. Let Γ be a subgroup of $\mathrm{GL}_n(\mathbb{Z})$, and let $G = \mathrm{Zcl}(\Gamma)$ be its Zariski closure. We say that Γ is *thin* if Γ is of infinite index in $G(\mathbb{Z})$.

We begin by reviewing briefly the tools used in various arithmetic problems associated to thin groups, as this will shed some light on what remains to be understood from the number theoretic point of view in this context. One of the main ingredients used in such problems is families of expander graphs. There are various equivalent definitions of such families of graphs (see [22]). One such definition can be given by considering the eigenvalues of the adjacency matrices of the graphs in the family. By the adjacency matrix

The author is supported by the Simons Foundation through the Postdoctoral Fellows program.

M of a finite graph X on n vertices, we mean the $n \times n$ matrix whose rows and columns are indexed by the vertices of X, with

$$M_{ij} = \begin{cases} 1 & \text{iff the vertices } v_i \text{ and } v_j \text{ are adjacent} \\ 0 & \text{otherwise} \end{cases}$$

Let $\lambda_0(M) \geq \cdots \geq \lambda_{n-1}(M)$ be the eigenvalues of M. If X is connected, as we will assume from now on, we have that $\lambda_0 > \lambda_1$. Furthermore, if X is a k-regular graph, we have that $\lambda_0 = k$. With this notation, we define a family of expander graphs as follows.

Definition 1.2. Let $\{X_i\}_{i\geq 1}$ be an infinite family of finite graphs (we assume here that each graph X_i is connected and k-regular for some fixed k) and let $|X_i| \to \infty$ as $i \to \infty$. Let M_i denote the adjacency matrix of X_i. We say that $\{X_i\}_{i\geq 1}$ is a family of expanders iff

$$\limsup_{n\to\infty} \lambda_1(M_n) < k.$$

In other words, a family of graphs as above is an expander family if there is a spectral gap between the top two eigenvalues of the family's corresponding adjacency matrices. This notion of expander graphs is featured in the arithmetic of finitely generated subgroups of $\mathrm{GL}_n(\mathbb{Z})$ as follows. Given a group $\Gamma \subset \mathrm{GL}_n(\mathbb{Z})$ via a finite symmetric generating set S, we let Γ_d and S_d denote the image of Γ and, respectively, S in $\mathrm{GL}_n(\mathbb{Z}/d\mathbb{Z})$ where $d \in \mathbb{Z}$ is square free. To each such Γ_d we associate the Cayley graph $\mathrm{Cay}(\Gamma_d, S_d)$ and so we obtain an infinite family of connected finite graphs associated to Γ. Whether or not Γ is thin, if this infinite family of finite graphs is an expander family, we say that Γ satisfies the expander property, and this property plays a crucial role in various arithmetic problems, two of which we mention in the next section. We note that checking whether or not Γ satisfies the expander property is relatively straightforward due to the following theorem (which is a culminating result in a long line of work – see [3], [4], [6], [15], [18], [25], [29], [30], etc) of Salehi-Golsefidy and Varju.

Theorem 1.3 (Salehi-Golsefidy-Varju [28])**.** *Let $\Gamma \leq \mathrm{GL}_n(\mathbb{Z})$ be a group with a finite symmetric generating set S and let G denote the Zariski closure of Γ. For $d \in \mathbb{Z}$ square free, let Γ_d and S_d denote the projection of Γ and S, respectively, in $\mathrm{GL}_n(\mathbb{Z}/d\mathbb{Z})$. Then the necessary and sufficient condition for*

$$\{\mathrm{Cay}(\Gamma_d, S_d) \mid d \in \mathbb{Z} \text{ square free}, (d, C) = 1\}$$

to be a family of expanders for some integer $C > 0$ is that the connected component of G is perfect.

Thus to determine whether Γ has the expander property one essentially needs information only about the Zariski closure of the group, which is completely independent of the thinness of the group and is in practice easier to determine than the index. So if this crucial expander property does not differentiate between thin and arithmetic groups in the above sense, what is the difference between the two in practice? One major difference is that there is currently no method to determine a good lower bound on the spectral gap associated to a thin group Γ, and such a lower bound can be important in applications. In fact, although for arithmetic groups there are more tools to determine the spectral gap, these tools are only

useful if we can show are group Γ is arithmetic in the first place (which in general is quite difficult). So it is clear that there is a need to be able to detect thin versus arithmetic groups. In addition, it is interesting to obtain some measure of how ubiquitous thin groups are in number theoretic applications as opposed to arithmetic groups: if thin groups are generic in some sense, it is natural that we should try to develop further the methods we have to study them.

In this article we give a flavor of how to approach questions about the genericity of thin groups as well as how one might decide whether a given group is thin. Our discussion is motivated by two arithmetic applications of Theorem 1.3: one is the affine sieve as developed in [4] and [27], and the other is the application to monodromy groups of [10]. We describe these applications via examples in the next section: the affine sieve will be introduced by considering Apollonian circle packings, and the application from [10] will be introduced by considering a family of hyperelliptic curves. These examples are also meant to show the contrast between the study of thin and arithmetic groups. In Section 2 we then survey what has been done to answer the question of how generic thin groups are in various situations. Finally, in Section 3 we focus on the issue of determining when certain monodromy groups are thin.

Acknowledgements: We thank MSRI as well as the organizers of the "Thin Groups and Super Strong Approximation" workshop for a fruitful and stimulating workshop. We also thank I. Capdeboscq, C. Meiri, I. Rivin, and P. Sarnak for the collaborations which led to much of the work summarized in this article.

1.1. **Two Examples: Thin versus Arithmetic Groups.** We now describe two examples of the applications of expanders discussed above: the first involves a thin group, and the second involves an arithmetic group.

Example 1:

Our first example concerns Apollonian circle packings and is meant to illustrate how the affine sieve can be useful in diophantine problems connected to thin groups. Apollonian packings are constructed by starting with the Descartes configuration of four mutually tangent circles, one of which is on the outside of the other three, and repeatedly packing smaller circles into the resulting triangular interstices as in the picture in Figure 1. A theorem of Apollonius of Perga states that there is indeed a unique way to inscribe a circle into every interstice below, and so this construction is well defined.

These packings give rise to problems in number theory as follows: one can show that if the original four circles have integer curvature, all of the circles in the packing will have integer curvature: such packings are called integer Apollonian packings. One can ask many arithmetic questions in this context (see [11], [16], [19], etc), but in this example we will focus on the study of quadruples of mutually tangent circles all of which have curvatures with few prime factors. The key to studying this and many other arithmetic properties of Apollonian packings is a theorem of Descartes in [9] which relates the curvatures of any four mutually tangent circles. Namely, if a, b, c, and d denote the curvatures of four mutually tangent circles

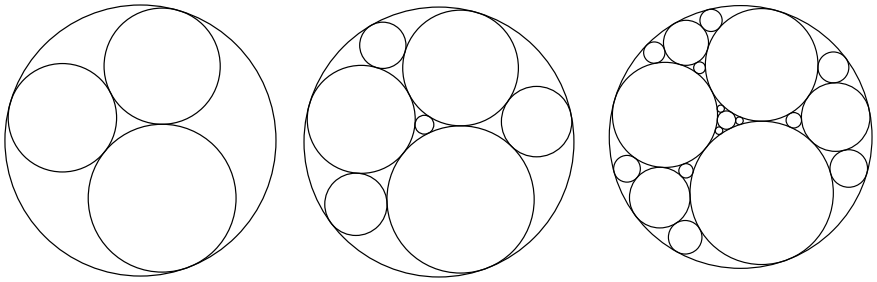

FIGURE 1. Apollonian circle packing

(where a circle is taken to have negative curvature if it is internally tangent to the other three), then

$$Q(a,b,c,d) := 2(a^2+b^2+c^2+d^2) - (a+b+c+d)^2 = 0. \tag{1.1}$$

A fairly easy consequence of this fact (see [11], for example) is that in a given packing P one can interpret the set of Descartes quadruples, or the curvatures of quadruples of mutually tangent circles, as the orbit of a group $A \subset \mathrm{O}_Q(\mathbb{Z})$ which is generated by reflections and known as the Apollonian group. Specifically, if $\mathbf{v}_P \in \mathbb{Z}^4$ is any Descartes quadruple in the packing P then there is a one to one correspondence between points of the orbit $A\mathbf{v}_P$ and Descartes quadruples in P, and every Descartes quadruple in P is a vector in $A\mathbf{v}_P$. So to study Apollonian packings one must study orbits of this group A. It can be shown (see [11] for example) that A is a thin group: it is Zariski dense in $\mathrm{O}_Q(\mathbb{C})$ yet it is of infinite index in $\mathrm{O}_Q(\mathbb{Z})$.

Now, suppose given an Apollonian orbit $\mathcal{O}$ corresponding to a packing P and a polynomial $f(x_1,x_2,x_3,x_4) \in \mathbb{Z}[x_1,x_2,x_3,x_4]$ we are interested in the set of points

$$\{\mathbf{x} \in \mathcal{O} \mid f(\mathbf{x}) \text{ has at most } r \text{ prime factors}\} \tag{1.2}$$

where r is some positive integer. For example, we might wish to count the number of points in a ball in this set, or determine for which r this set is large in some sense. For a general thin group, questions of this kind have been only recently handled using the affine sieve as developed in [4] and [27]: for any integer orbit $\mathcal{O}$ of a finitely generated subgroup G of $\mathrm{GL}_n(\mathbb{Z})$ which satisfies the expander property it is known that there is some finite $r > 0$ such that the set in (1.2) is large in the sense that it is Zariski dense in $\mathrm{Zcl}(\mathcal{O})$. We call the smallest such r the saturation number of the pair $(\mathcal{O}, f)$. Furthermore, the affine sieve enables us to count the number of points in the set (1.2) in a ball, and the expander property described before controls the remainder term in this sieve. However, there is still work to be done if we wish to implement the affine sieve with any accuracy. For example, the saturation number of $(\mathcal{O}, f)$ depends on the spectral gap of the group G: the larger the spectral gap, the smaller the saturation number. As we mentioned before, there is currently no method to get a good lower bound on the spectral gap for thin groups – the Apollonian group A in particular. Thus the affine sieve does not give good upper bounds for saturation numbers connected to the orbits of A. Luckily, while A is thin it is a relatively nice thin group: for example, it contains many unipotent subgroups which are a main tool in the proof of the following theorem.

Theorem 1.4 ([11]). *Let $\mathbf{v}_P$ be a primitive integer Descartes quadruple, let A be the Apollonian group and let $\mathcal{P} = A\mathbf{v}_P$. For $\mathbf{x} = (x_1, x_2, x_3, x_4)^t \in \mathcal{P}$ let $f(\mathbf{x}) = x_1x_2x_3x_4/12$, and let $\mathcal{P}_{28}$ denote those points $\mathbf{x} \in \mathcal{P}$ for which $f(\mathbf{x})$ has at most 28 prime factors. Then $\mathcal{P}_{28}$ is Zariski dense in $\mathrm{Zcl}(\mathcal{P})$.*

We remark here that it is conjectured that the 28 above should be 4, and without a good grip on the spectral gap for the Apollonian group it is unclear how one could come much closer to this conjectured value.

Example 2:

The second example comes from work of Ellenberg-Hall-Kowalski in [10]. Their results are quite general, but we will focus on the following very specific result (Corollary 5 in their paper) for contrast with the previous example above.

Theorem 1.5 (Ellenberg-Hall-Kowalski [10]). *Let k be a number field, and let $f \in k[X]$ be a squarefree polynomial of degree $2g$ with $g \geq 1$. Let U_f be the complement of the zeros of f in $\mathbb{A}^1$, and let $\mathcal{C}/U$ be the family of hyperelliptic curves given by*

$$\mathcal{C} : y^2 = f(x)(x - t),$$

with Jacobians $J_t = \mathrm{Jac}(\mathcal{C}_t)$. Then for any $d \geq 1$, the set

$$\bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \mathrm{End}_{\mathbb{C}}(J_t) \neq \mathbb{Z}\}$$

is finite.

In the proof of this theorem, Ellenberg et.al. consider the monodromy group Γ associated to the family of hyperelliptic curves above. In this case $\Gamma \subset \mathrm{Sp}_{2g}(\mathbb{Z})$ and is Zariski dense in Sp_{2g}. A crucial ingredient in the proof is that Γ satisfies the expander property which is an immediate consequence of Theorem 1.3. However, because in this case it is known from [31] that Γ is finite index in $\mathrm{Sp}_{2g}(\mathbb{Z})$ – i.e. it is arithmetic – one can show this expander property rather classically, without appealing to the intricate methods which go into the proof of Theorem 1.3. One way to do this for $g \geq 2$ is to note that $\mathrm{Sp}_{2g}(\mathbb{Z})$ and any finite index subgroup has Kazhdan property T (for a definition and discussion of property T, see [21]). Therefore Γ has property T as well, and the fact that Γ must then satisfy the expander property follows by a theorem of Margulis in [23], where expander graphs were explicitly constructed for the first time. In addition, in this case one can get a good bound on the spectral gap. However, this property T route is not available unless one knows that the group in question is arithmetic.

We should mention here that while Theorem 1.5 concerns just one monodromy group, [10] deals with an infinite family of monodromy groups some of which are known to be thin.

2. Generic Thin Groups

We now turn to our question of how generic or ubiquitous thin groups are, pointing out two different variants of the question. The first variant is inspired by the affine sieve, which is a tool to count prime

and almost prime points in integer orbits of subgroups of $\mathrm{GL}_n(\mathbb{Z})$: namely, given a suitable definition of "likely" which we specify shortly, we ask

1) How likely is it that a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Z})$ is thin?

On the other hand, we might wish to ask a more specific question about the genericity of thin groups by focusing on Ellenberg et.al.'s work on monodromy groups in [10]. Thus another variant of the question about the ubiquity of thin groups is

2) Is the generic monodromy group appearing in [10] thin?

Concerning Question 1 above, it is expected that the generic finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Z})$ is indeed thin for many reasonable definitions of generic. One can simplify the problem somewhat by considering this question for $G = \mathrm{SL}_n(\mathbb{Z})$. Specifically, for $n \geq 2$, one can consider pairs of elements $(\gamma_1, \gamma_2) \in G^2$ and ask for the probability that $\Gamma(\gamma_1, \gamma_2)$, the group generated by γ_1, γ_2, is an infinite index subgroup of G (one can also consider groups generated by k elements for a fixed $k \geq 2$). This is a little different, at first glance, than asking for the probability that $\Gamma(\gamma_1, \gamma_2)$ is thin – i.e. that the group is of infinite index in its Zariski closure. However, for many reasonable definitions of "generic", it is known that the generic subgroup of $\mathrm{SL}_n(\mathbb{Z})$ is in fact Zariski dense in SL_n (see [26], for example). In particular, $\mathrm{Zcl}(\Gamma(\gamma_1, \gamma_2))$ is all of SL_n with high probability, and so considering the group's index in $\mathrm{SL}_n(\mathbb{Z})$ is synonymous with considering thinness in this case.

We now describe two ways to interpret "probability" above, and note that there are of course other ways. In both cases we define a sequence of measures μ_T on G which in turn defines the probability we want.

One way to interpret the probability is combinatorial. Namely, fix a finite generating set $\{g_1, \ldots, g_r\}$ of G and let μ_T denote the normalized counting measure on the set W_T^2 of elements of $(\gamma_1, \gamma_2) \in G^2$ such that for $k = 1, 2$ γ_k can be written as a word of length $\leq T$ in the generators g_i. We then consider the limit

$$\lim_{T \to \infty} \mu_T(\{(\gamma_1, \gamma_2) \in W_T^2 \mid [G : \Gamma(\gamma_1, \gamma_2)] = \infty\}).$$

Aoun shows in [1] that this limit is in fact 1: i.e. that if we obtain our γ_i by taking random walks on a fixed generating set of G then Γ will be infinite index with high probability.

Another natural way to interpret this probability is via an archimedean model (in fact, in some sense this is the most intuitive formulation of the problem, since in arithmetic problems we are often interested in counting in archimedean balls). Namely, we let μ_T be the normalized counting measure on the set B_T^2 of elements $(\gamma_1, \gamma_2) \in G^2$ such that for $k = 1, 2$ $||\gamma_k|| < T$ or $||\gamma_k^{-1}|| < T$. Here we define $||\gamma|| > 0$ as follows:

$$||\gamma|| := \sqrt{\lambda_{\max}(\gamma^t \gamma)} \tag{2.1}$$

where $\lambda_{\max}$ denotes the maximal eigenvalue. We then consider the limit

$$\lim_{T \to \infty} \mu_T(\{(\gamma_1, \gamma_2) \in B_T^2 \mid [G : \Gamma(\gamma_1, \gamma_2)] = \infty\}).$$

This limit is also shown to be 1 in [14]. The general strategy in both of these interpretations of the question is to show that $\Gamma(\gamma_1, \gamma_2)$ is free with high probability. Since any free subgroup of $G = \mathrm{SL}_n(\mathbb{Z})$ where $n > 2$ is infinite index, this is enough for nearly all of the cases (in the case that $n = 2$ one uses the fact that the generic subgroup Γ is free to show that its limit set will generically have small Hausdorff dimension, which then implies the infinite index we need).

So in these senses thin subgroups of $\mathrm{SL}_n(\mathbb{Z})$ are generic.

As far as Question 2 above goes, a major obstacle in answering it is choosing an intuitive definition for a generic monodromy group which would make the question above approachable. As of yet, we have found no such definition, and nothing is known towards answering this very broad question. We discuss the very different issue of deciding whether a given monodromy group is thin in the next section.

3. Monodromy Groups

Since we have no satisfactory definition of a generic monodromy group, we restrict here to a special class of the monodromy groups which come up in [10] and study the issue of thinness within this class. Let $\theta = z\frac{d}{dz}$ and define the differential operator D on $\mathbb{P}^1(\mathbb{C})$ by

$$\begin{aligned} D &:= D(\alpha, \beta) \\ &= D(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) \\ &= (\theta + \beta_1 - 1) \cdots (\theta + \beta_n - 1) - z(\theta + \alpha_1) \cdots (\theta + \alpha_n) \end{aligned}$$

where $\alpha, \beta \in \mathbb{Q}^n$, $0 \leq \alpha_1 \leq \cdots \leq \alpha_n < 1$, and $0 \leq \beta_1 \leq \cdots \leq \beta_n < 1$ (one can also consider the more general case of $\alpha_i, \beta_i \in \mathbb{C}$ but we do not discuss this here). The differential equation $D(\alpha, \beta)u = 0$ is hypergeometric and is regular outside of three singularities at $z = 0, 1, \infty$. One associates a monodromy group to such a hypergeometric equation as follows. For $x_0 \in \mathbb{P}^1(\mathbb{C})\backslash\{0, 1, \infty\}$ let S_0 be the solution space to $D(\alpha, \beta)u = 0$ at x_0. We then have a representation of the fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C})\backslash\{0, 1, \infty\})$ in $\mathrm{GL}(S_0)$. We call the image of this representation $H(\alpha, \beta)$ and refer to it as the monodromy group associated to $D(\alpha, \beta)$. Beukers-Heckman prove various results about these groups which we mention below. The following theorem of Levelt which describes $H(\alpha, \beta)$ via a generating set is key both in their work and in joint work with Meiri and Sarnak in [13].

Theorem 3.1 (Levelt, [20])**.** *For $1 \leq i \leq n$ let α_i and β_i be as above. Define the complex numbers $A_1, \ldots, A_n, B_1, \ldots, B_n$ as the coefficients of the polynomials*

$$P(z) := \prod_{j=1}^{k}(z - e^{2\pi i\alpha_j}) = z^n + A_1 z^{n-1} + \cdots + A_n \quad \textit{and} \quad Q(z) := \prod_{j=1}^{k}(z - e^{2\pi i\beta_j}) = z^n + B_1 z^{n-1} + \cdots + B_n.$$

Then $H(\alpha,\beta)$ is the group generated by

$$A=\begin{pmatrix} 0 & 0 & \cdots & 0 & -A_n \\ 1 & 0 & \cdots & 0 & -A_{n-1} \\ 0 & 1 & \cdots & 0 & \vdots \\ 0 & 0 & \ddots & 0 & -A_2 \\ 0 & 0 & \cdots & 1 & -A_1 \end{pmatrix}, \quad B=\begin{pmatrix} 0 & 0 & \cdots & 0 & -B_n \\ 1 & 0 & \cdots & 0 & -B_{n-1} \\ 0 & 1 & \cdots & 0 & \vdots \\ 0 & 0 & \ddots & 0 & -B_2 \\ 0 & 0 & \cdots & 1 & -B_1 \end{pmatrix}.$$

Note that $H(\alpha,\beta)\subset \mathrm{GL}_n(\mathbb{Z})$ if the polynomials $P(z)$ and $Q(z)$ above factor as cyclotomic polynomials. Since we are interested in integral monodromy groups, we will assume this for the rest of the article. With the notation above, Beukers-Heckman show in [2] that $H=H(\alpha,\beta)$ falls into one of the following categories:

(0) A finite group (Beukers-Heckman list such cases completely in [2])
(1) If n is even, H is infinite, and $A_n/B_n=1$ then $H\subset \mathrm{Sp}_n(\mathbb{Z})$ and $\mathrm{Zcl}(H)=\mathrm{Sp}_n(\mathbb{C})$
(2) If n is odd and H is infinite; or if n is even, H is infinite, and $A_n/B_n=-1$, then $H\subset \mathrm{O}_{f_{\alpha,\beta}}(\mathbb{Z})$ for some quadratic form $f=f_{\alpha,\beta}$ in n variables and $\mathrm{Zcl}(H)=\mathrm{O}_f(\mathbb{C})$

In category (2) above we further consider two subcategories: one is that H fixes a quadratic form of signature $(n-1,1)$, and the other is that it fixes a quadratic form of signature (p,q) where $p,q>1$. We should mention that computing the corresponding signature in this case is easy given α,β: Beukers-Heckman show that if H is as in (2) above, H fixes a quadratic form of signature (p,q) where $p+q=n$ and

$$|p-q|=\left|\sum_{j=1}^{n}(-1)^{j+m_j}\right|$$

where $m_j=|\{k\mid \beta_k<\alpha_j\}|$ and the α_i and β_i are ordered as described at the beginning of this section. Our goal in the rest of this paper is to give a flavor of what can be said about the thinness of H in each of these three infinite cases. In the symplectic case, the best known method to detect thinness is to apply ping pong to show that the group is free. Outside of this one can also narrow down the given group to two possibilities: a thin group or a specific congruence subgroup of $\mathrm{Sp}_n(\mathbb{Z})$. In the orthogonal signature $(n-1,1)$ case, one has more tools at one's disposal since these groups act on hyperbolic space, and this well developed geometry often allows us to detect whether the given group is thin or not. Finally, although we lose these geometric tools in the orthogonal signature (p,q) case where $p,q>1$, there are ways to show thinness besides applying ping pong: in Section 3.3 we give an example of how one might do this in signature $(2,2)$.

3.1. **Symplectic Monodromy.** The question of whether $H=H(\alpha,\beta)$ is thin in the case that H is symplectic is perhaps the most elusive of the three scenarios outlined above. One method to answer this is to show that H is free (although it need not be in order to be thin) by applying the ping pong lemma: this has recently been done for a concrete example in [5]. However, the method in [5] is specific to the example treated there and it is not clear how to find the appropriate regions for applying ping pong to a general

group. Furthermore, in several cases we consider the group in question can be easily seen not to be free, in which case one must look elsewhere for a method to show thinness.

In ongoing work with Capdeboscq and Rivin, we have considered 14 examples of hypergeometric monodromy groups in $\mathrm{Sp}_4(\mathbb{Z})$ associated to Calabi Yau three-folds (these groups are in particular among the $H(\alpha, \beta)$'s we described above). Each of these groups is given via two generators, one of which is a transvection: these generators are derived in a paper of Chen-Yang-Yui in [8]. Notably, the authors of this work remark that they do not know whether these subgroups are lattices in Sp_4, and that two experts they have consulted on the matter have given them opposite conjectures: one asserts that the groups are probably all thin, while the other guesses that they must be finite index. We are inclined to agree with the former assessment of the situation, although we have made almost no progress in actually proving that any of the groups in [8] are thin.

Our belief that these groups are thin is based on a series of experiments which seem to imply that the number of elements in each of these groups of norm $\leq T$ is much too small for a finite-index subgroup of $\mathrm{Sp}_4(\mathbb{Z})$. We present the data from one of these experiments in Figure 2: this particular graph corresponds to the group $H = \langle A, B\rangle$ where

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 16 & 16 & 1 & 0 \\ 0 & -8 & -1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.1}$$

Specifically, the picture below is meant to depict the graph of $\log(N(T))$ versus $\log(T)$ where

$$N(T) = \#\{\gamma \in H \mid ||\gamma|| < T\}$$

with $||\cdot||$ as in (2.1). Because the graph of $\log(N(T))$ is only an approximation, we have denoted it by "$\log(N(T))$". The graph also depicts a linear fitting which has slope 1.396. The idea is that this slope is much too small for H to be finite index in $\mathrm{Sp}_4(\mathbb{Z})$: the same experiment for the full group $\mathrm{Sp}_4(\mathbb{Z})$ yields a graph of slope 6, and a finite index subgroup would have slope 6 as well.

Be that as it may, we have no way of ascertaining that the values of $N(T)$ which we found are actually correct, and so the graph above, while suggestive, is merely a guess. Specifically, since the only information we have about H is its generators, our method of counting elements of norm $< T$ is as follows: we consider walks on the generators of H and count the number of elements we find this way that have norm $< T$; eventually, once the length of the walk is long enough, all elements we find have norm $> T$ and we assume that we have found all elements of norm $< T$. However, it may be that there are many words of length 1000, say, whose norm is small and these words, if they exist, are not captured by our graph, so at this point this data cannot prove the thinness of H (which, by the way, may well be free: we have found no relations in its generators). We have produced similar graphs with small slope for many of the other examples in [8], all of which suggest thinness but are inconclusive for the same reason: we do not have a method, given only the generators of a subgroup of Sp_4, to decide whether a given element is in the group or not (in fact,

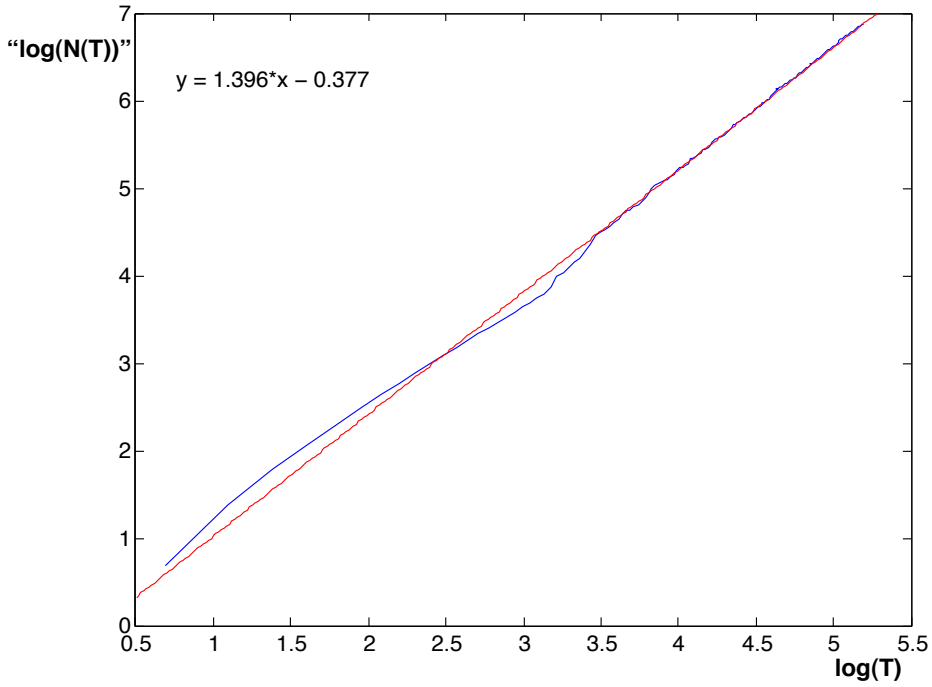

FIGURE 2. Counting elements in a symplectic monodromy group

this might be undecidable in general). This issue has hindered various other attempts to show that the groups in [8] are thin.

One can, however, use the fact that $\mathrm{Sp}_4(\mathbb{Z})$ has the congruence subgroup property to prove a dichotomy statement for each of the 14 groups H_i given in [8]: namely, each of these groups is either thin or is a congruence subgroup of $\mathrm{Sp}_4(\mathbb{Z})$. Furthermore, it is not difficult to determine for each H_i the precise candidate congruence subgroup. Because every one of these groups contains a transvection (the matrix B in (3.1) is a transvection and is always one of the generators), one can apply Theorem 3.1 of [17] to show that the projection of a given H_i in $\mathrm{Sp}_4(\mathbb{Z}/p\mathbb{Z})$ is surjective for all but a few explicit small primes. One can then use a computer to determine precisely the projection of H_i in $\mathrm{Sp}_4(\mathbb{Z}/p^k\mathbb{Z})$ for each of these small primes where k is a small positive integer (see [12] for a description of how one can deduce from this information what the projection is for higher powers of p), and consequently make explicit the candidate congruence subgroup for H_i.

Unfortunately, this does not bring us much closer to determining whether the groups H_i are thin: we come up against the same difficulty of deciding whether or not a given element in our candidate congruence subgroup is in the group or not.

3.2. **Orthogonal Monodromy: Signature** $(n-1,1)$**.** The case which is most straightforward to handle in some generality is the case that $H \subset \mathrm{O}(n-1,1)$. In [13], the (α,β) which give rise to $H(\alpha,\beta) \subset \mathrm{O}_f(\mathbb{Z})$

where f is a quadratic form in n variables with signature $(n-1,1)$ are described completely and are shown to belong to one of seven families outside of finitely many explicit cases in dimension $n \leq 7$. Using this description, the authors are able to write down the form f fixed by $H(\alpha,\beta)$ for in an infinite number of cases, as well as to produce infinite families of groups $H(\alpha,\beta)$ all of which are thin (we should note here that our group $H(\alpha,\beta) \subset \mathrm{O}(n-1,1)$ only when n is odd).

The strategy in doing this is to use the fact that in this case H is a group acting on hyperbolic space $\mathbb{H}^{n-1}$. As far as thinness goes, results of Nikulin, Vinberg and Prokhorov (see [24] for a discussion of these results) say that if n is large enough certain such groups must be thin. Specifically, let f be a quadratic form in n variables of signature $(n-1,1)$ and let $\mathrm{R}_f(\mathbb{Z})$ denote the subgroup of $\mathrm{O}_f(\mathbb{Z})$ which is generated by all of the reflections in hyperplanes in $\mathrm{O}_f(\mathbb{Z})$. Then Nikulin shows that for $n > 300$ the group $\mathrm{R}_f(\mathbb{Z})$ must be thin (Vinberg had proven a similar result on cocompact groups generated by reflections in hyperplanes, and Prokhorov had proven that for $n > 900$ the group $\mathrm{R}_f(\mathbb{Z})$ is thin).

In particular, if we could show that our groups $H(\alpha,\beta)$ contain finite index subgroups generated by reflections, this would imply that H is automatically thin once the dimension is large. However, in general we are not so lucky, and one has to work harder.

Namely, for $H = \langle A, B\rangle$ where A is of finite order k (it is often the case that one of the generators is of finite order), we first obtain a finite index subgroup H' of H as follows. Let $R_0 = A^{-1}B$, and let $R_i = A^{-i}R_0A^i$ for $1 \leq i \leq k-1$. Note that each R_i is a Cartan involution of $\mathbb{H}^{n-1}$, meaning that it fixes a point and reverses all geodesics around that point. One can show that the group

$$H' := \langle R_iR_{i+1} \,|0 \leq i \leq k-1\rangle$$

is of finite index in H. Furthermore, in [13] we give an algorithm which in infinitely many cases expresses each generator of H' as a product of reflections in hyperplanes, so $H' \subset R_f(\mathbb{Z})$ where f is the quadratic form fixed by H. Using the result of Nikulin above we then have that H', and therefore H is thin.

While there are infinitely many groups $H(\alpha,\beta)$ in this signature $(n-1,1)$ case which are still to be handled, it is conjectured that all but finitely many of these should be thin. The next step (after deciding thinness) is to clarify further the structure of these groups: for example, are they geometrically finite?

3.3. **Orthogonal Monodromy: the Split $(2,2)$ Case.** In the case that $H \subset \mathrm{O}(p,q)$ where $p,q > 1$ one cannot appeal to the tools from hyperbolic geometry as we described in the previous section. In fact, it is not currently clear how to attack the question of whether H is thin in this situation, and in most cases the problem is as difficult as in the symplectic case. However, given a concrete example where the signature is $(2,2)$ and the quadratic form has a perfect square determinant (we call this case split), one can rely on methods besides ping pong to decide thinness.

To demonstrate how one might tackle this problem, we consider the example $H = H(\alpha,\beta)$, where $\alpha = \{0,0,0,1/2\}$ and $\beta = \{1/4,1/4,3/4,3/4\}$ and show that it is in fact thin. We will do this in a fair amount of detail, since this computation, unlike the results discussed in the previous sections, is not

contained in any other paper. By Theorem 3.1, the generators of H are

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{3.2}$$

and $H \subset \mathrm{O}_Q(\mathbb{Z})$, where Q is

$$Q = \begin{pmatrix} 1 & 1 & -1 & -3 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ -3 & -1 & 1 & 1 \end{pmatrix},$$

of determinant 16 and signature $(2,2)$. We will now show the following.

Theorem 3.2. *The group $H = H(\alpha, \beta)$ as above is thin.*

To prove this, we use the spin homomorphism mapping $\mathrm{SL}_2 \times \mathrm{SL}_2$ onto the connected component of the identity in $\mathrm{SO}(2,2)$ which we explain momentarily. Note that this is analogous to the strategy used in [12] to study the congruence obstructions of the Apollonian group: in that case the spin homomorphism is a map from $\mathrm{SL}_2(\mathbb{C})$ to $\mathrm{SO}_{\mathbb{R}}(3,1)$. We wish to determine the preimage of $H \cap \mathrm{SO}_Q(\mathbb{Z})$ under this homomorphism (we will see that this intersection is indeed in the connected component of the identity). To this end, we have the following description of $H \cap \mathrm{SO}_Q(\mathbb{Z})$.

Claim 1: The group $H \cap \mathrm{SO}_Q(\mathbb{Z}) = \langle A^2, B \rangle$ where A, B are as in (3.2), and this group is of index 2 in H.

Proof. First note that, for any $n \in \mathbb{Z}$, we have $AB^nA \in \langle A^2, B \rangle$. Namely, since $A^{-1}BA^{-1}B = AB^{-1}AB^{-1} = B^{-1}AB^{-1}A = BA^{-1}BA^{-1} = I$, we have $h = A^2A^{-1}BA^{-1}BB^{-1} = ABA^{-1} \in \langle A^2, B \rangle$. Since $AB^nA = h^nA^2$, we have $AB^nA \in \langle A^2, B \rangle$ as desired. Any element of $H \cap \mathrm{SO}_Q(\mathbb{Z})$ can be written as a word

$$A^{n_1}B^{m_1}A^{n_2}B^{m_2}\cdots A^{n_s}B^{m_s} \tag{3.3}$$

for some $s \in \mathbb{N}$, $m_i, n_i \in \mathbb{Z}$ for $1 \leq i \leq s$, and $n_1 + n_2 + \cdots + n_s$ even since $\det(A) = -1$ and $\det(B) = 1$. We want to show that the word in (3.3) is in fact an element of $\langle A^2, B \rangle$.

If all of the exponents n_i for $1 \leq i \leq s$ are even, we are done. Suppose therefore that k is the smallest index for which n_k is odd. Then showing that the expression in (3.3) is in $\langle A^2, B \rangle$ is equivalent to showing

$$A^{n_k}B^{m_k}A^{n_{k+1}}B^{m_{k+1}}\cdots A^{n_s}B^{m_s} \in \langle A^2, B \rangle.$$

Suppose n_{k+1} is odd. Then for some $N, M \in \mathbb{Z}$, we have $A^{n_k}B^{m_k}A^{n_{k+1}} = A^{2M}AB^{m_k}AA^{2N} \in \langle A^2, B \rangle$, so wolog it suffices to show that

$$A^{n_\ell}B^{m_\ell}A^{n_{\ell+1}}B^{m_{\ell+1}}\cdots A^{\ell_s}B^{m_s} \in \langle A^2, B \rangle$$

where ℓ is the smallest index such that n_ℓ is odd and $n_{\ell+1}$ is even. Noting that $A^{n_\ell}B^{m_\ell}A^{n_{\ell+1}} = A^{2M}AB^{m_\ell}AA^{2N}A$ for some $N, M \in \mathbb{Z}$, this reduces to showing

$$AB^{m_{\ell+1}}A^{n_{\ell+2}}\cdots A^{\ell_s}B^{m_s} \in \langle A^2, B \rangle.$$

Continuing the reduction process using the fact that $B^K, A^{2K} \in \langle A^2, B\rangle$ for all $K \in \mathbb{Z}$ and $AB^N A \in \langle A^2, B\rangle$ for all $N \in \mathbb{Z}$, we reduce to either the identity I, in which case we are done, or to the element $AB^{m_s}A^{n_s}$ where n_s is even. But the latter case contradicts the assumption that $n_1 + n_2 + \cdots + n_s$ is even, so it does not occur.

Using again the relation $AB^{-1}AB^{-1} = I$ and applying similar arguments we have that there are only two cosets, $A\langle A^2, B\rangle$ and $I\langle A^2, B\rangle$ of $\langle A^2, B\rangle$ in H, so $[H : \langle A^2, B\rangle] = 2$ as desired. □

Claim 1 implies in particular that if $\langle A^2, B\rangle$ is thin then H is thin as well as stated in Theorem 3.2. Now note that Q is equivalent over $\mathbb{Q}$ to

$$Q' = C^T Q C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -4 \end{pmatrix} \text{ where } C = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and that $Q'(x_1, x_2, x_3, x_4) = 2x_2 \cdot 2x_3 - (2x_4 - x_1)(2x_4 + x_1)$ is the determinant of

$$M = \begin{pmatrix} 2x_2 & 2x_4 - x_1 \\ 2x_4 + x_1 & 2x_3 \end{pmatrix}.$$

The fact that one can bring Q to this form over $\mathbb{Q}$ makes this example particularly nice. Under this change of variables, $\langle A^2, B\rangle$ becomes $\langle A'^2, B'\rangle$ where

$$A'^2 = \begin{pmatrix} -1 & -2 & -8 & -8 \\ 0 & -1 & -4 & -4 \\ 1 & 0 & 3 & 2 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \quad B' = \begin{pmatrix} 1 & -2 & -2 & 4 \\ 1 & -1 & 0 & 2 \\ 0 & 1 & 1 & -2 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

We now define a map from $\rho : \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SO}_{Q'}$ as follows. Given a pair of elements g and h in SL_2, we have $\det(M) = \det(gMh^t)$, and in this sense a pair of elements in SL_2 fix Q'. As explained in Chapter 13.9 of [7], we map the pair $(g, h) \in \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ to an element $\gamma \in \mathrm{SO}_{Q'}(\mathbb{R})$ if

$$gMh^t = \begin{pmatrix} 2x'_2 & 2x'_4 - x'_1 \\ 2x'_4 + x'_1 & 2x'_3 \end{pmatrix},$$

where $(x'_1, x'_2, x'_3, x'_4)^t := \gamma(x_1, x_2, x_3, x_4)^t$. Given this, for each of our generators A'^2 and B above we solve for two matrices g, h in $\mathrm{SL}_2(\mathbb{R})$ which map to the generator. Note that there will not necessarily be a solution to this if one or both of the generators lie outside of the connected component of the identity. However, we are able to find solutions and we get that

$$\pm\left(\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ 2 & 3 \end{pmatrix}\right) \overset{\rho}{\longmapsto} A'^2 \tag{3.4}$$

and

$$\pm\left(\begin{pmatrix} -1 & -2 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}\right) \overset{\rho}{\longmapsto} B' \tag{3.5}$$

If we consider the projections of this group in each factor $\mathrm{SL}_2(\mathbb{Z})$, we obtain the groups Γ_1 and Γ_2, where

$$\Gamma_1 = \left\langle \pm \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} -1 & -2 \\ -1 & -1 \end{pmatrix} \right\rangle \; \Gamma_2 = \left\langle \pm \begin{pmatrix} -1 & -2 \\ 2 & 3 \end{pmatrix}, \pm \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \right\rangle.$$

One might hope that either Γ_1 or Γ_2 are of infinite index in $\mathrm{SL}_2(\mathbb{Z})$, as this would immediately imply that the preimage of $H \cap \mathrm{SO}_Q(\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ is also infinite index. Unfortunately, both Γ_1 and Γ_2 contain the finite index subgroup

$$\left\langle \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle$$

and so are both finite index. So we must work with the preimage itself and show the following, which together with Claim 1 immediately implies Theorem 3.2.

Proposition 3.3. *Let*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{3.6}$$

denote the generators of $SL_2(\mathbb{Z})$, with relations $S^2 = -I$ and $(ST)^3 = -I$. Let $G \subset \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ be the group generated by the elements in (3.4) and (3.5). Then for any integer $P \neq 0$ we have $(\pm T^P, \pm T^P) \notin G$, meaning in particular that the left cosets of this group under multiplication by $(\pm T^k, \pm T^k)$ where $k \in \mathbb{Z}$ are all distinct and that G is of infinite index in $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$.

Proof. We first note that the inverses of the generators of Γ in (3.4) and (3.5) are $\pm(T^{-2}, -ST^2S^{-1}T^2)$ and $\pm(TST^{-1}, ST^{-1}S)$ where S and T are as above, and we can rewrite this as

$$\Gamma = \langle \pm(-T^{-2}, T^2), \pm(TST^{-1}, ST^{-1}S) \rangle.$$

Ignoring for a moment the $\pm$, we denote by g_1 and g_2 the two generators above and suppose for contradiction that there is some integer $P \neq 0$ and some $\alpha, \beta \in \{\pm 1\}$ such that

$$(\alpha T^P, \beta T^P) = g_1^{m_1} g_2^{n_1} \cdots g_1^{m_s} g_2^{n_s} \tag{3.7}$$

where $m_i, n_i \in \mathbb{Z}$ and $n_i, m_i \neq 0$ for $i > 1$. Then in particular we have that

$$T^P = \pm T^{-2m_1} (TST^{-1})^{n_1} \cdots T^{-2m_s} (TST^{-1})^{n_s}. \tag{3.8}$$

Note furthermore that $(TST^{-1})^2 = -I$.

Let $n_{i_1}, n_{i_2}, \ldots, n_{i_k}$ denote the odd exponents among $n_1, n_2, \ldots, n_s$ with $i_1 < i_2 < \cdots < i_k$. Suppose $k > 0$ (i.e. there is at least one odd n_i). Then, given (3.8), there exist integers $M_1, M_2, \ldots, M_{k+1}$ with $|M_i| > 0$ for $1 < i < k+1$ such that

$$T^P = \pm T^{2M_1+1} S T^{2M_2} S T^{2M_3} \cdots S T^{2M_k} S T^{2M_{k+1}-1}. \tag{3.9}$$

We now consider two cases:

Case 1: $M_{k+1} \neq 0, 1$. In this case, (3.9) implies that

$$T^{P'} = \pm(ST^{2M_2})(ST^{2M_3})\cdots(ST^{2M_k})(ST^{2M_{k+1}-1})$$

where $P' = P - 2M_1 - 1$ and all powers of T on the right are > 1 in absolute value. In other words,

$$\begin{pmatrix} 1 & P' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & N_1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & N_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & -1 \\ 1 & N_k \end{pmatrix} \tag{3.10}$$

where $|N_i| > 1$ for all $1 \leq i \leq k$. We now need the following lemma.

Lemma 3.4. *Let* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an integer matrix with* $|b| > |a|$ *and* $|d| > |c|$. *Let* N *be an integer such that* $|N| > 1$. *Then we have that*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & N \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

where $|b'| > |a'| > |a|$ *and* $|d'| > |c'| > |c|$.

To prove this lemma, note that $a' = b$ and $b' = bN - a$. Since $|bN - a| \geq |bN| - |a| > 2|b| - |a| > |b|$ since $|b| > |a|$ we have the desired statement about b'. A similar argument shows that $|d'| > |c'| > |c|$ as well.

By the lemma, we have that the lower left entry of the expression on the right hand side of (3.10) cannot be 0, which contradicts (3.10).

Case 2: $M_{k+1} = 0$ or 1. First note that in this case the analog of (3.10) is that

$$\begin{pmatrix} 1 & P' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & N_1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & N_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & -1 \\ 1 & N_k \end{pmatrix} \tag{3.11}$$

where $|N_i| > 1$ for all $i < k$ and clearly we may assume $k > 1$. Again by the lemma, we have that

$$\begin{pmatrix} 0 & -1 \\ 1 & N_1 \end{pmatrix}\cdots\begin{pmatrix} 0 & -1 \\ 1 & N_{k-1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $c \neq 0$, $|b| > |a|$, and $|d| > |c|$. So in particular $d \neq 0$ and so the lower left entry of the expression on the right in (3.11) cannot be 0, contradictiong (3.11).

Thus our assumption that there exist odd exponents among the n_i in (3.7) was false, and so we have $n_i = 2n_i'$ for some $n_i' \in \mathbb{Z}$ for all i, and the sum of the exponents m_i must be $-P/2$ for (3.7) to hold. With this restriction on the n_i we now go to the first factor, where (3.7) implies that

$$T^P = \pm\gamma_2^{m_1}\gamma_1^{n_1'}\cdots\gamma_2^{m_s}\gamma_1^{n_s'}$$

where P is even and

$$\gamma_1 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \gamma_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Since $T^P = \gamma_2^{P/2}$ and $-I \notin \langle \gamma_1, \gamma_2 \rangle$, we have that in fact $T^P = \gamma_2^{m_1}\gamma_1^{n_1'} \cdots \gamma_2^{m_s}\gamma_1^{n_s'}$. This gives a nontrivial relation on γ_1 and γ_2 as long as one of the $n_i > 0$. But γ_1 and γ_2 generate a free subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and so we must have that $n_i = 0$ for all i, and that the sum of the exponents m_i is $P/2$ in order for (3.7) to hold. However, if $P \neq 0$ this contradicts the fact that the sum of the exponents m_i must be $-P/2$ from above and so our assumption that $(\pm T^P, \pm T^P) \in G$ for some $P \neq 0$ was false, and we are done. □

Therefore the group is of infinite index in $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, and so $H \cap \mathrm{SO}_Q(\mathbb{Z})$ is infinite index in $\mathrm{SO}_Q(\mathbb{Z})$ and in $\mathrm{O}_Q(\mathbb{Z})$. Since $(H : H \cap \mathrm{SO}_Q(\mathbb{Z})) = 2$ (see above), we have that H is thin as stated in Theorem 3.2.

References

[1] R. Aoun, *Random subgroups of linear groups are free*, Duke Math. J. **160**, pp. 117-173 (2011)

[2] F. Beukers, G. Heckman, *Monodromy for hypergeometric function ${}_nF_{n-1}$*, Invent. Math. **95**, pp. 325-354 (1989)

[3] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$*, Ann. of Math. **167**, pp. 625-642 (2008)

[4] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** No. 3, pp. 559-644 (2010)

[5] C. Brav, H. Thomas, *Classical and derived monodromy of the quintic threefold*, preprint at http://people.maths.ox.ac.uk/brav/monodromy.pdf

[6] E. Breuillard, B. Green, T. Tao, *Approximate subgroups of linear groups*, GAFA **21** No. 4, pp. 774-819 (2011)

[7] J.W.S. Cassels, *Rational Quadratic Forms*, Dover Publications, Inc., Mineola, NY (1978)

[8] Y-H. Chen, Y. Yang, N. Yui, *Monodromy of Picard-Fuchs differential equations for Calabi-Yau threefolds*, J. Reine Angew. Math. **616**, pp. 167-203 (2008)

[9] R. Descartes, *Euvres*, C. Adams and P. Tannery, eds. **4**, Paris (1901)

[10] J. Ellenberg, C. Hall, E. Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math. J. **161** No. 7, pp. 1233-1275 (2012)

[11] E. Fuchs, *Arithmetic properties of Apollonian circle packings*, Ph.D. thesis, Princeton University (2010)

[12] E. Fuchs, *Strong Approximation in the Apollonian group*, J. Number Theory **131**, pp. 2282-2302 (2011)

[13] E. Fuchs, C. Meiri, P. Sarnak, *Hyperbolic monodromy groups for the hypergeometric equation and Cartan involutions*, in preparation

[14] E. Fuchs, I. Rivin, *Subgroups of $SL_n(\mathbb{Z})$ are generically thin*, in preparation

[15] A. Gamburd, *Spectral gap for infinite index "congruence"' subgroups of $SL(2, \mathbb{Z})$*, Israel Jnl. of Math. **127**, pp. 157-200 (2002)

[16] R.L. Graham, J.C. Lagarias, C.L. Mallows, A.R. Wilks, C.H. Yan, *Apollonian circle packings: number theory*, J. Number Theory **100**, pp. 1-45 (2003)

[17] C. Hall, *Big symplectic or orthogonal monodromy modulo ℓ*, Duke Math. J. **141** No. 1, pp. 179-203 (2008)

[18] H. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$*, Ann. of Math. **167**, pp. 601-623 (2008)

[19] A. Kontorovich, H. Oh, *Apollonian circle packings and closed horospheres on hyperbolic 3-manifolds*, J. Amer. Math. Soc. **24**, pp. 603-648 (2011)

[20] A.H.M. Levelt, *Hypergeometric functions*, Thesis, University of Amsterdam (1961)

[21] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics **125**, Birkhäuser Verlag, Basel (1994)

[22] A. Lubotzky, *Expander graphs in pure and applied mathematics*, Bull. AMS **49**, pp. 113-162 (2012)

[23] G. Margulis, *Explicit constructions of expanders*, Problemy Peredaci Informacii **9** No. 4, pp. 71-80 (1973)

[24] V. Nikulin, *Discrete reflection groups in Lobachevsky spaces and algebraic surfaces*, Proceedings of the International Congress of Mathematicians **1** No. 2, Providence, RI, pp. 654-671 (1987)

[25] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*, preprint at arXiv.org:1001.4556

[26] I. Rivin, *Zariski Density and Genericity*, Int. Math. Res. Not. **19**, pp. 3649-3657 (2010)

[27] A. Salehi-Golsefidy, P. Sarnak, *Affine Sieve*, arXiv:1109.6432v1 (2011)

[28] A. Salehi-Golsefidy, P. Varju, *Expansion in perfect groups*, arXiv:1108.4900v2 (2011)

[29] P. Sarnak and X. Xue, *Bounds for multiplicities of automorphic representations*, Duke Math. J. **64**, pp.207-227 (1991)

[30] P. Varju, *Expansion in $SL_d(O_K/I)$, I square-free*, preprint at arXiv:1101.3664

[31] J-K. Yu, *Toward a proof of the Cohen-Lenstra conjecture in the function field case*, preprint (1995)

E-mail address: efuchs@math.berkeley.edu

Department of Mathematics, University of California, Berkeley CA