SMALL GENERATORS OF COCOMPACT ARITHMETIC FUCHSIAN GROUPS

MICHELLE CHU AND HAN LI

Abstract. In the study of Fuchsian groups, it is a nontrivial problem to determine a set of generators. Using a dynamical approach we construct for any cocompact arithmetic Fuchsian group a fundamental region in $SL_2(\mathbb{R})$ from which we determine a set of small generators.

1. Introduction

Arithmetic Fuchsian groups form a subclass of Fuchsian groups with a special connection to number theory and the theory of automorphic forms. These groups are necessarily of finite covolume and thus finitely generated. However, as with general Fuchsian groups, it is a nontrivial problem to determine a set of generators. One way to do this involves constructing a polygonal fundamental domain in $H^2$ and listing a set of generators corresponding to the side pairings of the polygon.

Johansson, Voight and Macasieb produced algorithms to determine fundamental-domains for some subclasses of arithmetic Fuchsian groups (see [7, 12, 17]).

We also note that Chinburg and Stover [5] obtain bounds for small generators of division algebras using lattice point methods. However, their generators are small in the division algebra and their representatives in $GL_n$ do not necessarily have small entries.

In this paper, we consider any cocompact arithmetic Fuchsian group and use dynamical techniques to construct a fundamental region in $SL_2(\mathbb{R})$ from which we determine a set of small generators. Our methods are reminiscent of methods used by Burger and Schroeder in [4] and in Page’s thesis (see [1, Chapter 2]).

Although each of our generators will be small, the number of generators could be quite large. Given a presentation, Voight gives an algorithm (which works for general finite covolume Fuchsian groups) to construct a new generating set with a minimal number of generators (see [17]).

1.1. Statement of Results. Let $G = SL_2(\mathbb{R})$ with a fixed Haar measure $\mu$, and $\Gamma$ be a cocompact arithmetic Fuchsian group (see subsection 2.1). Our main result gives a bound on norms of the generators in terms of the degree of the invariant trace field $k$, the volume of $G/\Gamma$, and the spectral gap of the Laplace-Beltrami operator on $H^2/\Gamma$.

Theorem 1.1. There exists a constant $C > 0$ depending only on the Haar measure $\mu$ and satisfying the following property. Let $\Gamma$ be a cocompact arithmetic Fuchsian group.
subgroup of $G$ with invariant trace field $k$. Then $\Gamma$ is generated by the finite subset

$$
\{ \gamma \in \Gamma : \|\gamma\| < C \cdot ([k : Q]^{\frac{1}{2} \sqrt{\lambda_1}}) \cdot \text{vol}_\mu(G/\Gamma)^{\frac{1}{2} \sqrt{\lambda_1}} \}
$$

Here $\text{vol}_\mu(G/\Gamma)$ is the covolume of $\Gamma$ with respect to the measure $\mu$, and $\lambda = \min\{\frac{1}{4}, \lambda_1(\Gamma)\}$ where $\lambda_1(\Gamma)$ is the smallest non-zero eigenvalue of the Laplace-Beltrami operator on $\mathbb{H}^2/\Gamma$.

Note that over a finite-dimensional space the choice of norm $\|\cdot\|$ does not matter. However, for completeness we take the $L^\infty$-norm. The coefficient $C$ in Theorem 1.1 can be explicitly calculated by following the methods of the proofs. Also, the result can be strengthened for certain families of arithmetic Fuchsian groups $\Gamma$, as we now describe.

Corollary 1.2. If $\Gamma$ is a cocompact congruence arithmetic Fuchsian group then it is generated by the finite subset

$$
\{ \gamma \in \Gamma : \|\gamma\| < C \cdot ([k : Q]^{\frac{1}{3} \log}) \cdot \text{vol}_\mu(G/\Gamma)^{\frac{1}{2} \sqrt{\lambda_1}} \}
$$

Corollary 1.3. If $\Gamma$ is torsion free cocompact arithmetic Fuchsian group then it is generated by the finite subset

$$
\{ \gamma \in \Gamma : \|\gamma\| < C \cdot (\log([k : Q]))^{\frac{1}{2} \sqrt{\lambda_1}} \cdot \text{vol}_\mu(G/\Gamma)^{\frac{1}{2} \sqrt{\lambda_1}} \}
$$

2. Arithmetic Fuchsian groups

We recall the definition and some properties of arithmetic Fuchsian groups.

2.1. Definition and properties. Let $k$ be a totally real number field and $A$ a quaternion algebra over $k$ ramified at all archimedean places except one. Let $R_k$ be the ring of integers in $k$, $O$ an $R_k$-order in $A$, and $O^1$ the elements of $A$-norm 1 in $O$. Let $\rho$ be a $k$-embedding of $A$ in $M_2(\mathbb{R})$, $2 \times 2$ matrices over $\mathbb{R}$. Then $\rho(O^1)$ is a Fuchsian group of finite covolume. By definition, a subgroup $\Gamma$ in $SL_2(\mathbb{R})$ is an arithmetic Fuchsian group if it is commensurable, up to conjugation, with some $\rho(O^1)$.

An arithmetic Fuchsian group $\Gamma$ is called a congruence subgroup if there is a maximal order $O$ and an integral 2-sided $O$-ideal $I$ of $O$ in $A$ such that $\Gamma$ contains $\rho(O^1(I))$ where $O^1(I) = \{a \in O^1 : a - 1 \in I\}$.

The field $k$ in the definition of an arithmetic Fuchsian group $\Gamma$ is a commensurability invariant and is recovered from $\Gamma$ by $k\Gamma = \mathbb{Q}(\text{tr}(\Gamma^{(2)}))$, where $\Gamma^{(2)}$ is the subgroup generated by the squares of elements in $\Gamma$. The number field $k\Gamma$ is the invariant trace field of $\Gamma$. The quaternion algebra is also recovered from $\Gamma$ by $A\Gamma = \{\sum a_i \gamma_i : a_i \in k, \gamma_i \in \Gamma^{(2)}\}$. For the remainder of the paper, we assume $\Gamma$ is cocompact. The group $\Gamma$ is cocompact when either $k \neq \mathbb{Q}$ or when $k = \mathbb{Q}$ and $A$ is a division algebra. We note also that for any $\gamma \in \Gamma$, $\text{tr}\gamma$ is an algebraic integer of degree at most 2 over $k\Gamma$.

For more on arithmetic Fuchsian groups, including proofs of the statements mentioned, the reader is referred to [13, Chapter 8].
2.2. Lehmer’s and Salem’s conjectures. The Mahler measure of an algebraic integer \( \theta \) is defined by
\[
M(\theta) = |a_0| \prod \max(1,|\theta_i|)
\]
where \( a_0 \) is the leading coefficient of the minimal polynomial for \( \theta \) over \( \mathbb{Z} \) and \( \theta_i \) ranges over the algebraic conjugates of \( \theta \).

In 1933 Lehmer posed the following conjecture:

**Conjecture 2.1.** [11] There exists a universal lower bound \( m > 1 \) such that \( M(\theta) \geq m \) for all \( \theta \) which are not roots of unity.

A Salem number is a real algebraic integer \( \theta > 1 \) such that \( \theta - 1 \) is a conjugate and all other conjugates lie on the unit circle. For Salem numbers, Lehmer’s conjecture restricts to the Salem conjecture.

**Conjecture 2.2.** There exists \( m_S > 1 \) such that if \( \theta \) is a Salem number then \( M(\theta) \geq m_S \).

The Salem conjecture is equivalent to the short geodesic conjecture of arithmetic 2-manifolds, which states that there is a universal lower bound for translation length for hyperbolic elements in arithmetic Fuchsian groups (see [15]). Assuming the Salem conjecture, the bounds in Theorem 1.1 can be modified to depend only on the covolume and the spectral gap whenever the group \( \Gamma \) contains no elliptic elements.

**Corollary 2.3.** If the Salem conjecture is true and \( \Gamma \) is a torsion free, cocompact, arithmetic Fuchsian subgroup of \( G \). Then \( \Gamma \) is generated by the finite subset
\[
\{ \gamma \in \Gamma : \|\gamma\| < C \cdot \left( \frac{\log(m_S)}{\log(2d)} \right)^{3/2} \}
\].

3. Preparation

3.1. Injectivity radius. Throughout this section, let \( d \) be the degree of the the invariant trace field of \( \Gamma \).

**Lemma 3.1.** Let \( \Gamma \) be a cocompact arithmetic Fuchsian group with invariant trace field of degree \( d \) and let
\[
W_d = \left\{ g \in G : 2 \cos \left( \frac{\pi}{2d} \right) < |\text{tr}(g)| < 2 \cosh \left( \frac{1}{16} \left( \frac{\log(\log(2d))}{\log(2d)} \right)^{3/2} \right) \right\}
\].

Then for any \( g \in G, g\Gamma g^{-1} \cap W_d = \{1\} \).

**Proof.** By the cocompactness condition, we consider only hyperbolic and elliptic elements in \( \Gamma \).

If \( \gamma \) is hyperbolic then also \( \gamma^2 \) is hyperbolic, with \( |\text{tr}(\gamma^2)| > 2 \) and \( \text{tr}(\gamma^2) \in k\Gamma \). Let \( u_\gamma \) be the root of the characteristic polynomial \( x^2 - \text{tr}(\gamma)x + 1 \) of \( \gamma \) which lies outside the unit circle (respectively, let \( u_{\gamma^2} \) be the root of the characteristic polynomial \( x^2 - \text{tr}(\gamma^2)x + 1 \) of \( \gamma^2 \) outside the unit circle). We have \( u_{\gamma^2} \) real and exactly two of its algebraic conjugates lie off the unit circle, namely \( u_{\gamma^2} \) and \( u_{\gamma^2}^{-1} \) (see e.g. [13, Lemma 12.3.1]). Therefore, \( \log M(u_{\gamma^2}) = \log |u_{\gamma^2}| = 2 \log |u_\gamma| \) where \( M(u_{\gamma^2}) \) is the Mahler measure (see equation 2.1). As a hyperbolic element, \( \gamma \) acts on the hyperbolic plane by translating along its invariant axis a distance of \( 2 \log |u_\gamma| \). It then follows that \( |\text{tr}(\gamma)| = 2 \cosh \left( \frac{1}{4} \log M(u_{\gamma^2}) \right) \) (see e.g. [13] Lemma...
Since \( u_{x, z} \) lies in an extension of degree 2 over \( k\Gamma \), it has algebraic degree bounded above by \( 2d \). We now apply the main theorem of [18] which states that any algebraic integer \( \theta \) of degree at most 2 has

\[
\log M(\theta) > \frac{1}{4} \left( \log(\log(2d)) \right)^3
\]

to get the following bound for the trace of a hyperbolic \( \gamma \in \Gamma \)

\[
|\text{tr}(g)| > 2 \cosh \left( \frac{1}{16} \left( \log(\log(2d)) \right)^3 \right).
\]

If \( \gamma \) is elliptic then by the discreteness of \( \Gamma \), \( \gamma \) has order \( m \) and thus eigenvalues \( \omega \) and \( \omega^{-1} \) with \( |\omega + \omega^{-1}| = |\text{tr}(\gamma)| < 2 \) and such that \( \omega \) is a primitive \( 2m \)-th root of unity. Since \( \text{tr}(\gamma) \) lies in a field of degree at most 2 over \( k\Gamma \), \( (\omega + \omega^{-1}) \) has algebraic degree of at most \( 2d \), or equivalently, \( \omega \) has algebraic degree of at most \( 4d \). Then \( |\text{tr}(\gamma)| = |u_\gamma + u_{\gamma}^{-1}| \) is bounded above by \( |e^{\pi d} + e^{-\pi d}| = 2 \cosh(\pi). \)

Take \( W_d \) as in [equation 3.1]. Since the trace is invariant under conjugation, for any \( g \in G \) we have \( g \Gamma g^{-1} \cap W_d = \{1\}. \)

The injectivity radius of \( G/\Gamma \) at a point \( x = h\Gamma \in G/\Gamma \) is related to the distance between the identity element and the nearest point in the lattice \( h\Gamma h^{-1} \). Since the trace of a matrix is invariant under conjugation, the bounds in [Lemma 3.1] for the traces of elements in any conjugate of \( \Gamma \) determine an injectivity radius for \( G/\Gamma \).

For any \( \eta > 0 \) denote the ball of radius \( \eta \) centered at the identity \( 1 \in G \) by

\[
B_G(\eta) = \{ g \in G : \| g - 1 \| < \eta \}.
\]

**Lemma 3.2.** There exists \( \delta = \delta(d) = cd^{-2} > 0 \) with \( c \) depending only on the Haar measure \( \mu \), such that the map \( B_G(\delta) \rightarrow G/\Gamma \) given by \( g \mapsto g.x \) is injective for any \( x \in G/\Gamma \).

**Proof.** Let

\[
\delta_0 = \min \left\{ \cosh \left( \frac{1}{16} \left( \log(\log(2d)) \right)^3 \right), 1, 1 - \cos \left( \frac{\pi}{2d} \right) \right\}.
\]

Then for any \( 0 < \delta_1 < \delta_0 \) and \( g \in B_G(\delta_1) \),

\[
|g_{1, 1} - 1| < \delta_1 \quad \text{and} \quad |g_{2, 2} - 1| < \delta_1,
\]

where \( g_{1, 1} \) and \( g_{2, 2} \) are the \((1, 1)\) and \((2, 2)\) matrix entries of \( g \). Then \( |\text{tr}(g) - 2| < 2\delta_1 \) and \( g \in W_d \).

By the Taylor series expansion of \( 1 - \cos(\pi/2d) \),

\[
1 - \cos \left( \frac{\pi}{2d} \right) \approx \frac{\pi^2}{8d^2} - \frac{\pi^4}{384d^4}.
\]

Since \( 1 - \cos(\pi/2d) \) goes to 0 at a faster rate than \( \left( \frac{1}{16} \left( \log(\log(2d)) \right)^3 \right) - 1 \) goes to 0, there exists a positive constant \( c \) depending only on the measure \( \mu \) such that \( \delta(d) := c \cdot d^{-2} < \delta_0 \) and such that for all \( g_1, g_2 \in B_G(\delta) \), we have \( g_1^{-1} g_2 \in B_G(\delta_0) \).

For any \( x = h\Gamma \in G/\Gamma \), if \( g_1, g_2 \in B_G(\delta) \) and \( g_1.x = g_2.x \) then \( g_1^{-1} g_2 \in h\Gamma h^{-1} \). Hence \( g_1^{-1} g_2 \in W_d \) and by [Lemma 3.1] it must be that \( g_1 = g_2. \)
Remark 3.3. When $\Gamma$ is torsion free, only the traces of hyperbolic elements are relevant. In this case the constant $\delta(d)$ in Lemma 3.2 can be improved to $e^{\left(\log\log(2d)\right)^6}$.

For a cleaner statement, we use the estimate $\log(d) - 4 \ll \left(\log\log(2d)\right)^6$.

If the Salem conjecture is true, there is a universal lower bound for the trace of a hyperbolic element in an arithmetic Fuchsian group. Then for $m_s$ the lower bound satisfying the Salem conjecture, the constant $\delta$ can be improved to $c\log^2(m_s)$ for all torsion free $\Gamma$. In particular, this constant would be independent of $d$.

3.2. Spectral gap. Let $\Gamma$ be a cocompact Fuchsian group acting on the hyperbolic plane $\mathbb{H}^2$ from the right. Let $\lambda_1(\Gamma)$ be the first non-zero eigenvalue of the Laplacian operator on the locally symmetric space $\mathbb{H}^2/\Gamma$. Denote by $\lambda = \lambda(\Gamma) := \min\{\frac{1}{4}, \lambda_1(\Gamma)\}$. Let

$$\alpha_t = \begin{pmatrix} e^t & 0 \\ 0 & e^{-\frac{t}{2}} \end{pmatrix} \in \text{SL}_2(\mathbb{R}), \quad \mathcal{D} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \text{sl}_2(\mathbb{R}).$$

Denote by $\mu_{G/\Gamma}$ the $G$-invariant probability measure supported on $G/\Gamma$ for which, whenever $X \subset G/\Gamma$ is a measurable set, we have that the volume $\text{vol}_\mu(X) = \text{vol}_\mu(G/\Gamma) \cdot \text{vol}_{G/\Gamma}(X)$.

Lemma 3.4. Let $\Gamma$ be a cocompact lattice in $G$. Then for any smooth functions $\varphi$, $\psi$ in $L^2_0(G/\Gamma) = \{f \in L^2(G/\Gamma) : \int f d\mu_{G/\Gamma} = 0\}$ it holds

$$|\langle \alpha_t, \varphi, \psi \rangle| \ll (e^{-t/3})^{1-\sqrt{\lambda}} \cdot \|D, \varphi\| \cdot \|D, \psi\|.$$

Proof. This lemma follows from work of Ratner in [16] but is given explicitly in [14, Corollary 2.1] and with explicit constant. We use the estimate $t(e^{-t/2}) \ll (e^{-t/3})$ for a cleaner statement.

3.3. Translates. Given any two points in the $G/\Gamma$, some element $h \in G$ will translate one to the other. We use the injectivity radius, the spectral gap, and the covolume to give an upper bound on the norm of some such element $h$.

Theorem 3.5. For any $g_1 \Gamma, g_2 \Gamma \in G/\Gamma$ there is some $h \in G$ and positive number $c$ such that $h g_1 \Gamma = g_2 \Gamma$ and

$$\|h\| < c \cdot \text{vol}_\mu(G/\Gamma)^{1-\frac{3}{1-\delta}} \cdot \delta^{\frac{1 IS}{\lambda}}.$$

where $\delta$ is in Lemma 3.2 and $\lambda$ is as in subsection 3.3.

Proof. Let $\varphi$ and $\psi$ be nonnegative, smooth bump functions supported in $B_G(\delta), g_1 \Gamma$ and $B_G(\delta), g_2 \Gamma$ respectively, and satisfying

$$\mu_{G/\Gamma}(\varphi) = \mu_{G/\Gamma}(\psi) = \text{vol}_\mu(G/\Gamma)^{-1}, \quad \|D, \varphi\|, \|D, \psi\| \ll \text{vol}_\mu(G/\Gamma)^{-\frac{1}{2}} \cdot \delta^{-\frac{5}{6}}.$$

These functions can be constructed as in [10, Lemma 2.4.7]. Applying Lemma 3.4 to the functions $\varphi - \mu_{G/\Gamma}(\varphi)$ and $\psi - \mu_{G/\Gamma}(\psi)$, we get

$$\|\langle \alpha_t, \varphi, \psi \rangle - \mu_{G/\Gamma}(\varphi) \cdot \mu_{G/\Gamma}(\psi)\| \ll (e^{-t/3})^{1-\sqrt{\lambda}} \cdot \|D, \varphi\| \cdot \|D, \psi\|.$$

Then for $t > 0$ such that

$$\|\alpha_t\| \leq e^t \ll \text{vol}_\mu(G/\Gamma)^{1-\frac{3}{1-\delta}} \cdot \delta^{-\frac{15}{2}}.$$


we must have $\langle \alpha_t, \varphi, \psi \rangle \neq 0$, since $\mu_{\Gamma} \cdot \mu_{\Gamma} \psi$ will dominate the error term in equation 3.10. Therefore, the set

$$(\alpha_t.\text{supp}(\varphi) \cap \text{supp}(\psi)) \subset (\alpha_t.(B_G(\delta).g_1 \Gamma) \cap (B_G(\delta).g_2 \Gamma))$$

is not empty. There is some $h \in B_G(\delta)^{-1}.\alpha_t.B_G(\delta)$ for which $h.g_1 \Gamma = g_2 \Gamma$. □

4. PROOF OF RESULTS AND CONCLUDING REMARKS

Proof of Theorem 1.1 Define the set

$$(4.1) \quad \mathcal{U} = \left\{ h \in G : \|h\| \leq \text{vol}_\mu(G/\Gamma)^{\frac{3}{5}} \cdot \delta^{\frac{-15}{16}} \right\}.$$ 

By Theorem 3.5 for any $g \in G$, there is some $h \in \mathcal{U}$ such that $h.\Gamma = g.\Gamma$. That is, we can write $g$ as $h\gamma$ for some $\gamma \in \Gamma$. Therefore, we have constructed an open set $\mathcal{U} \subset G$ such that $\mathcal{U} \Gamma = G$. It follows that $\{ \gamma \in \Gamma : \mathcal{U} \cdot \gamma \cap \mathcal{U} \neq \emptyset \}$ generates $\Gamma$ (see e.g. [3, Lemma 6.6]). Then $\Gamma$ is generated by the bigger set $\mathcal{U}^{-1}\mathcal{U} \cap \Gamma$, whose elements have norm bounded above by $\text{vol}_\mu(G/\Gamma)^{\frac{3}{5}} \cdot \delta^{\frac{-15}{16}}$.

The proof of Theorem 1.1 then follows by replacing $\delta$ with $c[k : \mathbb{Q}]^{-2}$, as given in Lemma 3.2 (where $d = [k : \mathbb{Q}]$. □

Proof of Corollary 1.2 The proof of Corollary 1.2 follows from the well-known result that

$$(4.2) \quad \lambda_1(\Gamma) \geq 975/4096$$

for every congruence arithmetic Fuchsian group. For the sake of reader’s convenience, we shall briefly explain equation 4.2 in the case when $k \Gamma = \mathbb{Q}$.

By the Jacquet-Langlands correspondence (see [6, Chapter 16]), if $\Gamma$ is a congruence arithmetic Fuchsian group with $k \Gamma = \mathbb{Q}$ then $\lambda_1(\Gamma) \geq \inf\{\lambda_1(\Lambda(N)) : N \in \mathbb{N}\}$, where $\Lambda(N) = \{ \gamma \in \text{SL}_2(\mathbb{Z}) : \gamma \equiv 1 \text{ mod } N \}$. As of this writing we have the estimate, which is due to Kim-Sarnark [9],

$$(4.3) \quad \inf\{\lambda_1(\Lambda(N)) : N \in \mathbb{N}\} \geq 975/4096.$$ 

We note that, for the case when $k \Gamma$ is a number field, equation 4.2 follows from the Jacquet-Langlands correspondence together with the bounds on the Ramanujan conjecture over number fields (see [2]). □

Proof of Corollary 1.3 and Corollary 2.3 The proof of Corollary 1.3 follows from the proof of Theorem 1.1 by replacing $\delta$ with $c \log(d)^{-4}$ as in Remark 3.3. Furthermore, if we assume the Salem conjecture is true, then Corollary 2.3 will follow by setting $\delta = c \log^2(m_S)$ as in Remark 3.3. □

Remark 4.1. The arguments in the proof of Theorem 1.1 can be modified to give a similar result for cocompact arithmetic Kleinian groups. All lemmas will go through except that one would need an analogue of Lemma 3.4. An analogue of Lemma 3.4 (or [14, Corollary 2.1]) does hold. However, more work would need to be done to get an explicit rate of the decay of correlations for functions on $\text{SL}_2(\mathbb{C})/\Gamma$, from the $\lambda_1$ of the corresponding hyperbolic 3-manifold $SU(2) \backslash \text{SL}_2(\mathbb{C})/\Gamma$. At this time, we are not aware of such a statement in the current literature.
5. Acknowledgements

The authors thank Alan W. Reid for helpful discussions and suggestions and Gregory A. Margulis for the techniques in his upcoming joint work with the second author. They also thank John Voight for helpful comments and for pointing out the results in [1]. Finally, the authors would like to thank the referee for being incredibly thorough and for helpful comments and suggestions that improved the quality of this paper and the clarity of the arguments.

References


Department of Mathematics, University of Texas at Austin, Austin, TX 78750, USA
E-mail address: mchu@math.utexas.edu

Department of Mathematics and Computer Sciences, Wesleyan University, Middletown, CT 06457, USA
E-mail address: hli03@wesleyan.edu