COUNTING ARITHMETIC LATTICES AND SURFACES

MIKHAIL BELOLIPETSKY, TSACHIK GELANDER, ALEX LUBOTZKY, AND ANER SHALEV

Abstract. We give estimates on the number $\mathrm{AL}_H(x)$ of conjugacy classes of arithmetic lattices Γ of covolume at most x in a simple Lie group H. In particular, we obtain a first concrete estimate on the number of arithmetic 3-manifolds of volume at most x. Our main result is for the classical case $H = \mathrm{PSL}(2, \mathbb{R})$ where we show that

$$\lim_{x\to\infty} \frac{\log \mathrm{AL}_H(x)}{x \log x} = \frac{1}{2\pi}.$$

The proofs use several different techniques: geometric (bounding the number of generators of Γ as a function of its covolume), number theoretic (bounding the number of maximal such Γ) and sharp estimates on the character values of the symmetric groups (to bound the subgroup growth of Γ).

1. Introduction

Let H be a noncompact simple Lie group with a fixed Haar measure μ. A discrete subgroup Γ of H is called a lattice if $\mu(\Gamma\backslash H) < \infty$. A classical theorem of Wang [Wa] asserts that if H is not locally isomorphic to $\mathrm{PSL}_2(\mathbb{R})$ or $\mathrm{PSL}_2(\mathbb{C})$, then for every $0 < x \in \mathbb{R}$ the number $\mathrm{L}_H(x)$ of conjugacy classes of lattices in H of covolume at most x is finite. This result was greatly extended by Borel and Prasad [BP]. In recent years there has been an attempt to quantify Wang's theorem and to give some estimates on $\mathrm{L}_H(x)$ (see [BGLM, Ge1, GLNP, Be, BL]).

If $H = \mathrm{PSL}_2(\mathbb{R})$ or $\mathrm{PSL}_2(\mathbb{C})$, then $\mathrm{L}_H(x)$ is usually not finite (and even uncountable in the first case). Still Borel [Bo] showed that the number $\mathrm{AL}_H(x)$ of conjugacy classes of *arithmetic* lattices in H of covolume at most x is finite for every $x \in \mathbb{R}$.

In this paper we study the asymptotic behavior of $\mathrm{AL}_H(x)$ when $x \to \infty$. Our first result gives a general upper bound.

Theorem 1.1. *Assume that H is of real rank one. There exists a constant $b = b(H, \mu)$ such that $\mathrm{AL}_H(x) \le x^{bx}$ for all $x \gg 0$.*

Theorem 1.1 is also true if the rank of H is greater than one, see Remark 5.1 below and [Ge2], but for most higher rank groups much better estimates are given in [BL]. Our next result shows that Theorem 1.1 is best possible in general.

Theorem 1.2. *For $H = \mathrm{PSO}(n, 1)$ there exists a constant $a = a(n) > 0$ such that $\mathrm{AL}_H(x) \ge x^{ax}$ for all $x \gg 0$.*

Date: April 21, 2010.

The authors acknowledge support from the BSF, ISF, EPSRC and ERC, and the valuable comments and corrections of the anonymous referee.

One novelty of the current work compared to [BGLM] and [Ge1] is that it deals with orbifolds rather than manifolds, i.e. we do not require the lattices to be torsion free. However, it is clear from the proof that the lower bound remains valid when restricting only to conjugacy classes of arithmetic *torsion free* lattices. Another novelty is that it covers the case of $H = \mathrm{PSO}(3,1) = \mathrm{Isom}(\mathbb{H}^3)$, for which the result translates to: *the number of arithmetic hyperbolic* 3 *orbifolds (or manifolds) of volume at most x is roughly x^{cx} for large x.* Prior to this work no explicit upper bound was known in this case, as well as for the case $H = \mathrm{PSO}(2,1)$. The upper bound obtained here confirms the expected estimate which follows from the Lehmer conjecture concerning algebraic integers (cf. [Ge1]).

The proofs of Theorems 1.1 and 1.2 allow one to compute concrete constants, but in general it seems very difficult to obtain sharp estimates for these constants. The main part of this paper is dedicated to the classical case $H = \mathrm{SO}(2,1)^\circ \cong \mathrm{PSL}_2(\mathbb{R})$ where we obtain a very sharp estimate:

Theorem 1.3. *Let $H = \mathrm{PSL}_2(\mathbb{R})$ endowed with the Haar measure induced from the Riemanian measure of the hyperbolic plane $\mathbb{H}^2 = \mathrm{PSL}_2(\mathbb{R})/\mathrm{PSO}(2)$. Then*

$$\lim_{x\to\infty} \frac{\log \mathrm{AL}_H(x)}{x \log x} = \frac{1}{2\pi}.$$

The proof of Theorem 1.3 shows:

Corollary 1.4. *Let $\mathrm{AS}(g)$ be the number of arithmetic Riemann surfaces of genus g. Then*

$$\lim_{g\to\infty} \frac{\log \mathrm{AS}(g)}{g \log g} = 2.$$

Let us now describe the main ingredients of the proofs. We start with a result on the number $d(\Gamma)$ of generators of lattices Γ, which is of independent interest.

Theorem 1.5. *Let H be a connected simple Lie group of real rank one. Then there is an effectively computable constant $C = C(H)$ such that for any lattice $\Gamma < H$ we have $d(\Gamma) \le C \cdot \mathrm{vol}(\Gamma\backslash H)$.*

The proof of Theorem 1.5 is geometric and valid for all lattices, not necessarily arithmetic. Note that Theorem 1.5 implies the celebrated Kazhdan–Margulis theorem [KM] asserting that there is a common lower bound on the covolumes of all lattices in H. Indeed, $d(\Gamma) \ge 2 \Rightarrow \mathrm{vol}(\Gamma\backslash H) \ge \frac{2}{C}$. It also has several other applications, for instance, it gives a linear bound on the first Betti number of orbifolds in terms of their volume (cf. [FGT] and see Remark 2.7 below and [Ge2]).

Another essential component in our proofs is the following.

Theorem 1.6. *Let $\mathrm{MAL}^u_H(x)$ (resp. $\mathrm{MAL}^{nu}_H(x)$) denote the number of conjugacy classes of maximal uniform (resp. non-uniform) irreducible arithmetic lattices of covolume at most x in $H = \mathrm{PGL}_2(\mathbb{R})^a \times \mathrm{PGL}_2(\mathbb{C})^b$. Then:*

(i) *There exists a positive constant $\alpha = \alpha(a,b)$, and for every $\epsilon > 0$ a positive constant $\beta = \beta(\epsilon, a, b)$, such that*

$$x^\alpha \le \mathrm{MAL}^u_H(x) \le x^{\beta(\log x)^\epsilon}, \text{ for } x \gg 0.$$

(ii) *There exist positive constants $\alpha' = \alpha'(a,b)$ and $\beta' = \beta'(a,b)$ such that*

$$x^{\alpha'} \le \mathrm{MAL}^{nu}_H(x) \le x^{\beta'}, \text{ for } x \gg 0.$$

Some yet unproved number-theoretic conjectures imply that a polynomial upper bound is true also in the first case (see [Be]).

Theorem 1.6 was proved in [Be] for higher absolute rank groups but the cases of $\mathrm{PSL}_2(\mathbb{R})$ and $\mathrm{PSL}_2(\mathbb{C})$ which are the most crucial for us were left open; in particular, Theorem 1.6 answers a question from [Be].

The general strategy of the proof of Theorem 1.6 is similar to [Be] but some special considerations are needed for small rank. (Note that in [Be] the proof is easier for very high rank - see Proposition 3.3 there). The seminal work of Borel [Bo] which gives a detailed description of the maximal arithmetic lattices in $\mathrm{PGL}_2(\mathbb{R})^a \times \mathrm{PGL}_2(\mathbb{C})^b$ combined with some ideas of Chinburg and Friedman [CF] enables us to prove it. Various number theoretic estimates are needed along the way.

The fact that the number of maximal arithmetic lattices grows slowly reduces the problem to the subgroup growth of a given such maximal lattice Γ.

Recall now that for any finitely generated group Γ, we have $s_n(\Gamma) \leq (n!)^{d(\Gamma)}$, where $s_n(\Gamma)$ denotes the number of subgroups of index at most n in Γ. This, combined with Theorems 1.5 and 1.6, proves Theorem 1.1. The proof of the precise bound in Theorem 1.3 requires more.

For $\mathrm{PSL}_2(\mathbb{R})$ the "miracle" is that the covolume of Γ and the subgroup growth of Γ are both controlled by $\chi(\Gamma)$ – the Euler characteristic of Γ. The covolume is $-2\pi\chi(\Gamma)$ by the Gauss-Bonnet formula, and the number $s_n(\Gamma)$ of subgroups of index at most n in Γ is $n^{(-\chi(\Gamma)+o(1))n}$, as was proved by Liebeck and Shalev [LiSh]. Thus the contribution of Γ to $\mathrm{AL}_H(x)$ is roughly

$$s_{\frac{x}{-2\pi\chi(\Gamma)}}(\Gamma) = \left(\frac{x}{-2\pi\chi(\Gamma)}\right)^{(-\chi(\Gamma)\frac{1}{-2\pi\chi(\Gamma)}+o(1))x} = x^{(\frac{1}{2\pi}+o(1))x},$$

which, on the face of it, proves Theorem 1.3. However, there is a delicate point here: the behavior of the error term $o(1)$ above depends on Γ. This can be a serious problem: the issue is illustrated in [BL] where it is shown, in contrary to a conjecture from [BGLM] and [GLNP], that for high rank Lie groups the growth of the total number of arithmetic lattices is strictly faster than those arising from finite index subgroups of a given lattice. Our next result yields a uniform bound on the subgroup growth of Fuchsian groups and overcomes this difficulty:

Theorem 1.7. *There exists an absolute constant c such that for every Fuchsian group Γ and for every $n \in \mathbb{N}$ we have*

$$s_n(\Gamma) \leq (cn)^{-\chi(\Gamma)n}.$$

The proof is a modification of the one given in [LiSh], it relies heavily on bounds for the character values of symmetric groups.

Theorems 1.6 and 1.7 imply the upper bound in Theorem 1.3 (see Section 5). The lower bounds in Theorems 1.2 and 1.3 are proved by analyzing the subgroup growth of specific lattices. There is one delicate point which has to be considered here: finite index subgroups of Γ may be conjugate in H without being conjugate in Γ. An argument which uses the congruence topology of Γ solves this problem and provides the lower bounds in all cases (see Section 5).

Note added in proof: Recently A. Eisenmann [E] proved an analogous result for $H = \mathrm{PSL}_2(k)$, where k is a p-adic field. His result says that if k does not contain $\zeta + \zeta^{-1}$ (where ζ is the p'th root of unity) then $\lim \frac{\mathrm{AL}_H(x)}{x \log x} = q - 1$, where q is the order of the residue field of k (here μ is normalized to give value 1 for the maximal compact subgroup of H.)

2. On the number of generators of a lattice

In this section we give a proof of Theorem 1.5. Since the center of H is finitely generated, replacing H by its adjoint group we may assume it is center free. We will assume below that H is not locally isomorphic to $\mathrm{PSL}_2(\mathbb{R})$. For $H = \mathrm{PSL}_2(\mathbb{R})$ the theorem follows easily from the Gauss–Bonnet formula and the explicit presentation of lattices there (cf. Section 4).

Let $K < H$ be a maximal compact subgroup and $X = H/K$ the associated rank 1 Riemanian symmetric space. Then H is a connected component of the group of isometries of X, and by our assumption $\dim X \geq 3$. For $g \in H,\ x \in X$ we denote by

$$d_g(x) = d(x, g \cdot x)$$

the displacement of g at x, and by

$$\mathrm{Min}(g) := \{x \in X : d_g(x) = \inf(d_g)\}$$

the (possibly empty) set where d_g attains its infimum. Recall that there are 3 types of isometries g of X:

- g is *elliptic* if it has a fixed point in X. In this case the set of fixed points $\mathrm{Fix}(g) = \mathrm{Min}(g)$ is a totally geodesic submanifold.
- g is *hyperbolic* if $\mathrm{Min}(g) \neq \emptyset$ but $\mathrm{Fix}(g) = \emptyset$. In this case $\mathrm{Min}(g)$ is an infinite two sided geodesic, it is called the *axis* of g.
- g is *parabolic* if $\mathrm{Min}(g) = \emptyset$. In this case g has a unique fixed point p at the visual boundary ∂X of X, $\inf(d_g) = 0$ and a geodesic $c : \mathbb{R} \to X$ satisfies $c(\infty) = p$ if and only if $\lim_{t\to\infty} d_g(c(t)) = 0$.

Moreover, if $g_1, \ldots, g_k \in H$ are commuting elements which are simultaneously elliptic (resp. hyperbolic, resp. parabolic), then they have a common fixed point (resp. axis, resp. fixed point at ∂X).

Recall the classical Margulis lemma (cf. [Th, Chapter 4]):

Lemma 2.1. *There is a constant $\epsilon_H > 0$, depending on H, such that if $\Lambda < H$ is a discrete group generated by $\{\gamma \in \Lambda : d_\gamma(x) \leq \epsilon_H\}$ for some $x \in X$, then Λ virtually nilpotent.*

Fix once and for all

$$\epsilon \leq \min\{\frac{\epsilon_H}{10}, 1\}.$$

Let Γ be a lattice in H. Denote by $M = \Gamma\backslash X$ the corresponding orbifold, and by $\pi : X \to M$ the canonical (ramified) covering map. For a subset $Y \subset M$ let $\tilde{Y} = \pi^{-1}(Y)$ be its preimage in $X = \tilde{M}$.

Let

$$\tilde{N} := \cup\{\mathrm{Min}(\gamma) : \gamma \in \Gamma \setminus \{1\},\ \inf d_\gamma < \epsilon\}.$$

Since Γ acts properly discontinuously on X, $\tilde{N}$ is a locally finite union of the sets $\mathrm{Min}(\gamma)$. Note that since H is connected, any $g \in H$ preserves the orientation of X, and in particular if g is elliptic $\mathrm{codim}_X(\mathrm{Fix}(g)) \geq 2$. As $\tilde{N}$ is a union of geodesics (axes of hyperbolic elements) and fixed sets of elliptic elements, the assumption that $\dim X \geq 3$ implies that $\mathrm{codim}_X(\tilde{N}) \geq 2$. It follows that $X \setminus \tilde{N}$ is connected.

For $\gamma \in \Gamma \setminus \{1\}$ and $x \in X \setminus \tilde{N}$ set

$$d'_\gamma(x) = d_\gamma(x) - \inf d_\gamma.$$

Let $f : \mathbb{R}^{>0} \to \mathbb{R}^{\geq 0}$ be a smooth function which tends to ∞ at 0, strictly decreases on $(0, \epsilon]$ and is identically 0 on $[\epsilon, \infty)$, and set for $x \in X \setminus \tilde{N}$

$$\tilde{\psi}(x) := \sum_{\gamma \in \Gamma \setminus \{1\},\ \inf d_\gamma \leq \epsilon} f(d'_\gamma(x)).$$

since $f(d'_\gamma(x)) \neq 0 \Rightarrow d_\gamma(x) \leq 2\epsilon$ and Γ is discrete, there are only finitely many non-zero summands for each x. Thus $\tilde{\psi}$ is a well defined Γ invariant smooth function on $X \setminus \tilde{N}$. Note that $\tilde{\psi}(x)$ tends to ∞ as x approaches $\tilde{N}$. Let $\psi : M \setminus N \to \mathbb{R}^{\geq 0}$ be the induced function on $M \setminus N$.

For $a \geq 0$, set

$$\tilde{\psi}_{\leq a} := \{x \in X \setminus \tilde{N} : \tilde{\psi}(x) \leq a\},$$

and $\psi_{\leq a} = \pi(\tilde{\psi}_{\leq a}) = \{x \in X \setminus \tilde{N} : \psi(x) \leq a\}$. Note that $d_\gamma(x) \geq \epsilon$ for every $x \in \tilde{\psi}_{\leq 0}$ and $\gamma \in \Gamma \setminus \{1\}$. Thus, the injectivity radius of M at any point in $\psi_{\leq 0}$ is at least $\frac{\epsilon}{2}$.

Lemma 2.2. *For $x \in X \setminus \tilde{N}$, the gradient $\nabla\tilde{\psi}(x) = 0$ if and only if $\tilde{\psi}(x) = 0$.*

The proof relies on the following simple observations which follow directly from the fact that X has strictly negative sectional curvature:

(1) If $c_1(t), c_2(t)$ are two disjoint unit speed geodesics with $c_1(-\infty) = c_2(-\infty)$, then $d(c_1(t), c_2(t))$ is a strictly increasing smooth function of t, and hence $\frac{d}{dt} d(c_1(t), c_2(t)) > 0$ for every t. In particular, if $g \cdot p = p$ for some $g \in H, p \in \partial X$ and c is a geodesic with $c(-\infty) = p$, then $\frac{d}{dt} d_g(c(t)) > 0$ for all t, provided c is not g invariant.

(2) Suppose that $A \subset X$ is a closed convex set and let $P_A : X \to A$ be the nearest point retraction. Then $d(P_A(x), P_A(y)) < d(x, y)$ for any $x, y \in X \setminus A$. We will say that a geodesic ray $c : [0, \infty) \to X$ starting at a point of A is *perpendicular* to A if $P_A(c([0, \infty)) = c(0)$. Then if $c_1, c_2 : [0, \infty) \to X$ are two different unit speed rays perpendicular to A, the function $d(c_1(t), c_2(t))$ is convex and strictly increasing. Hence if $c : [0, \infty) \to X$ is perpendicular to A and g is an isometry which leaves the set A invariant but moves $c(t)$, then $\frac{d}{dt} d_g(c(t)) > 0$ for any $t > 0$.

Note that (1) and (2) fail to hold in higher rank symmetric spaces. In rank one both assertions follow for instance from the well known Flat Strip Theorem: Two parallel segments in a Hadamard manifold bound a flat parallelogram, in particular, if the space has strictly negative curvature, then any two parallel segments are contained in a common geodesic (cf. [Ba, Corollary 5.8]).

Proof of Lemma 2.2. Let x be a point in $X \setminus (\tilde{N} \cup \tilde{\psi}_{\leq 0})$. Let Σ_x be the finite set of elements in $\Gamma \setminus \{1\}$ which contribute non-zero summands to the function $\tilde{\psi}$, i.e. those σ for which $f(d'_\sigma(x)) > 0$. We will show that there is a geodesic c through x (say, $x = c(t_0)$) such that $\frac{d}{dt}|_{t_0} d_\sigma(c(t)) > 0$, $\forall \sigma \in \Sigma_x$. This will imply that

$$\nabla\tilde{\psi}(x) \cdot \dot{c}(t_0) = \sum_{\sigma \in \Sigma_x} f'(d'_\sigma(x)) \frac{d}{dt}|_{t_0} d_\sigma(c(t)) < 0,$$

and in particular that $\nabla\tilde{\psi}(x) \neq 0$.

Let $\Delta_x = \langle \Sigma_x \rangle$. By Lemma 2.1, Δ_x admits a normal nilpotent subgroup Λ_x of finite index in Δ_x.

Suppose first that Δ_x is a finite group. Let y be a common fixed point of Σ_x. Then as $d_\sigma(x) > 0 = d_\sigma(y)$ for all $\sigma \in \Sigma_x$, we derive from observation (2) above (by considering $\{y\}$ as a closed convex set) that the geodesic pointing from y to x does the job.

Suppose now that Δ_x is infinite. Let γ be a nontrivial central element of the nilpotent group Λ_x, and let $C_{\Delta_x}(\gamma)$ be the conjugacy class of γ in Δ_x. Then $|C_{\Delta_x}(\gamma)| \leq [\Delta_x : \Lambda_x]$, $C_{\Delta_x}(\gamma)$ is contained in the center of Λ_x and consists of elements which are simultaneously elliptic, hyperbolic or parabolic. In the first case, let A be the set of common fixed points of the elements of $C_{\Delta_x}(\gamma)$, in the second case let A be the common axis, and in the third case let $p \in \partial X$ be the common fixed point at infinity. Note that in the second case, as the geodesic A is Δ_x-invariant, we derive that Δ_x consists of semisimple elements and $A = \mathrm{Min}(\alpha) = \mathrm{axis}(\alpha)$ for every $\alpha \in \Delta_x$ which is hyperbolic. It follows that A does not contain our point x, for otherwise Σ_x must consist of elliptic elements preserving A and as Δ_x is infinite, there are $\alpha_1, \alpha_2 \in \Sigma_x$ without a common fixed point. However, since the α_i preserve A and $d_{\alpha_i}(x) < \epsilon$, the element $\alpha_1\alpha_2$ is hyperbolic with axis A and displacement $< \epsilon$, a contradiction (either to the assumption that $x \in A$ or to the one that Σ_x has no hyperbolic elements). In the first two cases we can take c to be the geodesic through x perpendicular to the Δ_x-invariant closed convex set A, and in the third case we can take c to be the geodesic through x with $c(-\infty) = p$. The result follows from observations (1) and (2) above. □

Since $\lim_{t\to 0} f(t) = \infty$, it follows that for any finite value a, the injectivity radius is bounded from below on the closed set $\psi_{\leq a}$. Hence $\psi_{\leq a}$ is bounded, for otherwise it would admit an infinite 1-discrete subset, yielding infinitely many disjoint embedded balls of a fixed radius in M, contradicting the finiteness of $\mathrm{vol}(M)$. Therefore $\psi_{\leq a}$ is compact for any $a < \infty$. Thus the function ψ is proper. Applying standard Morse theory we get:

Proposition 2.3. *For every positive a, $\psi_{\leq a}$ is a deformation retract of $M \setminus N$.*

Proof. By Lemma 2.2 the proper smooth function $\psi : M \setminus N :\to \mathbb{R}^{\geq 0}$ has no positive critical values. Thus the proposition follows from [M, Theorem 3.1]. □

For $a > 0$, we will denote by $r_a : M \setminus N \to \psi_{\leq a}$ the retraction induced by the deformation retract supplied by Proposition 2.3.

Corollary 2.4. *For every $a \geq 0$ the set $\tilde{\psi}_{\leq a}$ is non empty and connected.*

Proof. For $a > 0$ this immediately follows from Proposition 2.3, and for $a = 0$ it follows since $\tilde{\psi}_{\leq 0} = \bigcap\{\tilde{\psi}_{\leq a} : a > 0\}$ a descending intersection of the sets $\psi_{\leq a}$. □

Since $\tilde{\psi}_{\leq a}$ is Γ–invariant and Γ acts freely on it, we conclude:

Corollary 2.5. *For every $a > 0$, Γ is a quotient of $\pi_1(\psi_{\leq a})$ – the fundamental group of $\psi_{\leq a} = \Gamma\backslash\tilde{\psi}_{\leq a}$.*

Now recall that the injectivity radius of M at any point of $\psi_{\leq 0}$ is at least $\epsilon/2$. Let $\mathcal{S}$ be a maximal $\epsilon/2$ discrete subset of $\psi_{\leq 0}$. For $t > 0$ denote by $\nu(t)$ the volume of a t–ball in X. Since the $\epsilon/4$–balls centered at points of $\mathcal{S}$ are pairwise disjoint and isometric to an $\epsilon/4$–ball in X, the size of $\mathcal{S}$ is bounded by $\mathrm{vol}(M)/\nu(\frac{\epsilon}{4})$. Moreover, since $\mathcal{S}$ is maximal, the union of the $\epsilon/2$–balls centered at points of $\mathcal{S}$ covers $\psi_{\leq 0}$. Denote this union by U. Since U is a neighborhood of the compact set $\psi_{\leq 0}$ and ψ is continuous, choosing $a_0 > 0$ sufficiently small, we have $\psi_{\leq a_0} \subset U$.

Lemma 2.6. *$\pi_1(\psi_{\leq a_0})$ is a quotient of $\pi_1(U)$.*

Proof. The inclusion $i : \psi_{\leq a_0} \to U$ induces a map $i^* : \pi_1(\psi_{\leq a_0}) \to \pi_1(U)$, and the retraction r_{a_0} restricted to U, $r_{a_0} : U \to \psi_{\leq a_0}$ induces a map $r_{a_0}^* : \pi_1(U) \to \pi_1(\psi_{\leq a_0})$. Since $r_{a_0} \circ i$ is the identity on $\psi_{\leq a_0}$, we see that $r_{a_0}^* \circ i^*$ is the identity on $\pi_1(\psi_{\leq a_0})$. It follows that $r_{a_0}^* : \pi_1(U) \to \pi_1(\psi_{\leq a_0})$ is onto. □

Since M is negatively curved, the $\epsilon/2$–balls centered at points of $\mathcal{S}$ are convex, and hence any non-empty intersections of such is convex, hence contractible. Thus these balls form a *good cover* of U, in the sense of [BT] (see also [Ge1]), and the nerve $\mathcal{N}$ of this cover is homotopic to U. Now $\pi_1(U) \cong \pi_1(\mathcal{N})$ has a generating set of size $\leq E(\mathcal{N})$ – the number of edges of the 1–skeleton $\mathcal{N}^1$. To see this one may choose a spanning tree $\mathcal{T}$ for the graph $\mathcal{N}^1$ and pick one generator for each edge belonging to $\mathcal{N}^1 \setminus \mathcal{T}$. Finally note that the edges of $\mathcal{N}$ correspond to pairs of points in $\mathcal{S}$ which are of distance at most ϵ. Thus the degrees of the vertices of $\mathcal{N}$ are uniformly bounded, in fact, one can show that $\nu(1.25\epsilon)/\nu(0.25\epsilon)$ is an upper bound for the degrees. Thus

$$d(\Gamma) \leq |E(\mathcal{N})| \leq \nu(1.25\epsilon)/\nu(0.25\epsilon) \cdot |\mathcal{S}| \leq \frac{\nu(1.25\epsilon)}{\nu(0.25\epsilon)^2} \cdot \mathrm{vol}(M).$$

Remark 2.7. It has been recently shown that Theorem 1.5 holds for all semisimple Lie groups, with no rank assumption (see [Ge2]).

3. Counting maximal arithmetic subgroups

The main goal of this section is to prove Theorem 1.6. Only the upper bound is needed for the main result of this paper (and a much weaker estimate suffices).

For simplicity of notations we will assume throughout the proof that $H = \mathrm{PGL}_2(\mathbb{R})$ and remark at various points if non-trivial modifications are needed for the general case. (For a proof of an even more general result including products of $\mathrm{PGL}_2(k)$, where k is any characteristic 0 local field, see the forthcoming thesis [E].) We normalize the Haar measure on H so that for a lattice Γ its covolume is equal to the hyperbolic volume of the corresponding locally symmetric space. Borel [Bo] described in detail the maximal arithmetic lattices in H. We will follow the exposition of his work in [MR].

Arithmetic lattices in H are all obtained in the following way: Let k be a totally real number field of degree $d = d_k$, and A a quaternion algebra over k. Assume that for all the archimedean valuations $v \in V_\infty$ except for a single one v_0, A ramifies over $k_v (\cong \mathbb{R})$, i.e., $A(k_v)$ is isomorphic to the Hamiltonian quaternion algebra, while $A(k_{v_0}) \cong \mathrm{M}_2(\mathbb{R})$. Let $\mathcal{O} = \mathcal{O}_k$ be the ring of integers in k and let $\mathfrak{D}$ be an order in $A(k)$, i.e., $\mathfrak{D}$ is a finitely generated $\mathcal{O}$-submodule of $A(k)$ which is also a subring that generates $A(k)$ over k. Furthermore, assume that $\mathfrak{D}$ is a maximal order in A. Let $\mathfrak{D}^*$ be the group of invertible elements of $\mathfrak{D}$. Now, $\mathfrak{D}^*$ is discrete in $\prod_{v \in V_\infty} (A(k_v))^* \cong \mathrm{U}(2)^{d-1} \times \mathrm{GL}_2(\mathbb{R})$, and its projection Γ to $\mathrm{PGL}_2(\mathbb{R})$ gives a discrete subgroup of $\mathrm{PGL}_2(\mathbb{R})$. A subgroup of $H = \mathrm{PGL}_2(\mathbb{R})$ which is commensurable with such Γ is called an *arithmetic subgroup* of H. It is always a lattice, i.e., a discrete subgroup of finite covolume in H. It is non-uniform if and only if $k = \mathbb{Q}$ and A is the split quaternion algebra $\mathrm{M}_2(\mathbb{Q})$, i.e., Γ is commensurable to $\mathrm{PGL}_2(\mathbb{Z})$. All the arithmetic lattices of $\mathrm{PGL}_2(\mathbb{R})$ are obtained in this way and two arithmetic lattices of H are commensurable if and only if they come, in the process as above, from the same algebra A. So for each such algebra A we can associate a well defined commensurability class of arithmetic lattices in H which is denoted by $\mathcal{C}(A)$.

Now, a quaternion algebra A over k is completely determined by the finite set of valuations $\mathrm{Ram}(A)$, a subset of the set of all valuations V of k which consists of those v for which $A(k_v)$ ramifies (i.e., $A(k_v)$ is a division algebra), while for $v \in V \setminus \mathrm{Ram}(A)$, $A(k_v)$ splits (namely, isomorphic to $\mathrm{M}_2(k_v)$). The subset $\mathrm{Ram}(A)$ must be of even size; in our case it is formed by exactly $d-1$ real valuations and a subset $\mathrm{Ram}_f(A)$, possibly empty, of non-archimedean valuations. The set $\mathrm{Ram}_f(A)$ can be identified with a subset of the prime ideals of $\mathcal{O}$. Let $\Delta(A) = \prod_{\mathcal{P}\in\mathrm{Ram}_f(A)} \mathcal{P}$, the product of all prime ideals at which A ramifies.

Borel showed that the commensurability class $\mathcal{C}(A)$ has infinitely many non-conjugate maximal elements but only finitely many of them have bounded covolume. The minimal covolume in the class $\mathcal{C}(A)$ is:

$$\frac{8\pi {\Delta_k}^{3/2}\zeta_k(2)\prod_{\mathcal{P}|\Delta(A)}(N(\mathcal{P})-1)}{(4\pi^2)^{d_k}[{R_{f,\infty}}^* : ({R_f}^*)^2][{}_2J_1 : J_2]}, \tag{1}$$

see [MR, Corollary 11.6.6, p. 361 and (11.6), p. 333]. (Note that in [MR, (11.28), p. 361] the formula is given for $\mathrm{PGL}_2(\mathbb{C})$, in which case the factor 8π in the nominator is replaced by $4\pi^2$.)

Here Δ_k is the absolute value of the discriminant of k, ζ_k is the Dedekind zeta function of k and $N(P)$ denotes the norm of the ideal P, i.e. the order of the quotient field $\mathcal{O}/P$. For the other notations we refer to [MR, p. 358]. For our purpose it is enough to know the following estimates:

$$1 \le [{R_{f,\infty}}^* : ({R_f}^*)^2][{}_2J_1 : J_2] \le 2^{d+|\mathrm{Ram}_f(A)|}h_k, \tag{2}$$

where h_k is the class number of k (see [MR, pp. 358–360]).

We can now begin with the proof of Theorem 1.6. Assume that x is a large real number. We first bound the number of possible fields k which can contribute a maximal arithmetic lattice of covolume at most x. Then, given k, we will bound the number of possible quaternion algebras A and finally, given k and A, we will estimate the number of conjugacy classes of maximal lattices in $\mathcal{C}(A)$ of covolume at most x.

Lemma 3.1. *There exist two constants c_1 and c_2 such that if for some quaternion algebra A over k as above $\mathcal{C}(A)$ contains a lattice of covolume at most x in $\mathrm{PGL}_2(\mathbb{R})$, then $d_k \le c_1 \log x + c_2$.*

Proof. By [CF, Lemma 4.3], we know that if $\Gamma \in \mathcal{C}(A)$, then

$$\mathrm{covol}(\Gamma) > 0.69\exp(0.37d_k - \frac{19.08}{h(k,2,A)}), \tag{3}$$

where $h(k,2,A)$ is the order of a certain quotient of the class group of k, in particular, $1 \le h(k,2,A) \le h_k$. This lemma is one of the main technical results of [CF], its proof uses a variety of number-theoretic techniques.

We obtain

$$0.69\exp(0.37d_k - 19.08) \le x, \tag{4}$$

and so

$$d_k \le 3\log x + 21. \tag{5}$$

□

Lemma 3.2. *There exist constants $c_3, c_4 \in \mathbb{R}^{>0}$ such that if for some A and k as above there is Γ in $\mathcal{C}(A)$ of covolume $\leq x$, then $\Delta_k \leq c_3 x^{c_4}$.*

Proof. Borel and Prasad [BP, (7) on p. 143] deduced from Brauer-Siegel Theorem and a result of Zimmert that

$$h_k \leq 10^2 (\frac{\pi}{12})^{d_k} \Delta_k. \tag{6}$$

Combining (1), (2) and (6), we obtain

$$\frac{8\pi {\Delta_k}^{3/2} \zeta_k(2) \prod_{P \in \mathrm{Ram}_f(A)} (N(P)-1)}{(4\pi^2)^{d_k} 2^{d_k + |\mathrm{Ram}_f(A)|} 10^2 (\frac{\pi}{12})^{d_k} \Delta_k} \leq x. \tag{7}$$

Now $\frac{N(P)-1}{2} \geq 1$ unless $|N(P)| = 2$, which can happen for at most d_k primes in $\mathrm{Ram}_f(A)$ and for those $\frac{N(P)-1}{2} = \frac{1}{2}$. Also, $\zeta_k(2) \geq 1$. Thus from (7) we deduce

$$x \geq \frac{8\pi {\Delta_k}^{1/2}}{10^2 (4\pi^2)^{d_k} 2^{2d_k} (\frac{\pi}{12})^{d_k}} = \frac{8\pi}{10^2} \frac{\Delta_k^{\frac{1}{2}}}{(\frac{4}{3}\pi^3)^{d_k}} \tag{8}$$

Now, use (5) to deduce that

$$\frac{8\pi}{10^2} \Delta_k^{\frac{1}{2}} \leq x (\frac{4}{3}\pi^3)^{3\log x + 21},$$

which implies the lemma. □

We can now appeal to a theorem of Ellenberg and Venkatesh ([EV], [Be, Appendix]):

Theorem 3.3. (i) *Let $N(x)$ denote the number of isomorphism classes of number fields k with $\Delta_k \leq x$. Then for every $\epsilon > 0$, there is a constant $c_5(\epsilon)$ such that $\log N(x) \leq c_5(\epsilon)(\log x)^{1+\epsilon}$ for every $x \geq 2$.*

(ii) *For a fixed d, let $N_d(x)$ be the number of isomorphism classes of number fields k of degree at most d with $\Delta_k \leq x$. Then there exist $c_5' = c_5'(d)$ and $c_5'' = c_5''(d)$ such that $N_d(x) \leq c_5' \cdot x^{c_5''}$ for all sufficiently large x.*

We can deduce from Lemma 3.2 and Theorem 3.3 that for every $\epsilon > 0$, the number of number fields k which contribute lattices of covolume at most x is bounded by $x^{c_6(\epsilon)(\log x)^\epsilon}$ for a constant $c_6(\epsilon)$ and $x \gg 0$. Given one of these fields k with degree d_k, we now estimate the number of relevant A's. This number is bounded from above by the number of possible ways to choose an even set of valuations $\mathrm{Ram}(A)$ consisting of $d_k - 1$ real valuations and $\mathrm{Ram}_f(A)$, which satisfy (7). There are d_k ways to choose the $d_k - 1$ real valuations. Now, $8\pi\Delta_k^{\frac{1}{2}} \geq 1$ and also $\zeta_k(2) \geq 1$, by Lemma 3.1, $d_k \leq c_1 \log x + c_2$, and hence by (7) we get

$$\frac{1}{2^{|\mathrm{Ram}_f(A)|}} \prod_{P \in \mathrm{Ram}_f(A)} (N(P) - 1) \leq c_7 x^{c_8}, \tag{9}$$

for some absolute constants c_7 and c_8. The number of primes P with $N(P) = 2$ or 3 is at most $2d_k$. For them $\frac{N(P)-1}{2} \geq \frac{1}{2}$ and for all the other primes $\frac{N(P)-1}{2} \geq N(P)^{\log_4(\frac{3}{2})}$. We can therefore deduce that:

$$\prod_{P \in \mathrm{Ram}_f(A)} N(P) \leq x^{c_9}, \tag{10}$$

for some absolute constant c_9.

Note that $\Delta(A) = \prod_{P\in \mathrm{Ram}_f(A)} P$ is a square free ideal of norm at most x^{c_9}, whose factors determine A modulo the d_k choices of the unique real valuation of k in which A splits.

Lemma 3.4. *Let $I_k(x)$ denote the number of ideals of $\mathcal{O}_k$ of norm less than x. Then $I_k(x) \leq \zeta_k(2)x^2 \leq (\frac{\pi^2}{6})^{d_k}x^2$.*

Proof. $I_k(x) = a_1 + a_2 + \ldots + a_{[x]}$ where a_n is the number of ideals of norm n. At the same time $\zeta_k(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Hence, for every large x, $\zeta_k(2)x^2 \geq I_k(x)$. It is easy to see that $\zeta_k(2) \leq \zeta_{\mathbb{Q}}(2)^{d_k}$ and it is well known that $\zeta_{\mathbb{Q}}(2) = \frac{\pi^2}{6}$. □

Again, as $d_k = O(\log x)$, we can deduce from Lemma 3.4 and (10) that given k, the number of possibilities for $\Delta(A)$ is polynomial in x. So all together we now have a bound of the form $x^{c(\epsilon)(\log x)^{\epsilon}}$ for the number of quaternion algebras which give rise to lattices of covolume $\leq x$, or, in other words, for the number of commensurability classes $\mathcal{C}(A)$ with representatives of covolume at most x. Before continuing, let us mention that if one is interested in non-uniform lattices there is at most one such A (i.e., $k = \mathbb{Q}$ and $A = \mathrm{M}_2(\mathbb{Q})$) and exactly one when x is large enough. This is the case for $\mathrm{PGL}_2(\mathbb{R})$. For general $H = \mathrm{PGL}_2(\mathbb{R})^a \times \mathrm{PGL}_2(\mathbb{C})^b$ this number is polynomial by Theorem 3.3 (ii) since the degree of the field of definition of a non-uniform lattice in such H is $a + 2b$.

Now fix k and A, or, equivalently, $\mathrm{Ram}(A)$. We need to count the maximal lattices within the class $\mathcal{C}(A)$. In [MR, Section 11.4] a class $m(A)$ of lattices in $\mathcal{C}(A)$ is described which essentially gives the maximal subgroups in $\mathcal{C}(A)$, namely, it contains all the maximal ones but maybe some more. We will show that even the total number of all of them is polynomial in x. An element of $m(A)$ is denoted by $\Gamma_{S,\mathfrak{D}}$ where $\mathfrak{D}$ is a maximal order in A (in [MR] it is denoted by $\mathcal{O}$ but we prefer to use $\mathfrak{D}$ as $\mathcal{O}$ for us is the ring of integers in k) and S is a finite set of finite primes of k disjoint from $\mathrm{Ram}_f(A)$. When S is the empty set we get the group $\Gamma_{\emptyset,\mathfrak{D}}$. This is a group of the minimal covolume in $\mathcal{C}(A)$ whose covolume is given by (1). Up to conjugacy, the number of such groups is the same as the number of conjugacy classes of maximal orders $\mathfrak{D}$ in A. This number is called the type number of A (cf. [MR, Section 6.7]). The type number is a power of 2 [MR, Corollary 6.7.7]) which divides $h_k 2^{d_k-1}$ (see [MR, eq. (6.13) p. 221]). Recall that $d_k = O(\log x)$ (by Lemma 3.1). On the other hand by (6), $h_k \leq 10^2(\frac{\pi}{12})^{d_k}\Delta_k$ and by Lemma 3.2, Δ_k is polynomially bounded in x. Thus, the type number of A is also polynomially bounded in x. We can therefore fix $\mathfrak{D}$ and count the number of possibilities for S. The exact form of $\Gamma_{S,\mathfrak{D}}$ is described in [MR, Section 11.4], but for our current purpose what is only relevant is its covolume which is given by Theorem 11.5.1 on page 357 there:

Proposition 3.5. $\dfrac{\mathrm{covol}(\Gamma_{S,\mathfrak{D}})}{\mathrm{covol}(\Gamma_{\emptyset,\mathfrak{D}})} = 2^{-m}\prod_{P\in S}(N(P)+1)$ *for some* $0 \leq m \leq |S|$.

Recall that the covolume of $\Gamma_{\emptyset,\mathfrak{D}}$ is given by (1), but at this point we do not need it. Just recall that a well known result of Siegel asserts that for all lattices Γ in $\mathrm{PGL}_2(\mathbb{R})$, $\mathrm{covol}(\Gamma) \geq \frac{\pi}{42}$. (Note that in both cases $G = \mathrm{PSL}_2(\mathbb{R})$ and $G = \mathrm{PGL}_2(\mathbb{R})$ we have used the measure induced from the hyperbolic structure on $G/K = \mathbb{H}^2$. Now the lattice of minimal covolume in $\mathrm{PGL}_2(\mathbb{R})$ has as fundamental domain the pull back of the triangle $(\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{7})$ while its intersection with $\mathrm{PSL}_2(\mathbb{R})$ is of minimal covolume there but needs two copies of that triangle.) We can deduce now that if

$\mathrm{covol}(\Gamma_{S,\mathfrak{D}}) \leq x$, then

$$\prod_{P\in S} \frac{N(P)+1}{2} \leq \frac{42}{\pi}x.$$

Arguing exactly as we did in (9), (10) and Lemma 3.4 when bounding the possibilities for $\mathrm{Ram}_f(A)$ we deduce that the number of possibilities for S is polynomial in x (in fact, it is even easier now as we do not need to exclude the primes 2 and 3).

If $H = \mathrm{PGL}_2(\mathbb{R})^a \times \mathrm{PGL}_2(\mathbb{C})^b$, instead of Siegel's theorem we can use the Kazhdan–Margulis theorem [KM], or Borel's result [Bo, Theorem 8.2] which implies that covolumes of arithmetic lattices in H are bounded from bellow by a positive constant which depends only on H. This finishes the proof of the upper bounds in both parts of 1.6.

The proof of the lower bounds is much easier but it requires a detailed description of the groups $\Gamma_{S,\mathfrak{D}}$ above. As the lower bounds are not really needed for the main results, we only sketch the argument assuming that the reader is familiar with Section 11.4 of [MR].

For the lower bound in case (a) of Theorem 1.6 we could vary the algebra A and easily deduce that for some $\delta > 0$, there are at least x^δ non conjugate (and also not commensurable after conjugation) maximal arithmetic lattices in $\mathrm{PGL}_2(\mathbb{R})$ with covolume at most x, but such a proof would not work for the non-uniform case where all arithmetic lattices are commensurable (after conjugation) and there is only one $A = \mathrm{M}_2(\mathbb{Q})$. For a proof which works in both cases fix k, A and $\mathfrak{D}$ so that $\mathcal{C}(A)$ is a commensurability class of arithmetic lattices in H. We need to show that there exist sufficiently many subsets S with $\prod_{v\in S} q_v \leq x^c$ and $\Gamma_{S,\mathfrak{D}}$ is maximal. For the group $\Gamma_{S,\mathfrak{D}}$ to be maximal there should exist an element $a \in k$ such that $\tilde{v}(a)$ is odd for $v \in S$ (here $\tilde{v}(a)$ denotes the logarithmic valuation on k_v), a is positive at the ramified real places of A, and $\tilde{v}(a)$ is even for $v \in V_f \setminus (\mathrm{Ram}_f(A) \cup S)$ (see discussion in Section 11.4 of [MR] for more details).

Let p be a rational prime and let S_p be the set of places $v \in V_f$ such that $\tilde{v}(p)$ is odd. Assume that p is unramified in k which is the case for all sufficiently large primes. Then S_p consists of the prime ideals of k which divide p, so if $p_1 \neq p_2$, then $S_{p_1} \neq S_{p_2}$. To every such p we can assign a maximal arithmetic subgroup $\Gamma_p = \Gamma_{S_p,\mathfrak{D}}$ which contains an element odd at v for $v \in S_p$ and even at the remaining places in $V_f \setminus \mathrm{Ram}_f(A)$. Then for $p_1 \neq p_2$ the groups Γ_{p_1} and Γ_{p_2} are non-conjugate maximal arithmetic subgroups of H. By Borel's volume formula (see (1) and Proposition 3.5)

$$\mathrm{covol}(\Gamma_p) \leq c_1 \prod_{v\in S_p} (q_v + 1),$$

where $c_1 = c_1(k, A)$ is a positive constant.

The set S_p contains at most d_k places of k and $\prod_{v\in S_p} q_v \leq p^{d_k}$. This implies

$$\mathrm{covol}(\Gamma_p) \leq c_1(2p)^{d_k}.$$

Thus, if $p \leq \frac{1}{2}(x/c_1)^{1/d_k} = x^{c_2}$, then $\mathrm{covol}(\Gamma_p) \leq x$. As k is fixed and so is d_k, it follows from the prime number theorem that for a large enough x there exists a constant $\delta > 0$ such that there are at least x^δ such primes p, and hence such Γ_p's.

This finishes the proof of the theorem. □

Remark 3.6. Theorem 1.6 gives a solution to Problem 6.5 of [Be] and implies that we can now remove the restriction that the group H has no simple factors of type A_1 in the main result there.

Remark 3.7. With the estimate of Lemma 3.2 at hand we can essentially repeat all the steps of the proof of Theorem A in [BP] for the groups G defined over number fields and having the absolute rank 1. The only missing ingredient, which is an analogue of a number-theoretic result from Section 6.1 in [BP] for the groups of type A_1, is now available because of Lemmas 3.1 and 3.2. This allows us to remove the restriction on the absolute rank from the statement of the Borel-Prasad theorem, which can be now formulated as follows:

Theorem 3.8. *Let $c > 0$ be given. Assume k runs through the number fields. Then there are only finitely many choices of k, of an absolutely almost simple algebraic group G' defined over k up to k-isomorphism, of a finite set S of places of k containing all the archimedean places, of arithmetic subgroup Γ' of $\mathrm{G}'_S = \prod_{v\in S} \mathrm{G}'(k_v)$ up to conjugacy, such that $\mu'_S(\mathrm{G}'_S/\Gamma') \le c$.*

We refer to [BP] for the definition of the measure μ'_S with respect to which the covolumes of arithmetic subgroups are computed (the so-called *Tits measure*), introduction and more details on this important result. Note that an analogous result for the groups over the global function fields is not true. For example, one can show that the covolume of $\mathrm{SL}_n(\mathrm{F}_q[t^{-1}])$ in $\mathrm{SL}_n(\mathrm{F}_q((t)))$ tends to zero if either n or $q \to \infty$ (see [BP, Section 7.12]).

4. Uniform bounds for Fuchsian groups and characters of Symmetric groups

In this section we study the subgroup growth of finitely generated non-elementary discrete subgroups of $\mathrm{PGL}_2(\mathbb{R})$, the so called Fuchsian groups.

By classical work of Fricke and Klein, the orientation-preserving Fuchsian groups Γ (i.e. those contained in $\mathrm{PSL}_2(\mathbb{R})$) have a presentation of the following form:

$$\begin{aligned} &\text{generators}: && a_1, b_1, \dots, a_g, b_g,\ \text{(hyperbolic)},\ x_1, \dots, x_d\ \text{(elliptic)}, \\ &&& y_1, \dots, y_s\ \text{(parabolic)},\ z_1, \dots, z_t\ \text{(hyperbolic boundary elements)} \\ &\text{relations}: && x_1^{m_1} = \cdots = x_d^{m_d} = 1,\ x_1 \cdots x_d\, y_1 \cdots y_s\, z_1 \cdots z_t\, [a_1, b_1] \cdots [a_g, b_g] = 1, \end{aligned} \tag{11}$$

where $g, d, s, t \ge 0$ and $m_i \ge 2$ for all i. The number g is referred to as the *genus* of Γ. Define $\mu(\Gamma) = -\chi(\Gamma)$, where $\chi(\Gamma)$ is the Euler characteristic of Γ (in the rest of this section we reserve the letter χ for characters of symmetric groups). Then for Γ as above we have

$$\mu(\Gamma) = 2g - 2 + \sum_{i=1}^{d} (1 - \frac{1}{m_i}) + s + t.$$

It is well known that $\mu(\Gamma) > 0$.

The non orientation-preserving Fuchsian groups have presentations as follows, with $g > 0$:

$$\begin{aligned} &\text{generators}: && a_1, \dots, a_g,\ x_1, \dots, x_d,\ y_1, \dots, y_s,\ z_1, \dots, z_t \\ &\text{relations}: && x_1^{m_1} = \cdots = x_d^{m_d} = 1, \\ &&& x_1 \cdots x_d\, y_1 \cdots y_s\, z_1 \cdots z_t\, a_1^2 \cdots a_g^2 = 1. \end{aligned} \tag{12}$$

In this case we have

$$\mu(\Gamma) = -\chi(\Gamma) = g - 2 + \sum_{i=1}^{d} (1 - \frac{1}{m_i}) + s + t,$$

and again, $\mu(\Gamma) > 0$.

We call Fuchsian groups as in (11) *oriented*, and those as in (12) *non-oriented*.

The Fuchsian groups with $s = t = 0$ are the uniform lattices; these are more challenging ones since the other Fuchsian groups are free products of cyclic groups.

In this section we prove Theorem 1.7 which provides a uniform bound on the subgroup growth of Fuchsian groups.

The novelty of Theorem 1.7 is that it holds for *all* n (not just for large n, where large may depend on Γ), and that it uses $\mu(\Gamma)$ as the only parameter. For a fixed group there are more refined asymptotic results (see [LiSh]), but it is the uniform version above which is crucial for our applications.

We shall now embark on the proof of Theorem 1.7. We assume throughout this section that Γ is an oriented Fuchsian group with the presentation given in (11). The proof in the non-oriented case (12) is very similar, hence omitted.

A major tool in our proof is character theory of symmetric groups (see [Sa]). We begin with some relevant notation and results.

Denote by $\mathrm{Irr}(S_n)$ the set of all irreducible characters of S_n. By a partition of a positive integer n we mean a tuple $\lambda = (\lambda_1, \ldots, \lambda_r)$ with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r \geq 1$ and $\sum_{i=1}^{r} \lambda_i = n$. Denote by χ_λ the irreducible character of S_n corresponding to the partition λ.

The following result of Fomin and Lulov [FL] plays a key role in our proof.

Proposition 4.1. (Fomin-Lulov [FL]) *Fix an integer $m \geq 2$. Suppose n is divisible by m, say $n = am$, and let $\pi \in S_n$ be a permutation of cycle-shape (m^a). Then for any irreducible character χ of S_n, we have*

$$|\chi(\pi)| \leq \frac{a!\, m^a}{(n!)^{1/m}} \cdot \chi(1)^{1/m}.$$

Consequently we have

$$|\chi(\pi)| \leq b n^{1/2} \cdot \chi(1)^{1/m},$$

where b is some absolute constant.

We note that the second assertion follows from first using Stirling's formula. In fact, as noted in [FL], we even have $|\chi(\pi)| \leq b n^{1/2 - 1/(2m)} \cdot \chi(1)^{1/m}$. In the rest of this section b denotes the constant above.

We shall also frequently use the Murnaghan-Nakayama Rule [Sa, p. 180]. By a *rim r-hook ν* in a λ-tableau, we mean a connected part of the tableau containing r boxes, obtained by starting from a box at the right end of a row and at each step moving downwards or leftwards only, which can be removed to leave a proper tableau denoted by $\lambda \backslash \nu$. If, moving from right to left, the rim hook ν starts in row i and finishes in column j, then the *leg-length* $l(\nu)$ is defined to be the number of boxes below the ij-box in the λ-tableau.

Lemma 4.2. (Murnaghan-Nakayama Rule) *Let $\rho\sigma \in S_n$, where σ is an r-cycle and ρ is a permutation of the remaining $n - r$ points. Then*

$$\chi_\lambda(\rho\sigma) = \sum_{\nu} (-1)^{l(\nu)} \chi_{\lambda \backslash \nu}(\rho),$$

where the sum is over all rim r-hooks ν in a λ-tableau.

In order to apply the Murnaghan-Nakayama rule it is useful to estimate the number of rim r-hooks in a tableau. We quote Lemma 2.11 from [LiSh]:

Lemma 4.3. *For any positive integer r and any partition λ of n, the number of rim r-hooks in a λ-tableau is at most $\sqrt{2n}$.*

We now deduce the following.

Lemma 4.4. *Let $\pi = \rho\sigma \in S_n$ be a permutation of order m, where ρ has cycle-shape (m^a) and σ permutes the remaining $n - ma$ points. Let $C(\sigma)$ be the number of cycles in σ. Then for any $\chi \in \mathrm{Irr}(S_n)$ we have*

$$|\chi(\pi)| \le b(2n)^{C(\sigma)/2}\chi(1)^{1/m}n^{1/2}.$$

Proof. Applying the Murnaghan-Nakayama Rule repeatedly for each cycle in σ and Lemma 4.3, we see that

$$|\chi(\pi)| \le \sum |\chi_i(\rho)|,$$

where $\chi_i \in \mathrm{Irr}(S_{ma})$, the sum has at most $(2n)^{C(\sigma)/2}$ terms, and $\chi_i(1) \le \chi(1)$. By Proposition 4.1, $|\chi_i(\rho)| \le b\chi_i(1)^{1/m}n^{1/2} \le b\chi(1)^{1/m}n^{1/2}$. This implies

$$|\chi(\pi)| \le b(2n)^{C(\sigma)/2}\chi(1)^{1/m}n^{1/2}$$

as required. □

For a permutation $\pi \in S_n$ we let π^{S_n} denote its conjugacy class. We now deduce the following.

Proposition 4.5. *Let $m \ge 2$ be an integer. Then for any positive integer n, any permutation $\pi \in S_n$ satisfying $\pi^m = 1$ and any character $\chi \in \mathrm{Irr}(S_n)$, we have*

$$|\pi^{S_n}| \cdot |\chi(\pi)| < b(n^n)^{1-1/m} \cdot \chi(1)^{1/m} \cdot (2e)^n.$$

Proof. Let π have cycle-shape $(m_1^{a_1}, \dots, m_k^{a_k})$, where $\sum m_i a_i = n$, $m_1 > m_2 > \dots > m_k$ and $m_1 = m$ (allowing the possibility that $a_1 = 0$). Set $A = \sum_{i=2}^k a_i$. Since

$$|\pi^{S_n}| = \frac{n!}{\prod_{i=1}^k m_i^{a_i} \prod_{i=1}^k a_i!} \le \frac{n!}{\prod_{i=1}^k a_i!},$$

Lemma 4.4 implies that

$$|\pi^{S_n}| \cdot |\chi(\pi)| \le \frac{n!}{\prod_{i=1}^k a_i!}(2n)^{A/2} b\chi(1)^{1/m}n^{1/2}. \tag{13}$$

Since $\frac{n^a}{a!} < e^a$ for any positive integer a, we have $\frac{n^{\sum a_i}}{\prod a_i!} < e^{\sum a_i}$. Let $B = \sum_{i=1}^k a_i$. Then

$$\frac{n!}{\prod_{i=1}^k a_i!} \le \frac{n^n}{\prod_{i=1}^k a_i!} = \frac{n^B}{\prod_{i=1}^k a_i!} n^{n-B} < e^B n^{n-B}.$$

In view of (13) this implies

$$|\pi^{S_n}| \cdot |\chi(\pi)| < e^B n^{n-B}(2n)^{A/2} b\chi(1)^{1/m}n^{1/2} \le bn^{n-B+A/2}\chi(1)^{1/m}e^B 2^{A/2}n^{1/2}.$$

Now, for $i \ge 2$ we have $m_i \le m/2$ (since m_i is a proper divisor of m), so $a_1 m + Am/2 \ge \sum_{i=1}^k a_i m_i = n$. Thus

$$B - A/2 = a_1 + A/2 \ge n/m.$$

We also have $e^B 2^{A/2} n^{1/2} \le e^n 2^{n/2} 2^{n/2} = (2e)^n$. Hence

$$|\pi^{S_n}| \cdot |\chi(\pi)| < bn^{n-n/m}\chi(1)^{1/m}(2e)^n,$$

which proves the result. □

We shall also use the following.

Lemma 4.6. *Fix a real number $s > 0$. Then*

$$\sum_{\chi \in \mathrm{Irr}(S_n)} \chi(1)^{-s} \to 2 \text{ as } n \to \infty.$$

In particular, $\sum_{\chi \in \mathrm{Irr}(S_n)} \chi(1)^{-s} \leq C(s)$ for all n, where $C(s)$ is a number depending only on s.

This result is proved in [LiSh] (see Theorem 1.1 there) following earlier results for the case $s \geq 1$. Here we apply it for a rather small value of s, namely $s = \frac{1}{42}$, which is the minimal value of $\mu(\Gamma)$ for a Fuchsian group Γ.

Next we study the space of homomorphisms $\mathrm{Hom}(\Gamma, S_n)$ from a Fuchsian group Γ to S_n by splitting it into subspaces whose sizes can be estimated. Let $g, d, s, t, m_1, \ldots, m_d$ be as in (11) and let $\mu = \mu(\Gamma)$.

Let $g_1, \ldots, g_d \in S_n$ be permutations satisfying $g_i^{m_i} = 1$ for each i. Let $C_i = g_i^{S_n}$ $(1 \leq i \leq d)$ be their conjugacy classes in S_n. Write $\mathbf{C} = (C_1, \ldots, C_d)$. Define

$$\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) = \{\phi \in \mathrm{Hom}(\Gamma, S_n) \ : \ \phi(x_i) \in C_i \text{ for } 1 \leq i \leq d\}.$$

Suppose now that Γ is a uniform lattice. The following formula, which essentially dates back to Hurwitz [Hu], connects $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|$ with characters of symmetric groups:

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| = (n!)^{2g-1} |C_1| \ldots |C_d| \sum_{\chi \in \mathrm{Irr}(S_n)} \frac{\chi(g_1) \cdots \chi(g_d)}{\chi(1)^{d-2+2g}}. \tag{14}$$

This formula includes the case $d = 0$ in which Γ is a surface group, $\mathrm{Hom}_{\mathbf{C}} = \mathrm{Hom}$ and empty products are taken to be 1.

In fact, formula (14) holds for any finite group G in place of S_n, its proof is carried out by counting solutions in G of the equations corresponding to the defining relations of Γ. See, for instance, Section 3 of [LiSh] for details and for a similar formula for non-oriented Fuchsian groups.

Lemma 4.7. *With the above notation we have*

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \leq c_1 b^d (n^n)^{\mu+1} (2e)^{dn},$$

where c_1 is some absolute constant.

Proof. Suppose first that Γ is uniform. We use formula (14) above. By Proposition 4.5, we have

$$|C_i||\chi(g_i)| \leq b(2e)^n (n^n)^{1-1/m_i} \chi(1)^{1/m_i}$$

for all $i = 1, \cdots, d$. This yields

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \leq (n^n)^{2g-1} b^d (2e)^{dn} (n^n)^{\sum_{i=1}^d (1-1/m_i)} \sum_{\chi \in \mathrm{Irr}(S_n)} \frac{\chi(1)^{\sum_{i=1}^d 1/m_i}}{\chi(1)^{d-2+2g}}.$$

Since $\mu = 2g - 2 + \sum_{i=1}^d (1 - 1/m_i)$, we conclude that

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| \leq b^d (2e)^{dn} (n^n)^{\mu+1} \sum_{\chi \in \mathrm{Irr}(S_n)} \chi(1)^{-\mu}.$$

By Lemma 4.6 and a well known Siegel's inequality $\mu \geq 1/42$, we have

$$\sum_{\chi \in \mathrm{Irr}(S_n)} \chi(1)^{-\mu} \leq \sum_{\chi \in \mathrm{Irr}(S_n)} \chi(1)^{-1/42} \leq c_1,$$

where $c_1 = C(1/42)$. The result follows by combining the two inequalities above.

It remains to deal with Fuchsian groups with $s + t > 0$. Let $r = 2g + s + t - 1$, Z_m denote a cyclic group of order m and F_r a free group of rank r. Then we have a free product decomposition

$$\Gamma \cong Z_{m_1} * \cdots * Z_{m_d} * F_r.$$

It follows immediately that

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| = (n!)^r \prod_{i=1}^{d} |C_i|. \tag{15}$$

We claim that if $\pi \in S_n$ satisfies $\pi^m = 1$, then

$$|\pi^{S_n}| \leq e^n (n^n)^{1-1/m}. \tag{16}$$

Indeed, let $a_1, \ldots, a_k$ be the multiplicities of the cycle lengths of π and let $B = \sum_{i=1}^k a_i$, the number of cycles in π. Then, as in the proof of Proposition 4.5, we have

$$|\pi^{S_n}| \leq \frac{n!}{\prod a_i!} \leq e^B n^{n-B}.$$

Since all cycle lengths of π are at most m, we have $n/m \leq B \leq n$. Thus $e^B n^{n-B} \leq e^n n^{n-n/m}$, proving the claim.

Recall that $C_i = g_i^{S_n}$ and $g_i^{m_i} = 1$. Therefore, using the claim, we obtain

$$|C_i| \leq e^n (n^n)^{1-1/m_i}$$

for all $i = 1, \ldots, d$. Plugging this in (15) we conclude that

$$|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)| = (n!)^r e^{dn} (n^n)^{\sum(1-1/m_i)} \leq (n^n)^{r+\sum(1-1/m_i)} e^{dn}.$$

Since $r + \sum(1 - 1/m_i) = \mu + 1$ the result follows (with an even better upper bound). □

We can now provide upper bounds for $|\mathrm{Hom}(\Gamma, S_n)|$. Given d define $d_1 = \max(d, 1)$.

Lemma 4.8. *There exists an absolute constant c_2 such that with the above notation we have*

$$|\mathrm{Hom}(\Gamma, S_n)| \leq (n^n)^{\mu+1} c_2^{d_1 n}$$

for all n.

Proof. We clearly have

$$|\mathrm{Hom}(\Gamma, S_n)| = \sum_{\mathbf{C}} |\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|,$$

where the sum is over all possible $\mathbf{C} = (C_1, \ldots, C_d)$. Now, S_n has $p(n)$ conjugacy classes, where $p(n)$ is the partition function, and each summand $|\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n)|$ can be bounded as in Lemma 4.7. This yields

$$|\mathrm{Hom}(\Gamma, S_n)| \leq p(n)^d \cdot c_1 b^d (n^n)^{\mu+1} (2e)^{dn}.$$

It is well known that $p(n) \leq c_3^{\sqrt{n}} \leq c_3^n$ for some absolute constant c_3. This yields

$$|\mathrm{Hom}(\Gamma, S_n)| \leq c_1 (n^n)^{\mu+1} c_4^{dn},$$

for the absolute constant $c_4 = 2ebc_3$. This easily implies the required conclusion (with $c_2 = c_1c_4$). □

We can now draw conclusions to the subgroup growth of Fuchsian groups.

Proposition 4.9. *There exists an absolute constant c_5 such that with the above notation we have*

$$s_n(\Gamma) \leq n^{\mu n} c_5^{d_1 n}$$

for all n.

Proof. For a positive integer n, denote by $a_n(\Gamma)$ the number of index n subgroups of Γ. Define

$$\mathrm{Hom}_{trans}(\Gamma, S_n) = \{\phi \in \mathrm{Hom}(\Gamma, S_n) : \phi(\Gamma) \text{ is transitive}\}.$$

It is well known that $a_n(\Gamma) = |\mathrm{Hom}_{trans}(\Gamma, S_n)|/(n-1)!$ (see, for instance, [LuSe, 1.1.1]). Obviously, $|\mathrm{Hom}_{trans}(\Gamma, S_n)| \leq |\mathrm{Hom}(\Gamma, S_n)|$, so applying Lemma 4.8 we obtain

$$a_n(\Gamma) \leq (n^n)^{\mu+1} c_2^{d_1 n}/(n-1)!,$$

and hence

$$s_n(\Gamma) \leq n \cdot (n^n)^{\mu+1} c_2^{d_1 n}/(n-1)!.$$

Since $n \cdot n^n/(n-1)! \leq c_6^n$ for some absolute constant c_6, we obtain

$$s_n(\Gamma) \leq c_6^n \cdot (n^n)^{\mu} c_2^{d_1 n},$$

which implies the conclusion (with $c_5 = c_2c_6$). □

We can finally prove the main result of this section, namely Theorem 1.7.

Note that $\mu = 2g - 2 + \sum_{i=1}^{d}(1 - 1/m_i) \geq -2 + d/2$. This yields $d \leq 2\mu + 4$, and so

$$d_1 \leq d + 1 \leq 2\mu + 5.$$

Next, since $\mu \geq 1/42$, we have $5 \leq 210\mu$, and so $2\mu + 5 \leq 212\mu$. This implies

$$d_1 \leq 212\mu.$$

Applying Proposition 4.9, we obtain

$$s_n(\Gamma) \leq n^{\mu n} c_5^{212\mu n} \leq (cn)^{\mu n},$$

where $c = c_5^{212}$.

This completes the proof of Theorem 1.7. □

We did not make an attempt to optimize the constants appearing here and in Theorem 1.7 in particular.

Remark 4.10. It is intriguing that there are no uniform lower bounds on the subgroup growth of Fuchsian groups. For example, let Γ be a triangle (p, q, r)-group with p, q, r distinct primes which are greater than n (so Γ has a presentation as in (11) with $g = s = t = 0$, $d = 3$ and $m_1 = p, m_2 = q, m_3 = r$). Then one easily sees that $s_n(\Gamma) = 0$. Since n can be arbitrarily large no uniform lower bounds exist.

Finally, we can provide a lower bound on $s_n(\Gamma)$ in terms of $\mu(\Gamma)$ which holds for all n larger than some number depending on Γ:

Proposition 4.11. *Let Γ be a Fuchsian group. Then we have*

$$s_n(\Gamma) \geq (n!)^{\mu(\Gamma)} \text{ for all sufficiently large } n.$$

Proof. A somewhat stronger result, namely $a_n(\Gamma) \geq (n!)^{\mu(\Gamma)} \cdot n^b$ for every fixed b and for all large n is given in Theorem 4.6 of [LiSh]. However, the proof given there only works for Fuchsian groups with torsion. The remaining Fuchsian groups are free groups and surface groups. For the free group $\Gamma = F_d$ $(d \geq 2)$ it is well known that $a_n(\Gamma) \sim (n!)^{d-1} \cdot n = (n!)^{\mu(\Gamma)} \cdot n$. For surface groups Γ it is known that $a_n(\Gamma) \sim 2(n!)^{\mu(\Gamma)} \cdot n$ (see [MP]). This implies the result. In fact, it follows that for any constant $c < 1$ and for any Fuchsian group Γ we have

$$a_n(\Gamma) \geq cn(n!)^{\mu(\Gamma)}, \text{ for all sufficiently large } n,$$

and this lower bound is best possible. □

5. Proof of the main results

We can use now the results of Sections 2, 3 and 4 to prove the main Theorems.

5.1. **The proof of Theorem 1.1.** Recall from [LuSe], Lemma 1.1.2 that if Γ is finitely generated group with $d(\Gamma)$ generators, then $s_n(\Gamma) \leq n^{d(\Gamma)n}$ where $s_n(\Gamma)$ denotes the number of subgroups of index at most n in Γ. Let now H be a fixed rank one simple Lie group. By Theorem 1.6 and [Be], $\mathrm{MAL}_H(x) = \mathrm{MAL}_H^u(x) + \mathrm{MAL}_H^{nu}(x) \leq x^{a \log x}$. Now, every arithmetic lattice Γ of covolume at most x is contained in a maximal lattice Λ of covolume, say, $y \leq x$, and $[\Lambda : \Gamma] \leq \frac{x}{y}$. Hence,

$$\mathrm{AL}_H(x) \leq \mathrm{MAL}_H(x) \cdot \max\{s_{\frac{x}{y}}(\Lambda) : y \leq x, \mathrm{covol}(\Lambda) = y\}$$

where Λ runs over the finitely many conjugacy classes of arithmetic lattices of covolume at most x. By Theorem 1.5, for such Λ, $d(\Lambda) \leq Cy$ for some constant $C = C(H)$, hence

$$s_{\frac{x}{y}}(\Lambda) \leq (\frac{x}{y})^{d(\Lambda)\frac{x}{y}} \leq (\frac{x}{y})^{Cy\frac{x}{y}}.$$

Now by Kazhdan-Margulis theorem (which also follows from Theorem 1.5 as we noted in the introduction), $y \geq C'$ for some $C' = C'(H)$, and hence

$$\mathrm{AL}_H(x) \leq x^{a \log x}(\frac{x}{C'})^{Cx} \leq x^{bx}$$

for some constant b when $x \gg 0$. □

Remark 5.1. As mentioned in Remark 2.7, Theorem 1.5 holds also for higher rank semisimple Lie groups, thus the proof shows that Theorem 1.1 is valid in general. We refer to [BL] for better estimates in the higher rank case.

5.2. **The proof of Theorem 1.2.** Fix $n \geq 2$. In [Lu2] it was shown that $H = \mathrm{PSO}(n, 1)$ has an arithmetic lattice Γ which is mapped onto the free group on two generators. Let $\mathrm{L}(n)$ be the set of subgroups of Γ of index at most n. Then

$$|\mathrm{L}(n)| = s_n(\Gamma) \geq s_n(F_2) \geq n!$$

(see [LuSe, Corollary 2.1.2] for the right hand side inequality). Thus, if $\mathrm{covol}(\Gamma) = v_0$, Γ contains at least $n!$ sublattices of covolume at most nv_0. We should prove that not too many of them are conjugate in H.

To prove this we argue as follows: Let $C(n)$ be the set of congruence subgroups of Γ of index at most n. By [Lu1], $|C(n)| \leq n^{c_0 \log n/\log\log n}$ for some constant c_0. There is a map $\phi : \mathrm{L}(n) \to C(n)$ sending a subgroup in $\mathrm{L}(n)$ to its closure in the congruence topology of Γ. There are therefore at least $\frac{n!}{n^{c_0 \log n/\log\log n}} \geq n^{c_1 n}$ subgroups in $\mathrm{L}(n)$ with the same congruence closure. If Γ_1 and Γ_2 are two such subgroups with congruence closure Γ_0 which are conjugate in H, say $\Gamma_1 = g\Gamma_2 g^{-1}$, then $g \in \mathrm{Comm}_H(\Gamma)$, the commensurability group of Γ in H. As Γ is arithmetic, $\mathrm{Comm}_H(\Gamma)$ acts by k-rational morphisms (more precisely, in the adjoint representation it has entries in k, where k is the number field over which Γ is defined), hence g preserves the congruence topology. Thus, g normalizes Γ_0, i.e. $g \in N_H(\Gamma_0)$. Recall that $N_H(\Gamma_0)$ is itself a lattice in H (cf. [R]), hence by Kazhdan-Margulis theorem (or by 1.5) has covolume at least C'. This implies that at most $c_2 n$ subgroups like Γ_2 can be conjugated to Γ_1 in H. Thus, H has at least $n^{c_1 n}/c_2 n \geq n^{c_1' n}$ conjugacy classes of arithmetic lattices of covolume at most nv_0. This proves Theorem 1.2.

5.3. **The proof of Theorem 1.3.** We shall prove a more precise statement:

Theorem 5.2. *Let $H = \mathrm{PSL}_2(\mathbb{R})$ and $\mathrm{AL}_H(x)$ the number of conjugacy classes of arithmetic lattices in H of covolume at most x. Then there exist $6 < r < s \in \mathbb{R}$ such that*

$$(rx)^{\frac{1}{2\pi}x} \leq \mathrm{AL}_H(x) \leq (sx)^{\frac{1}{2\pi}x}$$

for all sufficiently large x.

Proof. We will prove first the upper bound. As in the proof of Theorem 1.1 above, $\mathrm{AL}_H(x) \leq \mathrm{MAL}_H(x) \cdot \max\{s_{\frac{x}{y}}(\Lambda)\}$. Again, by Theorem 1.6, $\mathrm{MAL}_H(x) \leq x^{b \log x}$, but this time we also know that $y = \mathrm{covol}(\Lambda) = -2\pi\chi(\Lambda)$ and by Theorem 1.7, $s_{\frac{x}{y}}(\Lambda) \leq (c\frac{x}{y})^{-\chi(\Lambda)\frac{x}{y}}$. Thus altogether

$$\mathrm{AL}_H(x) \leq x^{b \log x} \cdot (c\frac{x}{y})^{-\chi(\Gamma)\frac{x}{-2\pi\chi(\Gamma)}} \leq (sx)^{\frac{1}{2\pi}x}$$

for a suitable constant s, as $y \geq \frac{\pi}{21}$ (by Siegel's theorem).

To prove the lower bound, take Γ to be the arithmetic lattice in $H = \mathrm{PSL}_2(\mathbb{R})$ of the lowest covolume $(\frac{\pi}{21})$, namely the $(2,3,7)$-triangle group. By Proposition 4.11, $s_n(\Gamma) \geq n^{-\chi(\Gamma)n}$ for $n \gg 0$. Again using the congruence topology of Γ and the upper bound on the number of congruence subgroups from [Lu1], we can deduce, as in the proof of Theorem 1.2 above, that Γ has at least $n^{-\chi(\Gamma)n}/[(n^{c_0 \log n/\log\log n})(c_2 n)] \geq (c_3 n)^{-\chi(\Gamma)n}$ subgroups of index at most n which belong to different H-conjugacy classes, where the constant c_3 could be taken $1-\epsilon$ for arbitrary positive ϵ. Each such subgroup is a lattice of covolume at most $x := n \cdot \mathrm{covol}(\Gamma) = -2\pi\chi(\Gamma)n$. Thus we have found at least $(c_3 \frac{x}{\mathrm{covol}(\Gamma)})^{-\chi(\Gamma)\frac{x}{-2\pi\chi(\Gamma)}} \geq (\frac{c_3}{(\pi/21)}x)^{\frac{x}{2\pi}}$ conjugacy classes of arithmetic lattices in H of covolume at most x. This finishes the proof of Theorem 5.2 and consequently of 1.3. □

Let us remark that the use of the $(2,3,7)$-triangle group was made only to ensure that $r > 6$. For proving the lower bound of Theorem 1.3 we could use any arithmetic lattice in $\mathrm{PSL}_2(\mathbb{R})$.

Proof of Corollary 1.4. The genus g surfaces are in one to one correspondence with the conjugacy classes of torsion free lattices in $\mathrm{PSL}_2(\mathbb{R})$ of covolume $4(g-1)\pi$. Thus Theorem 1.3 implies the upper bound in 1.4. The proof of the lower bound is similar to the proof of the lower bound in 1.3, just choose as a starting arithmetic lattice one which is *torsion free* and then count its finite index subgroups. □

References

[Ba] W. Ballmann, *Lectures on spaces of nonpositive curvature* (with an appendix by M. Brin), DMV Seminar, vol. 25, Birkhäuser, Basel, 1995.

[BGS] W. Ballmann, M. Gromov, V. Schroeder, *Manifolds of Nonpositive Curvature*, Progress in Mathematics, vol. 61, Birkhäuser, Boston, 1985.

[Be] M. Belolipetsky, Counting maximal arithmetic subgroups (with an appendix by J. Ellenberg and A. Venkatesh), *Duke Math. J.* **140** (2007), no. 1, 1–33.

[BL] M. Belolipetsky, A. Lubotzky, Counting manifolds and class field towers, *arXiv:0905.1841v1 [math.GR]*.

[Bo] A. Borel, Commensurability classes and volumes of hyperbolic 3-manifolds, *Ann. Scuola Norm. Sup. Pisa (4)* **8** (1981), 1–33.

[BP] A. Borel, G. Prasad, Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups, *Publ. Math. I.H.E.S.* **69** (1989), 119–171.

[BT] R. Bott, L. W. Tu, *Differential Forms in Algebraic Topology*, Springer, New York, 1982.

[BGLM] M. Burger, T. Gelander, A. Lubotzky, S. Mozes, Counting hyperbolic manifolds, *Geom. Funct. Anal.* **12** (2002), no. 6, 1161–1173.

[CF] T. Chinburg, E. Friedman, The smallest arithmetic hyperbolic three-orbifold, *Invent. Math.* **86** (1986), no. 3, 507–527.

[EV] J. Ellenberg, A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant, *Ann. of Math. (2)* **163** (2006), 723–741.

[E] A. Eisenmann, Counting Arithmetic Subgroups and Subgroup Growth of Virtually Free Groups, Thesis, Hebrew University (2010).

[FGT] T. Finis, F. Grunewald, P. Tirao, The cohomology of lattices in SL(2,C), *arXiv:0808.1204v1 [math.NT]*.

[FL] S. Fomin and N. Lulov, On the number of rim hook tableaux, *J. Math. Sci. (New York)* **87** (1997), 4118–4123.

[Ge1] T. Gelander, Homotopy type and volume of locally symmetric manifolds, *Duke Math. J.* **124** (2004), no. 3, 459–515.

[Ge2] T. Gelander, Volume vs rank of lattices, *preprint*.

[GLNP] D. Goldfeld, A. Lubotzky, N. Nikolov, L. Pyber, Counting primes, groups and manifolds, *Proc. of National Acad. of Sci.* **101** (2004), 13428–13430.

[Hu] A. Hurwitz, Über die Anzahl der Riemannschen Flächen mit gegebener Verzweigungspunkten, *Math. Ann.* **55** (1902), 53-66.

[KM] D. A. Kazhdan, G. A. Margulis, A proof of Selberg's hypothesis (in Russian), *Math. Sbornik (N.S.)* **75 (117)** (1968), 162–168.

[LiSh] M. W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552–601.

[Lu1] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), no. 2, 267–295.

[Lu2] A. Lubotzky, Free quotients and the first Betti number of some hyperbolic manifolds, *Transform. Groups* **1** (1996), no. 1–2, 71–82.

[LuSe] A. Lubotzky and D. Segal, *Subgroup Growth*, Birkhäuser, Basel, 2003.

[MR] C. Maclachlan, A. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Graduate Texts in Mathematics, vol. 219, Springer, New York, 2003.

[M] J. Milnor, *Morse theory* (based on lecture notes by M. Spivak and R. Wells), Annals of Math. Studies, no. 51, Princeton University Press, Princeton, NJ, 1963.

[MP] T. W. Müller and J.-C. Puchta, Character theory of symmetric groups and subgroup growth of surface groups, *J. London Math. Soc.* **66** (2002), 623–640.

[R] M. S. Raghunathan, *Discrete Subgroups of Lie Groups*, Springer, New York, 1972.

[Sa] B. E. Sagan, *The Symmetric Group: representations, combinatorial algorithms, and symmetric functions* (2nd edition), Springer, New York, 2001.

[Th] W. P. Thurston, *Three-Dimensional Geometry and Topology*, vol. 1, Princeton University Press, Princeton, NJ, 1997.

[Wa] H. C. Wang, Topics on totally discontinuous groups, in *Symmetric Spaces*, edited by W. Boothby and G. Weiss (1972), M. Dekker, 460–487.

Department of Mathematical Sciences, Durham University, Durham DH1 3LE, UK; Sobolev Institute of Mathematics, Koptyuga 4, 630090 Novosibirsk, Russia
E-mail address: mikhail.belolipetsky@durham.ac.uk

Institute of Mathematics, The Hebrew University, Givat Ram, Jerusalem, 91904, Israel

E-mail address: tsachik.gelander@gmail.com

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

E-mail address: shalev@math.huji.ac.il