Available online at www.sciencedirect.com

SciVerse ScienceDirect

ELSEVIER

Advances in Mathematics 229 (2012) 3123–3146

ADVANCES IN Mathematics

www.elsevier.com/locate/aim

Manifolds counting and class field towers

Mikhail Belolipetsky [a,*,1], Alexander Lubotzky [b,2]

[a] *IMPA, Estrada Dona Castorina, 110, 22460-320 Rio de Janeiro, Brazil*
[b] *Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel*

Received 17 December 2010; accepted 8 February 2012

Available online 23 February 2012

Communicated by Tomasz S. Mrowka

Dedicated to the memory of A.I. Fet

Abstract

In Burger et al. (2002) [12] and Goldfeld et al. (2004) [17] it was conjectured that if H is a simple Lie group of real rank at least 2, then the number of conjugacy classes of (arithmetic) lattices in H of covolume at most x is $x^{(\gamma(H)+o(1))\log x/\log\log x}$ where $\gamma(H)$ is an explicit constant computable from the (absolute) root system of H. In this paper we prove that this conjecture is false. In fact, we show that the growth is at rate $x^{c\log x}$. A crucial ingredient of the proof is the existence of towers of field extensions with bounded root discriminant which follows from the seminal work of Golod and Shafarevich on class field towers.

MSC: 22E40; 20G30; 20E07

Keywords: Arithmetic subgroups; Counting lattices; Subgroup growth; Lattices in higher rank Lie groups; Class field towers

1. Introduction

Let H be a non-compact simple Lie group endowed with a fixed Haar measure μ, K a maximal compact subgroup of H and $X = H/K$ the associated symmetric space. A classical theorem of Wang [38] asserts that if H is not locally isomorphic to $\mathrm{SL}_2(\mathbb{R})$ or $\mathrm{SL}_2(\mathbb{C})$, then for every

* Corresponding author.
E-mail addresses: mbel@impa.br (M. Belolipetsky), alexlub@math.huji.ac.il (A. Lubotzky).

[1] The author is partially supported by EPSRC grant EP/F022662/1.
[2] The author is partially supported by BSF (US–Israel), NSF and ERC.

0001-8708/$ – see front matter
doi:10.1016/j.aim.2012.02.002

$0 < x \in \mathbb{R}$ there exist only finitely many Riemannian orbifolds covered by X with volume at most x. Consequently, if $\mathrm{L}_H(x)$ (resp. $\mathrm{TFL}_H(x)$, $\mathrm{AL}_H(x)$) denotes the number of conjugacy classes of lattices (resp. torsion-free lattices, arithmetic lattices) in H of covolume at most x, then $\mathrm{L}_H(x)$ is finite for every x. For $\mathrm{AL}_H(x)$ this is also true even for $H = \mathrm{SL}_2(\mathbb{R})$ or $\mathrm{SL}_2(\mathbb{C})$ by a result of Borel [8].

In recent years there has been a growing interest in the asymptotic behavior of these functions (cf. [12,15–17,1,3]). Super-exponential upper bounds were given in many cases, and at least for rank one groups $\mathrm{SO}(n, 1)$ these bounds are optimal.

The current paper is devoted to the study of $\mathrm{L}_H(x)$ for groups H with real rank at least 2. Here one expects a slower rate of growth: Recall that in this case, by Margulis's arithmeticity theorem (see [25]), every lattice Γ in H is *arithmetic*, i.e. there exists a number field k with ring of integers $\mathcal{O}$ and the set of archimedean valuations V_∞, an absolutely simple, simply connected k-group G and an epimorphism $\phi : G = \prod_{v \in V_\infty} \mathrm{G}(k_v) \to H$, such that $\mathrm{Ker}(\phi)$ is compact and $\phi(\mathrm{G}(\mathcal{O}))$ is commensurable with Γ. Thus for groups H of real rank at least 2, we have $\mathrm{L}_H(x) = \mathrm{AL}_H(x)$. Moreover, Serre conjectured [35] that for all lattices Γ in such H, Γ has the *congruence subgroup property* (CSP), i.e. $\mathrm{Ker}(\widehat{\mathrm{G}(\mathcal{O})} \to \mathrm{G}(\widehat{\mathcal{O}}))$ is finite in the notations above. Assuming the conjecture, the question of counting lattices in H boils down to counting arithmetic groups and their congruence subgroups. A related conjecture which is also relevant for us is *Margulis–Platonov* (MP) *conjecture* (cf. [31]). It says that all normal subgroups of $\mathrm{G}(k)$ are of standard form coming from the nonarchimedean valuations of k with respect to which $\mathrm{G}(k_v)$ is anisotropic (in particular, $\mathrm{G}(k)$ does not have any noncentral proper normal subgroups if G is k_v-isotropic for all v).

The conjecture of Serre is proved by now for all non-uniform lattices and for "most" of the uniform ones, excluding certain cases when H is of type A_n, D_4 or E_6, and the same is also true for MP (see [28, Chapter 9] and [31] for the details and precise statements). Moreover, very precise estimates for the number of congruence subgroups in a given lattice are obtained in [22,18,23], some of these are conditional on the validity of the generalized Riemann hypothesis (GRH, cf. [39]). These results led to a conjecture in [12] that for groups H of $\mathbb{R}$-rank $\geqslant 2$, $\mathrm{L}_H(x)$ grows like $x^{c \log x / \log\log x}$. In fact, a more precise conjecture is made in [17], where it is suggested that

$$\lim_{x\to\infty} \frac{\log \mathrm{L}_H(x)}{(\log x)^2/\log\log x} = \gamma(H), \quad \text{with } \gamma(H) = \frac{(\sqrt{h(h+2)} - h)^2}{4h^2}, \tag{1}$$

where h is the Coxeter number of the (absolute) root system corresponding to H (i.e. the root system of the split form of H).

In this paper we prove that the conjecture is false! The correct rate of growth is $x^{\log x}$. It is still possible to show that the conjecture is essentially true if one restricts to *non-uniform* lattices for which we refer to [5].

Theorem 1. *Let H be a simple Lie group of real rank at least* 2. *Then*:

(i) *There exists a positive constant a such that $\mathrm{L}_H(x) \geqslant x^{a \log x}$ for all sufficiently large x.*
(ii) *Assuming the CSP and MP, there exists a positive constant b such that $\mathrm{L}_H(x) \leqslant x^{b \log x}$ for all sufficiently large x.*

A crucial ingredient in the proof of part (i) of the theorem is the existence of infinite class field towers of totally real fields as established by Golod and Shafarevich [19]. In Section 3, we

elaborate on it using the theory of Pisot numbers to get also sequences of fields of arbitrarily large degree but with a fixed number of complex places and a bounded root discriminant. Using these fields we construct a sequence of arithmetic lattices in H with covolume going to infinity and with a particularly large number of subgroups of small index. See below for details. It is interesting to mention that arithmetic lattices with fields of definition of growing degrees also come out in a connection with the Lehmer conjecture — see [2].

Our argument gives explicit estimates for the constants a and b in Theorem 1 but falls short from answering the following:

Problem 1. Does $\lim_{x\to\infty} \frac{\log \mathrm{L}_H(x)}{(\log x)^2}$ exist? And if so, what is its value?

The proof of the theorem uses methods developed in [1,18,23] (see also [17]). We would like to point out that unlike some of the results in [18] and [23], Theorem 1 does not depend on the GRH.

As all this suggests, our work is actually about counting arithmetic lattices and their congruence subgroups. It is therefore not surprising that it eventually boils down to various number theoretic problems. The wealth and diversity of number theoretic ingredients involved in proving Theorem 1 and results of [5] is exciting and may suggest some topics for future study.

Before describing the method of proof, let us put our main result in a more general perspective. In [12] the rate of growth of $\mathrm{TFL}_H(x)$ was determined for $H = \mathrm{SO}(n,1)$, $n \geqslant 4$; it is super-exponential. The lower bound there is already obtained by considering a suitable fixed lattice in $\mathrm{SO}(n,1)$ and its finite index subgroups. The upper bound is proved by geometric methods. These geometric methods were extended in [15] and [16] to more general semisimple groups. In [3] a very precise super-exponential estimate for $\mathrm{AL}_H(x)$ is given for $H = \mathrm{SL}_2(\mathbb{R})$. There again the full rate of growth is already obtained by considering the finite index subgroups of a single lattice. Moreover, in [18] and [23] (see also [17]) precise asymptotic estimates were given for the growth rate of the number of congruence subgroups in a fixed lattice Λ in H. (Some of the results there are conditional on the GRH.) The rate of growth turns out to depend only on H and not on Λ. All this suggested that the rate of growth of the finite index subgroups within one lattice is the main contribution to $\mathrm{L}_H(x)$. This led to the conjecture mentioned above. Moreover, in [1] it is shown that the growth rate of the *maximal* arithmetic lattices in H is very small. This provided more evidence in favor of the conjecture. Recently A. Salehi Golsefidy [34] showed that indeed in simple Lie groups over local fields of positive characteristic, the total growth of lattices is of the same growth type as the subgroup growth of a single lattice.

In [5] we will show that the conjecture is essentially true for non-uniform lattices but Theorem 1 here shows, somewhat surprisingly, that it is not true in general. In fact, we discover here a new phenomenon: the main contribution to the growth of uniform lattices in H does not come from subgroups of a single lattice. As it will be explained below, it comes from a "diagonal counting" when we run through different arithmetic groups Γ_i defined over number fields k_i of different degrees d_i, and for each Γ_i we count some of its subgroups. The difference between the uniform and non-uniform cases relies on the fact that all non-uniform lattices in H are defined over number fields of a bounded degree over $\mathbb{Q}$. On the other hand, uniform lattices may come from number fields k_i of arbitrarily large degrees, i.e., $d_i \to \infty$.

We now briefly sketch the main argument. If Γ is an arithmetic lattice obtained as $\phi(\mathrm{G}(\mathcal{O}))$ defined above, then there is an explicit formula [29] for its covolume in H. The analysis of this formula and also the growth of the low-index congruence subgroups of $\phi(\mathrm{G}(\mathcal{O}))$ shows that we can expect fast subgroup growth if we consider groups over fields of growing degree with

relatively slow growing discriminant $\mathcal{D}_k$. More precisely, we can combine these two entities together into the so-called root discriminant $rd_k = \mathcal{D}_k^{1/\deg k}$ and then look for a sequence of number fields k_i with degrees growing to infinity but with bounded rd_{k_i}. In a seminal work Golod and Shafarevich [19] came up with a construction of infinite class field towers. It is such a tower of number fields k_i that we use to define our arithmetic subgroups Γ_i. Galois cohomology methods show the existence of suitable k_i-algebraic groups G_i which give rise to arithmetic lattices $\Gamma_i = \mathrm{G}_i(\mathcal{O}_i)$ in H whose covolume is bounded exponentially in $d_i = \deg k_i$. We then present $c^{d_i^2}$ congruence subgroups of Γ_i whose covolume is still bounded exponentially in d_i. Using the theory of Bruhat–Tits buildings in Section 5 we show that sufficiently many of such congruence subgroups are not conjugate to each other in H. This will complete the proof of the lower bound of Theorem 1, at least for most real simple Lie groups H. The remaining cases require further consideration: for example, if H is a complex Lie group, the fields k_i should be replaced by suitable extensions obtained via the help of the theory of Pisot numbers. These fields do not form a class field tower any more but still have bounded root discriminant.

The proof of the upper bound presents a new type of difficulty: this time we need to obtain a uniform upper bound on growth which does not depend on the degrees of the defining fields. (This is what makes the growth rate $x^{\log x}$ instead of $x^{\log x/\log\log x}$.) A key ingredient of the proof is an important theorem of Babai, Cameron and Pálfy (see Theorem 7.7) which bounds the size of permutation groups with restricted Jordan–Holder components. This theorem was previously used in [22] to study the subgroup growth of lattices defined over global fields of positive characteristic. Bringing related technique to the number field case presents certain challenges and requires developing some new "subgroup growth" methods. We refer to Section 7 for the details of the argument.

The paper is organized as follows. After introducing some notations and conventions in Section 2, we supply in Section 3 the needed number theoretic background: we quote the Golod–Shafarevich work and use it with the theory of Pisot numbers to get families of number fields with bounded root discriminant and a given number of complex embeddings. In Section 4 we analyze carefully Prasad's formula for the covolume of arithmetic lattices. In Section 5 we tackle the subtle difference between counting covers of a given manifold M (which is what we get by counting finite index subgroups of $\pi_1(M)$) and counting manifolds covering M — which is what is relevant in the current paper. This issue often occurs in geometric considerations, for example, in constructions of manifolds which are isospectral but not isometric. We develop the required technique only up to the point needed in the current paper and leave some questions for further research. The theory of Bruhat–Tits building and their combinatorial growth plays a major role here. In Section 6 we prove the lower bound of Theorem 1 using the results in Sections 3, 4 and 5, while in Section 7 we prove the upper bound. Finally, in Section 8 we extend the theorem to semisimple Lie groups.

2. Notations and conventions

Let H be a semisimple Lie group without compact factors. Its subgroup Γ is called a *lattice* if Γ is discrete in H and its covolume (with respect to some and hence any Haar measure on H) is finite. A lattice is called *irreducible* if ΓN is dense in H, for every non-compact, closed, normal subgroup N of H. A lattice is called *uniform* (resp. *non-uniform*) if H/Γ is compact (resp. non-compact).

Two groups Γ_1 and Γ_2 are called *commensurable* if $\Gamma_1 \cap \Gamma_2$ is of finite index in both of them. If Γ is a lattice in H, its *commensurability subgroup* (or *commensurator*) in H is defined as

$$\mathrm{Comm}_H(\Gamma) = \left\{ g \in H \;\middle|\; g^{-1}\Gamma g \text{ and } \Gamma \text{ are commensurable} \right\}.$$

For a group (resp. profinite group) G we define its *rank* $\mathrm{rk}(G)$ as the supremum of the minimal number of generators over the finitely generated subgroups (resp. open subgroups) of G. If G is a finite group, its *p-rank* is defined by $\mathrm{rk}_p(G) = \mathrm{rk}(P)$, where p is a prime and P is a Sylow p-subgroup of G.

Along the lines we shall often come to arithmetic considerations, for which we now fix some notations. Throughout this paper k will always denote a number field, $\mathcal{O} = \mathcal{O}_k$ is its ring of integers and $\mathcal{D}_k$ is the absolute value of the discriminant Δ_k. The set of valuations (places) of k, $V = V(k)$, is the union of the set V_∞ of archimedean and the set V_f of nonarchimedean (finite) places of k. The number of archimedean places of k is denoted by $a = a_k = \#V_\infty$, and r_1, r_2 denote the number of real and complex places of k, respectively (so $a = r_1 + r_2$ and $d = d_k = [k : \mathbb{Q}] = r_1 + 2r_2$). Given a nonarchimedean place $v \in V_f$, the completion of k with respect to v is a nonarchimedean local field k_v, its residue field, which will be denoted by $\mathbb{F}_v$ or $\mathbb{F}_q$, is a finite field of cardinality $q = q_v$. Finally, $\mathbb{A} = \mathbb{A}(k) = \prod'_{v \in V} k_v$ is the ring of adèles of k, where $\prod'$ denotes a restricted product.

All logarithms in this paper will be taken to base 2. For a real number x, $[x]$ denotes the largest integer $\leqslant x$. The number of elements of a finite set S will be denoted by $\#S$, while the order of a finite group G will be denoted by $|G|$.

Whenever it is not stated otherwise, the constants c_1, c_2 and etc. depend only on the Lie group H.

3. Number theoretic background

3.1. Let $\alpha_1, \ldots, \alpha_d$ be a $\mathbb{Z}$-basis of $\mathcal{O}_k$ (i.e. an integral basis of k), and let $v_1, \ldots, v_d$ denote the archimedean embeddings of k. By definition, the *discriminant* $\Delta_k = \det[v_j(\alpha_i)]^2$ and $\mathcal{D}_k$ is its absolute value. The discriminant is related to the volume of the fundamental domain of the integral lattice in k. As we will see later on, this relation goes further to the covolumes of arithmetic lattices in semisimple Lie groups. We will also use a notion of *root discriminant* of k which is defined by $rd_k = \mathcal{D}_k^{1/d}$, where $d = [k : \mathbb{Q}]$.

Let us recall the following well-known results.

Theorem 3.1 *(Minkowski). (See [21, Theorem 4, p. 119].) Let k be a number field of degree $d = r_1 + 2r_2$. There exists a nonzero $\alpha \in \mathcal{O}_k$ whose norm satisfies*

$$\left|N(\alpha)\right| \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{\mathcal{D}_k}.$$

The proof of this theorem follows from the existence of lattice points in convex bodies in $\mathbb{R}^d$ whose volume is big enough relative to a fundamental region for the lattice.

By Stirling's formula, $d! = \sqrt{2\pi d}(\frac{d}{e})^d e^{\theta/12d}$ with $0 < \theta < 1$ (see [21, p. 122]). This, together with the fact that $|N(\alpha)| \geqslant 1$ for $0 \neq \alpha \in \mathcal{O}_k$, allows us to deduce that $\mathcal{D}_k > (\frac{\pi}{4})^{2r_2} \frac{1}{2\pi d} e^{2d - (1/6d)}$. We shall often use the following form of this estimate:

Corollary 3.2. *(See [21, Theorem 5, p. 121].) There exists an absolute constant $C > 0$ such that for any $k \neq \mathbb{Q}$, $d \leqslant C \log \mathcal{D}_k$.*

3.2. Let us call a sequence of pairwise non-isomorphic fields $(k_i)_{i\in\mathbb{N}}$ *asymptotically bounded* if there exists a constant c_0 such that for every i, the root discriminant $rd_{k_i} \leqslant c_0$. The definition implies that the degree of the fields in an asymptotically bounded sequence goes to infinity (it can be deduced from Minkowski's theorem that the number of fields with bounded $\mathcal{D}_k$ is finite, hence the number of fields with bounded root discriminant and bounded degree is also finite). The existence of asymptotically bounded sequences is not obvious, it follows from the work of Golod and Shafarevich on the class field towers.

Theorem 3.3. *(See Golod and Shafarevich [19].) There exists an infinite tower of unramified extensions of a totally real number field k.*

Given an unramified extension l/k, we have $\mathcal{D}_l = \mathcal{D}_k^{[l:k]}$ (by [21, Proposition 8, p. 62 and Proposition 14, p. 66]), and thus $rd_l = rd_k$. Therefore the root discriminant is constant along a tower of unramified extensions, which implies that such towers are asymptotically bounded. A well-known explicit sequence of totally real fields which satisfy Golod–Shafarevich criterion was constructed by Martinet in [26], the degrees of the fields are powers of 2 and $c_0 = rd_{k_i} = 1058.565\ldots$. A question about the smallest possible value of c_0 is important for various applications and is still open. It is known that a smaller constant can be achieved if we do not require the extensions to be unramified. The best current result in this direction is obtained by Hajir and Maire in [20], it provides an asymptotically bounded sequence of totally real fields with $c_0 = 954.3\ldots$.

3.3. Our next goal is to construct asymptotically bounded sequences of fields which have a fixed nonzero number of complex places. Note that the results mentioned above do not apply to this case, as in an unramified tower the number of complex places is either zero or grows with the degree (the same applies also to tamely ramified towers in [20]). In order to deal with this problem we use some results about Pisot numbers.

Assume that the field k has at least one real place. The number $\theta \in k$ is called a *Pisot number* (or Pisot–Vijayaraghavan number) if for a real place $v_1 : k \to \mathbb{R}$ we have $v_1(\theta) > 1$ and for all other $v_j \in V_\infty$, $|v_j(\theta)| < 1$.

Lemma 3.4. *Let k be a totally real number field of degree d.*

(a) *There exists a Pisot number $\theta \in k$ such that θ has degree d and $|N(1-\theta)| < \mathcal{D}_k^\delta$ for some absolute constant δ.*
(b) *Moreover, for any t such that $1 \leqslant t \leqslant d$ there exist t different Pisot numbers $\theta_1, \ldots, \theta_t$ satisfying the conditions of part* (a) *and such that $\alpha = (1-\theta_1)\ldots(1-\theta_t)$ is negative at t archimedean places of k and positive at the remaining $d - t$ places.*

Proof. (a) It is well known that there exist Pisot numbers $\theta \in k$ which generate k over $\mathbb{Q}$ (see e.g. [6, Theorem 5.2.2, p. 85]), thus it remains to show that we can choose such θ that the upper bound for the norm of $1 - \theta$ holds. In order to do so we need to recall the proof of the existence of θ: The argument uses Minkowski's theorem and implies that we can choose θ such

that $1 < v_1(\theta) \leqslant 2^{d-1}\sqrt{\mathcal{D}_k}$ and $|v_j(\theta)| \leqslant 1/2$ for $v_j \in V_\infty \smallsetminus \{v_1\}$ (see [6] for the details). Now if $P(x)$ is the minimal polynomial of θ, then $|N(1-\theta)| = |P(1)|$. We have

$$\big|P(1)\big| = \big|\big(1-v_1(\theta)\big)\cdot\cdots\cdot\big(1-v_d(\theta)\big)\big| \leqslant \big(2^{d-1}\sqrt{\mathcal{D}_k}+1\big)\left(\frac{3}{2}\right)^{d-1} = 3^{d-1}\sqrt{\mathcal{D}_k}+\left(\frac{3}{2}\right)^{d-1}.$$

By Corollary 3.2, the degree d is bounded by $C\log\mathcal{D}_k$, hence we obtain $|N(1-\theta)| \leqslant \mathcal{D}_k^{\delta}$ where δ depends only on C.

(b) Using part (a) we can find t different Pisot numbers $\theta_1,\dots,\theta_t \in k$ such that $v_i(\theta_i) > 1$, $|v_j(\theta_i)| < 1$ for $j \neq i$ and $|N(1-\theta_i)| < \mathcal{D}_k^{\delta}$ ($1 \leqslant i \leqslant t$, v_j are the infinite places of k). It follows that $\alpha = (1-\theta_1)\dots(1-\theta_t)$ satisfies the conditions at the infinite places. □

Corollary 3.5. *Given $t \in \mathbb{N}$, there exists an asymptotically bounded sequence of fields $(l_i)_{i\in\mathbb{N}}$ such that $r_2(l_i) = t$ for all i.*

Proof. We start with an infinite unramified tower (k_i) of totally real fields with $rd_{k_i} \leqslant c_0$ provided by Theorem 3.3. As the degrees $d_i \to \infty$, we can assume that $d_i \geqslant t$ for all i. Let $k = k_i$ be one of the fields. Let $\theta_1,\dots,\theta_t \in k$ be Pisot numbers chosen as in part (b) of the lemma and let $\alpha = (1-\theta_1)\dots(1-\theta_t)$. Then the field $l = k[\sqrt{\alpha}\,]$ has precisely t complex places and we have the following bound for its discriminant:

$$\mathcal{D}_l \leqslant \mathcal{D}_k^2 2^{2d}\big|N(\alpha)\big| \leqslant \mathcal{D}_k^2 2^{2d}\mathcal{D}_k^{t\delta};$$
$$rd_l \leqslant 2\mathcal{D}_k^{\frac{2+t\delta}{2d}} \leqslant 2c_0^{\frac{2+t\delta}{2}}$$

(here the first inequality follows from [21, Proposition 8, p. 62], [21, Proposition 14, p. 66] and some elementary properties of the norm). Repeating this procedure for all k_i we obtain an asymptotically bounded sequence of fields with the required properties. □

From Minkowski's theorem it follows that there exists a positive lower bound for the constants c_0 of asymptotically bounded sequences of fields. Although we do not require it in this paper, it would be interesting to know more about this bound and its dependence on the number of complex places of the fields in the sequences.

4. Arithmetic subgroups and their covolumes

4.1. Let H be a semisimple connected linear Lie group without compact factors. It is known that if H contains irreducible lattices then all of its almost simple factors are of the same type. Such groups H are called *isotypic* or *typewise homogeneous* (see [25, Chapter 9.4]). So from now on we shall assume that H is isotypic. Moreover, without loss of generality we can further assume that the center of H is trivial. This implies that H is isomorphic to $\operatorname{Ad} H$, where Ad denotes as usual the adjoint representation. The group $\operatorname{Ad} H$ is the connected component of identity of the $\mathbb{R}$-points of a semisimple algebraic $\mathbb{R}$-group. There exist, therefore, absolutely simple $\mathbb{R}$-groups G_i, all of the same type, such that $H = (\prod_{i=1}^{a}\mathrm{G}_i(\mathbb{R})\times\mathrm{G}_{a+1}(\mathbb{C})^b)^o$. A classical theorem of Borel [7] (see also [9]) asserts that such H does contain irreducible lattices.

Let now G be an algebraic group defined over a number field k which admits an epimorphism $\phi : \mathrm{G}(k\otimes_{\mathbb{Q}}\mathbb{R})^o \to H$ whose kernel is compact. In this case, $\phi(\mathrm{G}(\mathcal{O}))$ is an irreducible lattice

in H. Such lattices and the subgroups of H which are commensurable with them are called *arithmetic*. It can be shown that to define all arithmetic subgroups of H it is sufficient to consider only simply connected, absolutely almost simple k-groups G which have the same (absolute) type as the almost simple factors of H and are defined over the fields with at most b complex and at least a real places. In this case, as G is a simply connected k-group, $\mathrm{G}(k \otimes_{\mathbb{Q}} \mathbb{R})$ is connected. We shall call such groups G and corresponding fields k *admissible*.

The local-global principle provides a standard way to construct arithmetic subgroups which will be particularly useful for us. Let $\mathrm{P} = (\mathrm{P}_v)_{v \in V_f}$ be a collection of parahoric subgroups $\mathrm{P}_v \subset \mathrm{G}(k_v)$ of a simply connected k-group G. The family P is called *coherent* if $\prod_{v \in V_\infty} \mathrm{G}(k_v) \cdot \prod_{v \in V_f} \mathrm{P}_v$ is an open subgroup of the adèle group $\mathrm{G}(\mathbb{A}_k)$. Now let

$$\Lambda = \Lambda(\mathrm{P}) = \mathrm{G}(k) \cap \prod_{v \in V_f} \mathrm{P}_v,$$

where P is a coherent collection. Following [29], we shall call Λ the *principal arithmetic subgroup* associated to P. We shall also call $\Lambda' = \phi(\Lambda)$ a principal arithmetic subgroup of H.

4.2. The Lie group H carries a Haar measure μ which is uniquely defined up to a constant factor. The choice of a particular normalization of μ is not essential for our considerations. From now on we shall fix a Haar measure on $\mathrm{G}(k \otimes_{\mathbb{Q}} \mathbb{R})$ for some admissible G/k following [29, Sections 1.4, 3.6], this also defines a normalized Haar measure on H which does not depend on the choice of G. We can compute the covolumes of principal arithmetic subgroups with respect to μ using Prasad's volume formula. By [29, Theorem 3.7], we have:

$$\mu\big(H/\Lambda'\big) = \mathcal{D}_k^{\dim(\mathrm{G})/2} \big(\mathcal{D}_l/\mathcal{D}_k^{[l:k]}\big)^{\frac{1}{2}s} \left(\prod_{i=1}^{r} \frac{m_i!}{(2\pi)^{m_i+1}} \right)^{[k:\mathbb{Q}]} \tau_k(\mathrm{G}) \mathcal{E}(\mathrm{P}),$$

where

(i) $\dim(\mathrm{G})$, r and m_i denote the dimension, rank and Lie exponents of G;
(ii) l is a Galois extension of k defined as in [29, 0.2] (if G is not a k-form of type ${}^6\mathrm{D}_4$, then l is the split field of the quasi-split inner k-form of G, and if G is of type ${}^6\mathrm{D}_4$, then l is a fixed cubic extension of k contained in the corresponding split field; in all the cases $[l : k] \leqslant 3$);
(iii) $s = s(\mathrm{G})$ is an integer defined in [29, 0.4], in particular, $s = 0$ if G is an inner form of a split group and $s \geqslant 5$ if G is an outer form;
(iv) $\tau_k(\mathrm{G})$ is the Tamagawa number of G over k (since G is simply connected and k is a number field, $\tau_k(\mathrm{G}) = 1$); and
(v) $\mathcal{E}(\mathrm{P}) = \prod_{v \in V_f} e_v$ is an Euler product of the local factors $e_v = e(\mathrm{P}_v)$.

The local factors e_v can be effectively computed using the Bruhat–Tits theory. In order to justify this claim we will need a few more definitions.

4.3. Let k_v be a nonarchimedean local field of characteristic zero (a finite extension of the p-adic field $\mathbb{Q}_p$), and let G be an absolutely almost simple, simply connected k_v-group. The Bruhat–Tits theory [11] associates to G/k_v a simplicial complex $\mathcal{B} = \mathcal{B}(\mathrm{G}/k_v)$ on which $\mathrm{G}(k_v)$

acts by simplicial automorphisms. The complex $\mathcal{B}$ is called the *affine building* of G/k_v. A *parahoric subgroup* P of $G(k_v)$ is defined as a stabilizer of a simplex of $\mathcal{B}$. Every parahoric subgroup is compact and open in $G(k_v)$ in the p-adic topology. Maximal parahoric subgroups are the maximal compact subgroups of $G(k_v)$; they are characterized by the property of being the stabilizers of the vertices of $\mathcal{B}$. A maximal parahoric subgroup is called *special* if it fixes a *special vertex* of $\mathcal{B}$. A vertex $x \in \mathcal{B}$ is special if the affine Weyl group W of $G(k_v)$ is a semidirect product of the translation subgroup by the isotropy group W_x of x in W. In this case, W_x is canonically isomorphic to the (finite) Weyl group of the k_v-root system of G. If G is quasi-split over k_v and splits over an unramified extension of k_v, then $G(k_v)$ contains also *hyperspecial* parahoric subgroups (see [37, 1.10]); these subgroups are parahoric subgroups of $G(k_v)$ of the maximal volume [37, 3.8.2].

Every special (or hyperspecial) parahoric subgroup P_v has a normal pro-p subgroup the quotient by which is a quasi-simple group (i.e. it is simple modulo the center), and hence it also has a maximal prosolvable normal subgroup with a finite simple (non-abelian) quotient. Such a maximal normal subgroup is unique.

Following [29], we associate to a parahoric subgroup $P_v \subset G(k_v)$ two reductive groups $\overline{\mathcal{M}}_v$ and $\overline{M}_v$ over the residue field $\mathbb{F}_v$ of k_v: Using the Bruhat–Tits theory one can define a smooth affine group scheme G_v over the ring of integers $\mathcal{O}_v$ of k_v, whose generic fiber ($= G_v \times_{\mathcal{O}_v} k_v$) is isomorphic to $G(k_v)$ and whose group of integral points is isomorphic to P_v. Then $\overline{M}_v$ denotes a maximal connected reductive $\mathbb{F}_v$-subgroup of $G_v \times_{\mathcal{O}_v} \mathbb{F}_v$. The group $\overline{\mathcal{M}}_v$ is defined in a similar way for the quasi-split inner form $\mathcal{G}$ of $G(k_v)$ and a specially chosen parahoric subgroup of $\mathcal{G}$. We refer to [29, 2.2] for the details and finally write down the expression for the local factor e_v in the volume formula:

$$e_v = e(P_v) = \frac{\#\mathbb{F}_v^{(\dim(\overline{M}_v)+\dim(\overline{\mathcal{M}}_v))/2}}{\#\overline{M}_v(\mathbb{F}_v)}.$$

Assume now that G is quasi-split over k_v and P_v is a special parahoric subgroup, which is, moreover, assumed to be hyperspecial if G splits over an unramified extension of k_v. In this case, $\overline{\mathcal{M}}_v$ is isomorphic to $\overline{M}_v$ and $\overline{M}_v(\mathbb{F}_v)$ is a finite simple group of the same type as G. So the computation of $e(P_v)$ becomes easy (see [29, Remark 3.11] and Section 6 below). We recall that these conditions on G and P_v are indeed satisfied for almost all nonarchimedean places of k: G is quasi-split over almost every k_v and $\prod_{v\in V_\infty} G(k_v) \cdot \prod_{v\in V_f} P_v$ being open in $G(\mathbb{A}_k)$ implies that P_v is hyperspecial for almost every v. Thus generically the computation of the local factors in the volume formula is pretty straightforward.

4.4. Let Γ be a maximal arithmetic lattice in H. It is known that Γ can be obtained as a normalizer in H of the image Λ' of some principal arithmetic subgroup Λ of $G(k)$ (see [10, Proposition 1.4(iv)]). Moreover, such Λ's are principal arithmetic subgroups of *maximal type* in a sense of Rohlfs (see [33] and also [13] for precise definitions). In order to prove the main theorem we will need certain control over the structure of Λ and the index $[\Gamma : \Lambda']$ in terms of the covolume of Γ. For this purpose we recall two results which follow from [1].

Let $\Gamma = N_H(\Lambda')$ ($\Lambda' = \phi(\Lambda)$, $\Lambda = G(k) \cap \prod_{v\in V_f} P_v$) be a maximal arithmetic lattice of covolume less than x, with x large enough.

Proposition 4.1. *Let T be the smallest set of nonarchimedean places of k such that for every $v \in V_f \smallsetminus T$, G is quasi-split over k_v, splits over an unramified extension of k_v, and P_v is hyperspecial. Then there exists a constant $C_1 = C_1(H)$ such that $\prod_{v\in T} q_v \leqslant x^{C_1}$.*

Proof. This result follows from [1, Sections 4.1, 4.3, 4.4] but is not stated there explicitly. We recall the main steps of the proof.

Let T_1 be the subset of the nonarchimedean places of k such that G is not quasi-split over k_v for $v \in T_1$, let $R \subset V_f$ be the set of places for which G is quasi-split but is not split over an unramified extension of k_v, and let $T_2 \subset V_f \smallsetminus (T_1 \cup R)$ be the set of places for which P_v is not hyperspecial. Then $T = T_1 \cup R \cup T_2$ is a finite subset of V_f. Moreover,

$$\mu(H/\Gamma) \geqslant c_1 \prod_{v\in T_1} q_v^{\delta_1}, \quad \text{by [1, 4.3];}$$

$$\mu(H/\Gamma) \geqslant c_2\big(\mathcal{D}_l/\mathcal{D}_k^{[l:k]}\big)^{\delta_2} \geqslant c_2 \prod_{v\in R} q_v^{\delta_2}, \quad \text{by [1, 4.1], see also [1, 4.3];}$$

$$\mu(H/\Gamma) \geqslant c_3 \prod_{v\in T_2} q_v^{\delta_3}, \quad \text{by [1, 4.4],}$$

where $c_1, c_2, c_3 > 0$ are some absolute constants and $\delta_1, \delta_2, \delta_3 > 0$ are constants which depend only on the Lie type of H.

Altogether, these inequalities imply that there exist $c > 0$ and $\delta = \delta(H) > 0$ such that $x \geqslant \mu(H/\Gamma) \geqslant c \prod_{v\in T} q_v^{\delta}$, and the proposition follows. □

Proposition 4.2. *(See [1, Corollary 6.1].) There exists a constant $C_2 = C_2(H)$ such that for $Q = \Gamma/\Lambda'$ we have $|Q| \leqslant x^{C_2}$.*

4.5. For future use let us give a variant of the "level versus index" lemma where the level is controlled by the covolume of the lattice. To put it in a perspective, recall the classical lemma asserting that in $\Delta = \mathrm{SL}_2(\mathbb{Z})$, every congruence subgroup of index n contains $\Delta(m) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}))$ for some $m \leqslant n$, i.e. the level m is at most the index n. This was generalized in [22] to the congruence subgroups of an arbitrary arithmetic group Δ by paying a price for m; i.e. it was shown that $m \leqslant Cn$ for some constant C which depends on the arithmetic group Δ. Here we want to bound C in terms of the covolume.

Let us first introduce some notations. As before, let $\Lambda = \mathrm{G}(k) \cap \prod_{v\in V_f} \mathrm{P}_v$ where k is a number field with the ring of integers $\mathcal{O}$, G is a k-form of H and P_v is a parahoric subgroup of $\mathrm{G}(k_v)$, and let G_v be an $\mathcal{O}_v$-scheme with the generic fiber isomorphic to $\mathrm{G}(k_v)$ such that $\mathrm{G}_v(\mathcal{O}_v) = \mathrm{P}_v$. This induces a congruence subgroup structure on P_v defined as follows:

$$\mathrm{P}_v(r) = \mathrm{Ker}\big(\mathrm{G}_v(\mathcal{O}_v) \to \mathrm{G}_v\big(\mathcal{O}_v/\pi_v^r\mathcal{O}_v\big)\big),$$

where π_v is a uniformizer of $\mathcal{O}_v$. These congruence subgroups induce a congruence structure on Λ, $\Lambda(\pi_v^r) = \mathrm{P}_v(r) \cap \Lambda$. More generally, for every ideal I of $\mathcal{O}$ look at its closure $\overline{I}$ in $\widehat{\mathcal{O}} = \prod_v \mathcal{O}_v$.

Then $\overline{I}$ is equal to $\prod_{i=1}^{l} \pi_{v_i}^{e_i} \widehat{\mathcal{O}}$ for some $Y = \{v_1, \ldots, v_l\} \subset V_f$ and $e_1, \ldots, e_l \in \mathbb{N}$. We then define the I-congruence subgroup of Λ,

$$\Lambda(I) = \Lambda \cap \left(\prod_{i=1}^{l} \mathrm{P}_{v_i}(e_i) \cdot \prod_{v \notin Y} \mathrm{P}_v \right).$$

In particular, for every $m \in \mathbb{N}$, the m-congruence subgroup $\Lambda(m) = \Lambda(m\mathcal{O})$ is defined. Any subgroup of Λ which contains $\Lambda(I)$ for some nonzero ideal I is called a *congruence subgroup*.

Let now Λ be a principal arithmetic subgroup of a maximal type in $\mathrm{G}(k)$ and let Λ' be its image in H. Assume also that $\mu(H/\Lambda') \leqslant x$, where $x \gg 0$.

Lemma 4.3. *If Λ_1 is a congruence subgroup of Λ of index n, then $\Lambda_1 \supseteq \Lambda(m\mathcal{O})$ where $m \in \mathbb{N}$ with $m \leqslant x^C n$ and C is a constant which depends only on H.*

Proof. A similar result is proved in [24, Proposition 6.1.2] but the proposition there provides only $m \leqslant C_0 n$ for some constant C_0 depending on Λ. In fact, the proof of the proposition gives $C_0 = 1$ if certain conditions (i)–(iv) are satisfied for all primes. The role of C_0 is to compensate for the bad primes. Now, if Λ is a principal arithmetic subgroup of a maximal type as described above, then the conditions (i)–(iv) are satisfied for all the primes $v \in V_f \smallsetminus T$, where T is the set from Proposition 4.1. We need to compensate for the primes $v \in T$. For each one of them, we can start the induction argument in the proof of Proposition 6.1.2 [24] from the first congruence subgroup so, by Proposition 4.1, we can replace C_0 by x^C for some constant C depending only on H. □

Remark 4.4. Note that the index of $m\mathcal{O}$ in $\mathcal{O}$ (and hence also of $\Lambda(m\mathcal{O})$ in Λ) is not necessarily polynomial in m, but rather it is bounded by m^d where d is the degree of the defining field k of the arithmetic subgroup Λ. As d is bounded by $O(\log x)$, the index of $\Lambda(m\mathcal{O})$ in Λ is bounded by $(xn)^{c \log x}$. A better result is probably true: $\Lambda_1 \supseteq \Lambda(I)$ for some $I \lhd \mathcal{O}$ such that $[\Lambda : \Lambda(I)] \leqslant (xn)^c$ with a constant c depending only on H. This indeed follows from Lemma 4.3 if the degree of the field k is bounded.

5. Counting covers versus counting manifolds

The results of this paper rely heavily on "subgroup growth" [24] but there is a crucial difference: If M is a finite volume manifold covered by a symmetric space $X = H/K$ (H is a semisimple Lie group and K is a maximal compact subgroup of H) with $\Gamma = \pi_1(M)$, then there is a one-to-one correspondence between the n-sheeted **covers** of M and the Γ-conjugacy classes of index n subgroups of Γ. Thus, if $a_n(\Gamma)$ denotes the number of subgroups of Γ of index n and $b_n(M)$ — the number of n-sheeted covers of M, then

$$b_n(M) \leqslant a_n(\Gamma) \leqslant n b_n(M).$$

Thus, counting subgroups and counting covers are essentially the same, up to a linear factor. On the other hand, in this paper we count **manifolds**, so two covers of M are identified if they are isomorphic as manifolds even if they are not isomorphic as covers. In group theoretic terms it means that we are counting $\mathrm{Iso}(X)$-conjugacy classes of lattices, where $\mathrm{Iso}(X)$ is the group

of isometries of X. Now, H is of finite index in $\mathrm{Iso}(X)$ and so, up to a constant factor, we are counting H-conjugacy classes of lattices in H.

Ideally, what we would like to have is:

Conjecture 5.1. *There exists a constant $c = c(H)$, such that if Γ is a lattice in H and Γ_1 is a subgroup of Γ of covolume at most x in H, then the number of subgroups of Γ which are H-conjugate to Γ_1 is bounded by x^c if x is large enough.*

We do not know if this conjecture is true or just a wishful thinking. In this section we shall establish a weaker version which will suffice for our applications.

Observe first that if Γ_1 and Γ_2 are index n subgroups of a lattice Γ in H, then $\Gamma_1\backslash H/K$ is isometric to $\Gamma_2\backslash H/K$ if and only if there exists $h \in \mathrm{Iso}(X)$ which conjugates Γ_1 to Γ_2, i.e. Γ_1 and Γ_2 are conjugate in $\mathrm{Iso}(X)$. For counting purposes (up to a constant factor) we can assume $h \in H$. Such an h conjugating Γ_1 to Γ_2 is an element of the commensurability group $\mathrm{Comm}_H(\Gamma) = \{h \in H \mid [\Gamma : \Gamma \cap h^{-1}\Gamma h] < \infty\}$. Recall that if Γ is non-arithmetic irreducible lattice in H, then $[\mathrm{Comm}_H(\Gamma) : \Gamma] < \infty$ by a well-known result of Margulis [25, Theorem 1, p. 2]. This implies that counting covers of a non-arithmetic manifold M is, up to a constant factor (depending on M, though), the same as counting manifolds covering M. This is the reason why in [12] the lower bound on the number of hyperbolic manifolds was presented using covers of non-arithmetic manifolds. A similar remark applies in a different context to [4]. But, in this paper, when we deal with the higher rank H, all lattices are arithmetic and so we must consider the delicate issue of the difference between isomorphism classes of covers and isomorphisms of manifolds.

Let G be an absolutely simple, simply connected algebraic group defined over a number field k and let us fix a k-embedding $\mathrm{G} \subset \mathrm{GL}_s$ for some s. Let Z denote the center of G and $\pi : \mathrm{G} \to \overline{\mathrm{G}} := \mathrm{G}/\mathrm{Z}$ be the natural projection defined over k. If Γ is commensurable to $\mathrm{G}(\mathcal{O}) = \mathrm{G}(k) \cap \mathrm{GL}_s(\mathcal{O})$ ($\mathcal{O}$ is the ring of integers of k), then $\pi(\Gamma) \subset \overline{\mathrm{G}}(k)$, $\mathrm{Comm}_{\mathrm{G}}(\Gamma) = \mathrm{Comm}_{\mathrm{G}}(\mathrm{G}(\mathcal{O}))$ and $\pi(\mathrm{Comm}_{\mathrm{G}}(\Gamma))$ is also in $\overline{\mathrm{G}}(k)$ (see e.g. [25, Lemma VII.6.2]).

For every $v \in V_f$, let P_v be a maximal parahoric subgroup of $\mathrm{G}(k_v)$ such that $\mathrm{P} = (\mathrm{P}_v)_{v \in V_f}$ is a coherent collection. By the Bruhat–Tits theory (see Section 4.3), for every v there exists a smooth affine group scheme G_v defined over $\mathcal{O}_v$, the ring of integers of k_v, such that $\mathrm{G}_v(\mathcal{O}_v) = \mathrm{P}_v$ and $\mathrm{G}_v(k_v)$ is k_v-isomorphic to $\mathrm{G}(k_v)$. Let K_v^o be the normal pro-p subgroup of P_v, $K_v^o = \mathrm{Ker}(\mathrm{G}_v(\mathcal{O}_v) \to \mathrm{G}_v(\mathbb{F}_{q_v}))$ where $\mathbb{F}_{q_v} = \mathcal{O}_v/m_v$ is the residue field of $\mathcal{O}_v$ w.r.t. the maximal ideal m_v.

Recall that when $\mathrm{G}(k_v) = \mathrm{G}_v(k_v)$ acts on the Bruhat–Tits building $\mathcal{B}_v$ associated with it, P_v is the stabilizer of some vertex $w_v \in \mathcal{B}_v$ and K_v^o is the set of elements of $\mathrm{G}(k_v)$ which fixes pointwise the link of w_v. This link is isomorphic to the projective building of the finite group $\mathrm{G}_v(\mathbb{F}_{q_v})$, in particular, this implies that the number of vertices of the link is at most $\#\mathrm{G}_v(\mathbb{F}_{q_v}) \leqslant q_v^{\dim(\mathrm{G})}$.

Let Λ be the principal arithmetic subgroup of $\mathrm{G}(k)$ associated with $\mathrm{P} = (\mathrm{P}_v)_{v \in V_f}$ as in Section 4.1, i.e. $\Lambda = \mathrm{G}(k) \cap \prod_{v \in V_f} \mathrm{P}_v$. Let $I \subset V_f$ be a fixed finite subset of nonarchimedean places of k. It defines an ideal of $\mathcal{O}$ which we denote by the same letter. The group Λ is embedded diagonally in $\prod_{v \in I} \mathrm{G}(k_v)$. Let $\Lambda(I) = \Lambda \cap \prod_{v \in I} K_v^o$, the I-congruence subgroup of Λ. It is a finite index normal subgroup of Λ and the index is bounded by $\prod_{v \in I} q_v^{\dim(\mathrm{G})}$.

Denote by $\overline{\Lambda}$ the image $\pi(\Lambda)$ of Λ in $\overline{\mathrm{G}}(k)$. The group $\overline{\mathrm{G}}(k)$ acts on $\mathrm{G}(k)$ by the adjoint action. Let

$$N\big(\Lambda(I),\Lambda\big)=\big\{g\in\overline{\mathrm{G}}(k)\;\big|\;g\big(\Lambda(I)\big)\subseteq\Lambda\big\}.$$

This is not a subgroup but rather a union of finitely many cosets of $\overline{\Lambda}$ including $\overline{\Lambda}$ itself. We call the number of these cosets the *index of* $\overline{\Lambda}$ *in* $N(\Lambda(I),\Lambda)$ and denote it by $[N(\Lambda(I),\Lambda):\overline{\Lambda}]$.

Proposition 5.2. *Let Λ be a principal arithmetic subgroup associated with $\mathrm{P}=(\mathrm{P}_v)_{v\in V_f}$, such that P_v is a maximal parahoric subgroup for every v. If $\mu(H/\Lambda')\leqslant x$, then for every ideal I as above,*

$$\big[N\big(\Lambda(I),\Lambda\big):\overline{\Lambda}\big]\leqslant x^{C}\Big(\prod_{v\in I}q_v\Big)^{\dim(\mathrm{G})},$$

where $C=C(H)$ is a constant.

Proof. Denote

$$\mathcal{P}=\prod_{v\in V_f}\mathrm{P}_v\subset\prod_{v\in V_f}{}'\,\mathrm{G}(k_v)\quad\text{and}\quad\mathcal{K}=\prod_{v\in I}K_v^o\times\prod_{v\in V_f\smallsetminus I}\mathrm{P}_v.$$

Then, by the strong approximation theorem [28, Theorem 7.12, p. 427], Λ (resp. $\Lambda(I)$) is dense in $\mathcal{P}$ (resp. $\mathcal{K}$) and $\mathcal{P}\cap\mathrm{G}(k)=\Lambda$ (resp. $\mathcal{K}\cap\mathrm{G}(k)=\Lambda(I)$), when $\mathrm{G}(k)$ is embedded diagonally in $\prod'_{v\in V_f}\mathrm{G}(k_v)$.

Let now

$$N(\mathcal{K},\mathcal{P})=\big\{g\in\overline{\mathrm{G}}(\mathbb{A}_f)\;\big|\;g(\mathcal{K})\subseteq\mathcal{P}\big\}.$$

It is easy to see that $N(\mathcal{K},\mathcal{P})\supseteq N(\Lambda(I),\Lambda)\supseteq\overline{\Lambda}$. Indeed, if $g\in N(\Lambda(I),\Lambda)$, then it is in $N(\mathcal{K},\mathcal{P})$ by the density of Λ (resp. $\Lambda(I)$) in $\mathcal{P}$ (resp. $\mathcal{K}$) and the continuity of the action. The second inclusion is obvious. This implies

$$\big[N\big(\Lambda(I),\Lambda\big):\overline{\Lambda}\big]\leqslant\big[N(\mathcal{K},\mathcal{P}):\overline{\mathcal{P}}\big]\cdot\big[N(\Lambda,\Lambda):\overline{\Lambda}\big],$$

where $\overline{\mathcal{P}}=N(\mathcal{P},\mathcal{P})=\prod_{v\in V_f}\bar{\mathrm{P}}_v$, $\bar{\mathrm{P}}_v$ is the stabilizer of P_v in $\overline{\mathrm{G}}(k_v)$, and $\overline{\mathcal{P}}\cap\overline{\mathrm{G}}(k)=N(\Lambda,\Lambda)$. Now, by Proposition 4.2, $[N(\Lambda,\Lambda):\overline{\Lambda}]\leqslant x^C$.

If $v\in V_f\smallsetminus I$, then the projections of $\mathcal{K}$ and $\mathcal{P}$ to $\mathrm{G}(k_v)$ are both P_v, so if $g\in N(\mathcal{P},\mathcal{K})$, its v-component is in the stabilizer $\bar{\mathrm{P}}_v$ of P_v. For $v\in I$, let us denote $N(K_v^o,\mathrm{P}_v)=\{g\in\overline{\mathrm{G}}(k_v)\mid g(K_v^o)\subseteq\mathrm{P}_v\}$ and let $[N(K_v^o,\mathrm{P}_v):\bar{\mathrm{P}}_v]$ denote the number of $\bar{\mathrm{P}}_v$-cosets in $N(K_v^o,\mathrm{P}_v)$. Clearly, $N(\mathcal{K},\mathcal{P})$ is contained in $\prod_{v\in I}N(K_v^o,\mathrm{P}_v)\times\prod_{v\in V_f\smallsetminus I}N(\mathrm{P}_v,\mathrm{P}_v)$, which implies

$$\big[N(\mathcal{K},\mathcal{P}):\overline{\mathcal{P}}\big]=\prod_{v\in I}\big[N\big(K_v^o,\mathrm{P}_v\big):\bar{\mathrm{P}}_v\big]\cdot\prod_{v\in V_f\smallsetminus I}\big[N(\mathrm{P}_v,\mathrm{P}_v):\bar{\mathrm{P}}_v\big]=\prod_{v\in I}\big[N\big(K_v^o,\mathrm{P}_v\big):\bar{\mathrm{P}}_v\big].$$

We shall show that $[N(K_v^o,\mathrm{P}_v):\bar{\mathrm{P}}_v]\leqslant q_v^{\dim(\mathrm{G})}$ which will finish the proof.

The subgroup P_v, being a maximal parahoric subgroup of $\mathrm{G}(k_v)$, is the stabilizer of a vertex w_v of $\mathcal{B}_v$ and K_v^o is the subgroup of $\mathrm{G}(k_v)$ which fixes pointwise all the vertices $w \in \mathcal{B}_v$ of distance at most 1 from w_v, and the fixed point set of K_v^o is exactly this set. Thus if $g \in N(K_v^o, \mathrm{P}_v)$, then the fixed point set of $g(K_v^o)$ includes w_v, which is equivalent to $g(w_v)$ being fixed by K_v^o, i.e., $g(w_v)$ is of distance $\leqslant 1$ from w_v. As it was pointed out above, the link of a vertex of the Bruhat–Tits building of $\mathrm{G}(k_v)$ has order at most $q_v^{\dim(\mathrm{G})}$. The number of cosets of $\bar{\mathrm{P}}_v$ in $N(K_v^o, \mathrm{P}_v)$ is, therefore, also bounded by $q_v^{\dim(\mathrm{G})}$ and the proposition is now proven. □

Corollary 5.3. *If Λ_1 is a subgroup of index n in Λ containing $\Lambda(I)$, then the number of subgroups of Λ which are conjugate to Λ_1 within $\overline{\mathrm{G}}(k)$ is bounded by $nx^C(\prod_{v\in I} q_v)^{\dim(\mathrm{G})}$.*

Proof. The number of Λ-conjugates of Λ_1 is at most n. Now, if $g \in \overline{\mathrm{G}}(k)$ and $g(\Lambda_1) = \Lambda_2 \subseteq \Lambda$, then $g(\Lambda(I)) \subseteq \Lambda$, and so $g \in N(\Lambda(I), \Lambda)$. The latter contains at most $x^C(\prod_{v\in I} q_v)^{\dim(\mathrm{G})}$ cosets of $\overline{\Lambda}$ by the proposition, therefore the total number of possibilities for Λ_2 is bounded by $nx^C(\prod_{v\in I} q_v)^{\dim(\mathrm{G})}$. □

6. Proof of the lower bound

Our strategy will be the following: By using an asymptotically bounded sequence of fields k_i of degree d_i over $\mathbb{Q}$, we shall construct principal arithmetic subgroups Λ_i in H of covolume bounded by $c_1^{d_i}$ for some constant c_1. We then present in each Λ_i, $c_2^{d_i^2}$ subgroups of index at most $c_3^{d_i}$ (where c_1, c_2, c_3 are constants > 1). We further show that "generically" these subgroups are not conjugate to each other. We therefore can deduce that asymptotically H has at least $c_2^{d_i^2}$ non-conjugate lattices of covolume at most $(c_1c_3)^{d_i}$. This will prove the lower bound in Theorem 1 with $a = \log c_2/(\log c_1c_3)^2$.

If H is a real simple Lie group, let (k_i) be a totally real infinite class field tower as in Theorem 3.3, and if H is complex let (k_i) be an asymptotically bounded sequence provided by Corollary 3.5 with $t = r_2(k_i) = 1$. In both cases $d_i = d_{k_i} \to \infty$ and $rd_i = \mathcal{D}_{k_i}^{1/d_i} \leqslant c_0$, for an absolute constant c_0.

Let $k = k_i$ be one of the fields and $d = d_k$. In order to construct arithmetic lattices in H which are defined over k and have certain properties we appeal to results of [9] and [30].

Let $\widetilde{H}$ be the simply connected cover of H and let $\widetilde{H}_{cpt}$ be its compact real form. Recall that the real groups of types B_n, C_n, E_7, E_8, F_4 and G_2 are inner, while types A_n, D_n and E_6 admit both inner and outer real forms. Moreover, compact groups of types A_n ($n > 1$), D_{2n+1} and E_6 are outer (cf. [36]). We define an extension l of the field k as follows:

(i) If $\widetilde{H}$ is either complex or it is real and inner and if $\widetilde{H}_{cpt}$ is inner, let $l = k$;
(ii) If $\widetilde{H}$ is either complex or it is real and outer and if $\widetilde{H}_{cpt}$ is outer, let l be a quadratic extension of k such that the real places of k do not split in l;
(iii) If $\widetilde{H}$ is real outer and $\widetilde{H}_{cpt}$ is inner, let l be a quadratic extension of k such that $v_1 \in V_\infty(k)$ does not split in l while all the rest real v split;
(iv) If $\widetilde{H}$ is real inner and $\widetilde{H}_{cpt}$ is outer, let l be a quadratic extension of k such that $v_1 \in V_\infty(k)$ splits in l while all the rest real v do not split in l.

(We say that a real place v of k splits in a quadratic extension l if there exist two extensions of v to l.)

Note that we can always choose l so that $\mathcal{D}_{l/k} \leqslant c_0'^{\,d}$ with some absolute constant c_0': In case (i) it is clear. In case (ii) we can take $l = k[i]$ for which $c_0' = 4$ (as only primes of k which lie over 2 may possibly ramify in $k[i]$). In case (iii), let $l = k[\sqrt{1-\theta}]$, and in case (iv), $l = k[\sqrt{\theta-1}]$, where θ is a Pisot number in k provided by Lemma 3.4(a). To show that in the last two cases $\mathcal{D}_{l/k} \leqslant c_0'^{\,d}$ we can apply the same argument as in Corollary 3.5.

Let p_0 be a fixed rational prime and let v_0 be a fixed place of k above p_0.

Proposition 6.1. *There exists an absolutely simple simply connected k-group* G *such that*

(1) $\mathrm{G}(k\otimes_{\mathbb{Q}}\mathbb{R})$ *admits an epimorphism to H whose kernel is compact* (*i.e.* G *is admissible in the sense of Section* 4.1);
(2) G *is quasi-split over k_v for every $v \in V_f \smallsetminus \{v_0\}$*;
(3) *The quasi-split inner form of* G *splits over l.*

Proof. Let G_0 be an absolutely simple, simply connected, quasi-split k-group of the same absolute type as H which splits over l and does not split over k if $k \neq l$. Similarly to [30, Propositions 4, 5] it follows from [30, Theorem 1(i)] that there exists an inner twist G of G_0 over k which satisfies (1) and (2). Property (3) is satisfied automatically by the definition of G_0, which is the quasi-split inner form of G. □

Let $\mathrm{P} = (\mathrm{P}_v)_{v\in V_f}$ be a coherent collection of parahoric subgroups of G such that for every $v \neq v_0$, P_v is special and it is hyperspecial whenever l is unramified over k at v. Let $\Lambda = \mathrm{G}(k) \cap \prod_{v\in V_f} \mathrm{P}_v$ be the corresponding principal arithmetic subgroup of $\mathrm{G}(k)$. By the definition of G, the projection $\Lambda' = \phi(\Lambda)$ (induced by $\phi : \mathrm{G}(k\otimes_{\mathbb{Q}}\mathbb{R}) \to H$) is an arithmetic lattice in H. We shall now use Prasad's formula (see Section 4.2) to compute its covolume:

$$\mu\big(H/\Lambda'\big) = \mathcal{D}_k^{\dim(\mathrm{G})/2}\big(\mathcal{D}_l/\mathcal{D}_k^{[l:k]}\big)^{\frac{1}{2}s}\left(\prod_{i=1}^{r}\frac{m_i!}{(2\pi)^{m_i+1}}\right)^{[k:\mathbb{Q}]}\tau_k(\mathrm{G})\mathcal{E}(\mathrm{P}).$$

By the construction, the field l in the volume formula is the extension of k defined above, so we have

$$\mathcal{D}_k \leqslant c_0^d, \qquad \mathcal{D}_l/\mathcal{D}_k^{[l:k]} = \mathcal{D}_{l/k} \leqslant c_0'^{\,d}.$$

Since G is a simply connected group over a number field k, the Tamagawa number $\tau_k(\mathrm{G}) = 1$. It remains to analyze the Euler product

$$\mathcal{E}(\mathrm{P}) = \prod_{v\in V_f}\frac{q_v^{(\dim(\overline{\mathrm{M}}_v)+\dim(\overline{\mathcal{M}}_v))/2}}{\#\overline{\mathrm{M}}_v(\mathbb{F}_v)}.$$

For $v \neq v_0$, $\mathrm{G}(k_v)$ is quasi-split and P_v is special, so $\overline{\mathrm{M}}_v$ is isomorphic to $\overline{\mathcal{M}}_v$ over $\mathbb{F}_v$ and $\overline{\mathrm{M}}_v(\mathbb{F}_v)$ is a finite simple group of the same type as G. Indeed, since P_v is a maximal parahoric subgroup, the radical of $\overline{\mathrm{M}}_v$ is trivial, so $\overline{\mathrm{M}}_v(\mathbb{F}_v)$ is a finite semisimple group whose diagram can be obtained by deleting the vertex corresponding to P_v and all the adjacent edges from the extended Dynkin diagram of $\mathrm{G}(k_v)$. It remains to recall the definition of the special parahoric

subgroups to see that $\overline{\mathrm{M}}_v(\mathbb{F}_v)$ is a simple group of the same type as G. So the order of $\overline{\mathrm{M}}_v(\mathbb{F}_v)$ is known (see e.g. [27]):

$$\#\overline{\mathrm{M}}_v(\mathbb{F}_v) = q_v^{\dim(\overline{\mathrm{M}}_v)} \prod_{i=1}^{r} \bigl(1 \pm q_v^{-(m_i+1)}\bigr)$$

(except for the groups of type D_4 whose splitting field is of degree 3 over $\mathbb{F}_v$, but these groups do not arise in our setting). The sign $\pm$ in the formula depends on the splitting type of $\overline{\mathrm{M}}_v(\mathbb{F}_v)$.

In all the cases we obtain (for $v \neq v_0$):

$$\#\overline{\mathrm{M}}_v(\mathbb{F}_v) \geqslant q_v^{\dim(\overline{\mathrm{M}}_v)} \prod_{i=1}^{r} \bigl(1 - q_v^{-(m_i+1)}\bigr).$$

Also, as $\overline{\mathrm{M}}_v$ is isomorphic to $\overline{\mathcal{M}}_v$ over $\mathbb{F}_v$, we have $\frac{\dim(\overline{\mathrm{M}}_v)+\dim(\overline{\mathcal{M}}_v)}{2} = \dim(\overline{\mathrm{M}}_v)$.

We now can bound the covolume of Λ':

$$\mu\bigl(H/\Lambda'\bigr) \leqslant c_0^{d\cdot\dim(\mathrm{G})/2} {c_0'}^{d\cdot\frac{1}{2}s} \left(\prod_{i=1}^{r} \frac{m_i!}{(2\pi)^{m_i+1}}\right)^d \lambda_{v_0} \prod_{v\in V_f} \frac{1}{(1-q_v^{-(m_1+1)})\dots(1-q_v^{-(m_r+1)})},$$

$$\lambda_{v_0} = \frac{(1-q_{v_0}^{-(m_1+1)})\dots(1-q_{v_0}^{-(m_r+1)}) q_{v_0}^{(\dim(\overline{\mathrm{M}}_{v_0})+\dim(\overline{\mathcal{M}}_{v_0}))/2}}{\#\overline{\mathrm{M}}_{v_0}(\mathbb{F}_{v_0})}.$$

The λ_{v_0}-factor corresponds to the distinguished place v_0 of k at which we have no control over the structure of G. Still it is easy to see that

$$\lambda_{v_0} \leqslant q_{v_0}^{(\dim(\overline{\mathrm{M}}_{v_0})+\dim(\overline{\mathcal{M}}_{v_0}))/2} \leqslant q_{v_0}^{\dim(\mathrm{G})} \leqslant p_0^{d\cdot\dim(\mathrm{G})}$$

(here we use the assumption that v_0 lies over a fixed prime p_0).

Now, the Euler product

$$\prod_{v\in V_f} \frac{1}{(1-q_v^{-(m_1+1)})\dots(1-q_v^{-(m_r+1)})} = \zeta_k(m_1+1)\dots\zeta_k(m_r+1)$$

$$\leqslant \zeta(m_1+1)^d\dots\zeta(m_r+1)^d \leqslant \zeta(2)^{dr} = \left(\frac{\pi^2}{6}\right)^{dr},$$

where ζ_k is the Dedekind zeta function of k and ζ is the Riemann zeta function. The inequalities $\zeta_k(s) \leqslant \zeta(s)^d$ and $\zeta(s) \leqslant \zeta(2)$ $(s \geqslant 2)$ which we use here are elementary and easy to check.

We obtain

$$\mu\bigl(H/\Lambda'\bigr) \leqslant c_1^d, \quad \text{where } c_1 = c_0^{\frac{1}{2}\dim(\mathrm{G})} {c_0'}^{\frac{1}{2}s} \prod_{i=1}^{r} \frac{m_i!}{(2\pi)^{m_i+1}} p_0^{\dim(\mathrm{G})} \left(\frac{\pi^2}{6}\right)^r.$$

Remark 6.2. Instead of bounding the Euler product $\mathcal{E}(\mathrm{P})$, one can also give its precise expression (at least up to a rational factor which in our case is λ_{v_0}) as a product of Dedekind zeta functions and certain Dirichlet L-functions evaluated at $m_i + 1$, $i \leqslant r$. However, in order to determine the L-factors a case-by-case analysis is needed. Since the bound we get is sufficient for our purpose, we shall not go into details and skip the case-by-case routine.

Now fix a prime $p' \neq p_0$ and look at the p'-congruence subgroup $\Lambda(p')$ of Λ. The group $Q = \Lambda/\Lambda(p')$ is a quasi-semisimple finite group of order at most $p'^{d\dim(\mathrm{G})}$, and it contains an elementary abelian p'-group A of dimension at least d. This A has at least $p'^{[\frac{1}{4}d^2]}$ subgroups [24, Proposition 1.5.2], hence Λ has at least $p'^{[\frac{1}{4}d^2]}$ subgroups of index at most c_3^d, where $c_3 = p'^{\dim(\mathrm{G})}$. This gives $p'^{[\frac{1}{4}d^2]}$ lattices in H of covolume at most $(c_1c_3)^d$.

We finally claim that any given lattice in this set of $p'^{[\frac{1}{4}d^2]}$ lattices has at most p'^{c_4d} lattices within the set which are conjugate to it in H. This indeed follows from Corollary 5.3. Thus we get $p'^{[\frac{1}{4}d^2-c_4d]} \geqslant c_2^{d^2}$ different conjugacy classes of lattices in H of covolume at most $(c_1c_3)^d$ as promised.

7. Proof of the upper bound

Let us recall the main result of [1] which we are going to use in this section (see also [3] for the groups of type A_1):

Theorem 7.1. *Let H be a semisimple Lie group of real rank $\geqslant 2$ without compact factors. Denote by $m_H(x)$ the number of conjugacy classes of maximal irreducible lattices in H of covolume at most x. Then for every $\epsilon > 0$ there exists $c = c(\epsilon, H)$ such that $m_H(x) \leqslant x^{c(\log x)^\epsilon}$ for every $x \gg 0$.*

It is actually conjectured in [1] that $m_H(x)$ is polynomially bounded, but we will not need this conjecture here.

We shall count the lattices of covolume at most x by first counting the maximal ones (the number of which is small by Theorem 7.1), and then counting finite index subgroups within such maximal lattices.

In the proof below the following proposition will be used several times.

Proposition 7.2. *(See [24, Proposition 1.3.2(i)].) Let G be a group, $N \lhd G$ and $Q = G/N$. Then*

$$s_n(G) \leqslant s_n(N)s_n(Q)n^{\mathrm{rk}(Q)},$$

where $s_n(X)$ denotes the number of subgroups of X of index at most n and $\mathrm{rk}(Q)$ is the rank of Q.

It is easy to see that our results are independent of the choice of the Haar measure μ on H. For the sake of convenience in this section we shall fix μ so that $\mu(H/\Gamma) \geqslant 1$ for every lattice Γ. This is possible since by Kazhdan–Margulis theorem (see [32, Chapter XI]) there exists a positive lower bound for the covolumes of lattices in H.

We have:

$$\mathrm{L}_H(x) \leqslant m_H(x) \cdot \sup_{\substack{\Gamma \\ \mu(H/\Gamma)\leqslant x}} s_x(\Gamma), \tag{2}$$

where Γ runs over the maximal lattices in H.

Every such maximal Γ is equal to $N_H(\Lambda')$ as in Proposition 4.2, where $\Lambda' = \phi(\Lambda)$ in the notations there.

We can first use Proposition 7.2 to deduce that $s_x(\Gamma) \leqslant s_x(\Lambda')s_x(Q)x^{\mathrm{rk}(Q)}$, where $Q = \Gamma/\Lambda'$. By Proposition 4.2, $|Q| \leqslant x^{c_2}$ hence $s_x(Q) \leqslant |Q|^{\log|Q|} \leqslant x^{c_2^2 \log x}$ and $\mathrm{rk}(Q) \leqslant c_2 \log x$. Thus to prove the upper bound of Theorem 1 it suffices to give a similar bound for $s_x(\Lambda')$. Clearly, $s_x(\Lambda') \leqslant s_x(\Lambda)$. So it is sufficient to bound $s_x(\Lambda) = s_x(\widehat{\Lambda})$, where $\widehat{\Lambda}$ is the profinite completion of Λ.

To estimate $s_x(\widehat{\Lambda})$ let us recall that we assume Serre's conjecture, i.e. that Λ satisfies the congruence subgroup property. It means that the congruence kernel $C = \mathrm{Ker}(\widehat{\Lambda} \to \prod_v \mathrm{P}_v)$ is finite. To simplify the exposition we shall assume that $C = \{e\}$ and later explain how to remove this assumption.

So we need to bound from above $s_x(\prod_v \mathrm{P}_v)$. Let T be the set of "bad" valuations from Proposition 4.1. Thus, $\prod_{v\in T} q_v \leqslant x^{c_1}$ (see there) and for every $v \notin T$, P_v is hyperspecial. Now we can use Proposition 7.2 again, this time with $G = \prod_v \mathrm{P}_v$, $N = \prod_{v\notin T} \mathrm{P}_v$ and $Q = \prod_{v\in T} \mathrm{P}_v$, to deduce

$$s_x(\Lambda) \leqslant s_x(N)s_x(Q)x^{\mathrm{rk}(Q)}. \tag{3}$$

The group Q is a product of $\#T$ p-adic analytic compact groups (for possibly different primes p). Collecting together those with the same p (i.e. those $v \in T$ which lie over the same rational prime p), we get a subgroup A_p such that $A_p \subseteq \prod_{v|p} \mathrm{SL}_s(\mathcal{O}_v)$, where $\mathcal{O}$ is the ring of integers of k, the field of definition of Λ, and s is a fixed number such that $H \subseteq \mathrm{SL}_s(\mathbb{R})$. If $d = d_k$ and M_v is the maximal ideal of $\mathcal{O}_v$, then we have $p^d = \prod_{v|p}[\mathcal{O}_v : M_v]^{e_v} = \prod_{v|p} q_v^{e_v} = \prod_{v|p} p^{f_v e_v}$, where $q_v = p^{f_v}$ and e_v denotes the ramification degree. Now, $\mathrm{SL}_s(\mathcal{O}_v)$ is a p-adic analytic virtually pro-p group of dimension $\leqslant s^2 f_v e_v$. It follows that $K_p = \mathrm{Ker}(A_p \to \prod_{v|p} \mathrm{SL}_s(\mathbb{F}_{q_v}))$ is a pro-p group of rank at most $s^2 d = O(\log x)$ (by [14, Theorem 5.2 and Theorem 3.8]). We can bound the rank of A_p/K_p using the following result:

Proposition 7.3. *(See [24, Corollary 24, p. 326].)*

$$\mathrm{rk}\big(\mathrm{GL}_s(\mathbb{F}_{p^f})\big) < 2s^2 f.$$

Putting all this together, Q is a product $\prod_{p\in S} A_p$ of finitely many groups A_p, where S is the set of rational primes lying below T. It has a normal subgroup $K = \prod_{p\in S} K_p$ with $\mathrm{rk}_l(K) \leqslant s^2 d = O(\log x)$ for every l. The quotient Q/K is a subgroup of $\prod_{v\in T} \mathrm{SL}_s(\mathbb{F}_{q_v})$ and by Proposition 7.3,

$$\mathrm{rk}\Big(\prod_{v\in T} \mathrm{SL}_s(\mathbb{F}_{q_v})\Big) \leqslant \sum_{v\in T} \mathrm{rk}\big(\mathrm{SL}_s(\mathbb{F}_{q_v})\big) \leqslant 2s^2 \sum_{v\in T} f_v = O(\log x).$$

Here the last estimate follows from the fact that $\prod_{v\in T} p_v^{f_v} = \prod_{v\in T} q_v \leqslant x^c$ (by Proposition 4.1). Thus, by definition of the rank, $\mathrm{rk}(Q/K) = O(\log x)$.

So, we deduce that $\mathrm{rk}(Q) = O(\log x)$.

We are left by (3) with bounding $s_x(Q)$ and $s_x(N)$.

Let us consider $s_x(Q)$. Recall first:

Proposition 7.4. *(See [24, Corollary 1.7.5, p. 28].) Let X be a finite group. Then*

$$s_n(X) \leqslant n^{\nu(n)+r+1},$$

where $r = \mathrm{rk}(X)$ and $\nu(n)$ is the number of distinct prime divisors of n (so $\nu(n) = O(\frac{\log n}{\log\log n})$ by the prime number theorem).

We can apply Proposition 7.4 to the profinite group Q to deduce that $s_x(Q) \leqslant x^{c_3 \log x}$ as needed. Before moving to bounding $s_x(N)$, let us summarize what we have seen so far as we will use it again later.

Claim 7.5. *With the notations as above, let T_0 be a finite set of valuations of k with $\prod_{v\in T_0} q_v \leqslant x^c$ and let $Q = \prod_{v\in T_0} \mathrm{P}_v$. Then $\mathrm{rk}(Q) = O(\log x)$ and $s_x(Q) \leqslant x^{O(\log x)}$.*

Now we can turn to the more challenging task of bounding $s_x(N)$. This time N is a product of infinitely many groups $N = \prod_{v\notin T} \mathrm{P}_v$. Each group P_v is an extension of a pro-p group K_v^o by an almost simple group $L_v^o = \mathrm{P}_v/K_v^o$ of the form $\mathrm{G}_v(\mathbb{F}_{q_v})$, where G_v is the group scheme over the ring $\mathcal{O}_v$ in k_v (see Section 4.3).

Let $K^o = \prod_{v\notin T} K_v^o$ and $L^o = \prod_{v\notin T} L_v^o$, so $N/K^o \cong L^o$. Let K_v be the preimage in P_v of the center of L_v^o and $K = \prod_{v\notin T} K_v$.

Following [24, Window 3, §2], we say that a profinite group X *is in* B_k (for a fixed $k \in \mathbb{N}$) if no composition factor of X is isomorphic to $\mathrm{Alt}(m)$ with $m > k$ or to a classical finite simple group of Lie type of degree exceeding k (here *degree* means the degree of the natural projective representation). Our group N, as well as any open subgroup of it, is in B_k for a suitable k depending only on the Lie group H but not on Λ.

Recall that a *chief factor* of a group X is a quotient A/B where $B \subset A$ are both normal subgroups of X and B is a proper subgroup of A, maximal with respect to being normal in X. In this case A/B is isomorphic to S^m for some finite simple group S, and we say that this is a *non-abelian chief factor* if S is non-abelian. We will say that X *has simple non-abelian chief factors* if for every non-abelian chief factor A/B as above we have $m = 1$. By Jordan–Holder theorem, the groups appearing as chief factors are determined by any chosen chief series. Thus if X has a normal prosolvable subgroup K with X/K isomorphic to a direct product of non-abelian finite simple groups, one can deduce that X has simple non-abelian chief factors. This is clearly the case for our group N.

Recall that a subgroup M of X is called *subnormal* if there exists a sequence $X = M_0 > M_1 > \cdots > M_m = M$ with $M_{i+1} \lhd M_i$ and M_{i+1} is a maximal normal subgroup of M_i, in which case we say that M is a subnormal subgroup of *length* m in X. The number of non-abelian factors M_i/M_{i+1} will be called the *non-abelian length* of M in X.

Lemma 7.6. *Let X be a profinite group with simple non-abelian chief factors and M a subnormal subgroup of X of non-abelian length m_0 in X. Let $C(M)$ be the core of M, i.e.*

$C(M) = \bigcap_{g\in X} M^g$ is the largest subgroup of M which is normal in X. Then the non-abelian length of $C(M)$ in X is equal to m_0.

Proof. Clearly, the non-abelian length of $C(M)$ is at least m_0. We prove the converse by induction on m (the length of M in X). Assume by the induction hypothesis that the non-abelian length of $C(M_{m-1})$ is m_1 and it is at most m_0', which is the non-abelian length of M_{m-1} in X.

If M_{m-1}/M is abelian, then $m_0 = m_0'$. The group $\overline{M} = M_m \cap C(M_{m-1})$ is a normal subgroup of $C(M_{m-1})$ (since $M_m \lhd M_{m-1}$ and $C(M_{m-1}) \lhd M_{m-1}$) and

$$C(M_{m-1})/\overline{M} \cong C(M_{m-1})M_m/M_m \trianglelefteq M_{m-1}/M_m,$$

so it is abelian. It follows that $C(M_{m-1})/C(M_m)$ is also abelian (since $C(M_m) = C(\overline{M})$ and $C(\overline{M})$ is the intersection of the X-conjugates of $\overline{M}$ in $C(M_{m-1})$, where the latter is normal in X). Thus the non-abelian length of $C(M)$ is also m_1 and we are done with this case.

If M_{m-1}/M is non-abelian, then $m_0 = m_0' + 1$. In the notations of the previous paragraph we get that $C(M_{m-1})/\overline{M}$ is isomorphic to a normal subgroup of a simple group $S = M_{m-1}/M_m$. If it is trivial, then $C(M) = C(M_{m-1})$ and we finish by induction. If not, then $C(M_{m-1})/C(M_m)$ is a product of copies of S on which X acts transitively. But as every non-abelian chief factor of X is simple, there is only one such copy and the non-abelian length of $C(M)$ in X is at most $m_0' + 1 = m_0$. □

Assume now further that X is in B_k and recall an important result of Babai, Cameron and Pálfy (cf. [24, Theorem 4, p. 339]):

Theorem 7.7. *Let Y be a primitive permutation group of degree n and $Y \in B_k$. Then $|Y| \leqslant n^{f_1(k)}$, where $f_1(k)$ depends only on k.*

We mention in passing that while Theorem 7.7 as stated depends on the classification of the finite simple groups (CFSG), the way we are going to use it here (for profinite groups with "known" finite simple factors) is independent of the CFSG.

The important corollary for us is the following:

Proposition 7.8. *If X is in B_k and D is a subgroup of X of index n then there exists a subnormal subgroup M of X contained in D with $[X : M] \leqslant n^{f_1(k)}$.*

Proof. Let $X = D_0 > D_1 > \cdots > D_d = D$ be a sequence of subgroups such that D_{i+1} is a maximal subgroup of D_i. Define by induction M_{i+1} to be the core of $D_{i+1} \cap M_i$ in M_i (i.e. the maximal normal subgroup of M_i contained in $D_{i+1} \cap M_i$). Note that either $D_{i+1} \cap M_i = M_i$ (in which case $D_{i+1} \supseteq M_i$ and $M_{i+1} = M_i$) or $D_{i+1} \cap M_i$ is a maximal subgroup of M_i of index at most $[D_i : D_{i+1}]$. The action of M_i on the coset space $M_i/(D_{i+1} \cap M_i)$ is by a primitive permutation group, which is in B_k by our assumption. Thus, Theorem 7.7 implies that $|M_i/M_{i+1}| \leqslant [D_i : D_{i+1}]^{f_1(k)}$, and altogether $|X/M_d| \leqslant [X : D]^{f_1(k)}$. □

Let us now apply all these preparations to the group $N = \prod_{v\notin T} \mathrm{P}_v$. For this group we have an extra property:

Lemma 7.9. *Let M be a subnormal subgroup of N with a sequence $N = M_0 \rhd M_1 \rhd \cdots \rhd M_m = M$ in which M_i/M_{i+1} are finite simple groups. Then for every i for which M_i/M_{i+1} is non-abelian, there is a unique v such that $M_i \cap \mathrm{P}_v = \mathrm{P}_v$ while $M_{i+1} \cap \mathrm{P}_v = K_v$. Here K_v is the unique prosolvable subgroup of P_v for which P_v/K_v is a non-abelian finite simple group* (*such K_v exists since P_v is hyperspecial*).

Proof. First note that $M_i \cap \mathrm{P}_v$ is a subnormal subgroup of P_v and K_v is the unique maximal normal subgroup of P_v (see Section 4.3). For almost every v, $M \supseteq \mathrm{P}_v$, but for finitely many v this inclusion may not hold, in which case there is a first i such that $M_i \supseteq \mathrm{P}_v$, so $M_i \cap \mathrm{P}_v = \mathrm{P}_v$, but $M_{i+1} \cap \mathrm{P}_v \subseteq K_v$. In this case

$$\mathrm{P}_v/(M_{i+1} \cap \mathrm{P}_v) = M_{i+1}\mathrm{P}_v/M_{i+1} \lhd M_i/M_{i+1},$$

and so $\mathrm{P}_v/(M_{i+1} \cap \mathrm{P}_v) = M_i/M_{i+1}$.

For a given i, there is only one such v. Indeed, assume $M_i \supseteq \mathrm{P}_{v_1} \times \mathrm{P}_{v_2}$ but $M_{i+1} \cap \mathrm{P}_{v_1} \subseteq K_{v_1}$ and $M_{i+1} \cap \mathrm{P}_{v_2} \subseteq K_{v_2}$. Now, $M_{i+1} \cap (\mathrm{P}_{v_1} \times \mathrm{P}_{v_2})$ is a normal subgroup of $\mathrm{P}_{v_1} \times \mathrm{P}_{v_2}$; looking at it modulo $K_{v_1} \times K_{v_2}$ we get a normal subgroup of the product $\mathrm{P}_{v_1}/K_{v_1} \times \mathrm{P}_{v_2}/K_{v_2}$ of two non-abelian finite simple groups, which has a trivial intersection with each factor. It is therefore the trivial subgroup, i.e., $M_{i+1} \cap (\mathrm{P}_{v_1} \times \mathrm{P}_{v_2}) \subseteq K_{v_1} \times K_{v_2}$. So

$$(\mathrm{P}_{v_1} \times \mathrm{P}_{v_2})/\big(M_{i+1} \cap (\mathrm{P}_{v_1} \times \mathrm{P}_{v_2})\big) \cong M_{i+1}(\mathrm{P}_{v_1} \times \mathrm{P}_{v_2})/M_{i+1}.$$

The right hand side is a subnormal subgroup of M_i/M_{i+1} which is a simple group but the left hand side has a quotient $(\mathrm{P}_{v_1} \times \mathrm{P}_{v_2})/(K_{v_1} \times K_{v_2})$ which is a product of two simple groups — a contradiction.

Finally, we note that since all the non-abelian composition factors of X are obtained from the various P_v/K_v, it is clear that for every i there is such a place v. □

Note that if E is a normal subgroup of N, then for every $v \notin T$, either $E \cap \mathrm{P}_v \supseteq \mathrm{P}_v$ or $E \cap \mathrm{P}_v \subseteq K_v$, in which case $L_v = \mathrm{P}_v/K_v$ is one of the non-abelian composition factors appearing in N/E.

Before continuing, let us make an observation which will be needed later.

Corollary 7.10. *Let $d(N)$ denote the minimal number of generators of the profinite group $N = \prod_{v \notin T} \mathrm{P}_v$. Then $d(N) = O(\log x)$.*

Proof. Indeed, K^o is a product of infinitely many p-adic analytic pro-p groups $\mathcal{K}_p = \prod_{v|p} K_v^o$, but for every p, $\mathcal{K}_p$ is a subgroup of a uniform pro-p group of dimension bounded by $O(\log x)$ and hence $d(K^o) = O(\log x)$. The quotient N/K^o is an infinite product of finite quasi-simple groups. The multiplicity of each one is bounded by $O(\log x)$ and hence $d(N/K^o) = O(\log x)$. Altogether $d(N)$ is also bounded by a constant multiple of $\log x$. □

We are now ready to bound $s_x(N)$: If D is a subgroup of index at most x in N, then by Proposition 7.8 it contains a subnormal subgroup M of N of index at most x^c. The non-abelian composition factors between M and N correspond to a finite set T_1 of valuations $v \notin T$, and since $q_v \leqslant |L_v| \leqslant q_v^{\dim(\mathrm{G})}$, it follows that $\prod_{v \in T_1} q_v \leqslant x^{c_1}$. Let $C(M)$ be the core of M. By Lemma 7.6 it has the same non-abelian finite simple composition factors. Moreover, from the discussion above it follows that $C(M)$ contains P_v for every $v \notin T \cup T_1$.

Now note that the number of possibilities for T_1 is bounded by x^{c_2} (this follows from $\prod_{v\in T_1} q_v \leqslant x^{c_1}$ and [1, Section 4.1 and Proposition 3.2(ii)]), and so we can fix T_1 and reduce the problem to estimating $s_x(\prod_{v\in T_1} \mathrm{P}_v)$. This brings us to the situation which was already considered in this section. The required estimate is provided by Claim 7.5. This finishes the proof of the upper bound of Theorem 1 under the assumption that $C = \mathrm{Ker}(\widehat{\Lambda} \to \prod \mathrm{P}_v)$ is trivial.

Let us now explain how to handle the case when C is non-trivial. First recall that the CSP and MP imply that it is always cyclic — a subgroup of $\mu(k)$ — the group of roots of unity in k (cf. [31, Theorem 2]). Recall that if μ_n is the group of n-roots of unity, then $\mathbb{Q}[\mu_n]/\mathbb{Q}$ is an extension of degree $\phi(n)$ which is at least $\sqrt{n}$. This implies that $\mu(k)$ is of order bounded by $O(d_k^2) = O(\log^2 x)$. Thus C is of order $O(\log^2 x)$. Secondly, note that along the way of the proof we saw that every subgroup M of N of index at most x contains an infinite product $N_1 = \prod_{v\notin T_1} \mathrm{P}_v$, where T_1 satisfies $\prod_{v\in T_1} q_v \leqslant x^c$. Therefore, the number of generators $d(M) \leqslant d(N_1) + \mathrm{rk}(Q_1)$, where $Q_1 = N/N_1 = \prod_{v\in T_1} \mathrm{P}_v$. By Corollary 7.10, $d(N_1)$ is bounded by $O(\log x)$, and by Claim 7.5, $\mathrm{rk}(Q_1)$ is bounded by $O(\log x)$. Hence, $d(M) = O(\log x)$. Moreover, using again Claim 7.5 we deduce that every subgroup M of $\widehat{\Lambda}/C$ of index at most x can be generated by at most $c' \log x$ elements. We can now apply Lemma 1.3.1(i) from [24, p. 15]: As C acts trivially on the group $\widehat{\Lambda}$, derivations are just homomorphisms and it follows that the number of subgroups of $\widehat{\Lambda}$ whose projection in $\widehat{\Lambda}/C$ is M is bounded by $|C|^{d(M)} \leqslant (\log x)^{c' \log x}$. This finishes the proof of Theorem 1. □

8. Growth of lattices in semisimple Lie groups

In this final section we are going to discuss how to extend the results of the paper to semisimple Lie groups. Given such a group H it is natural to consider only *irreducible* lattices in H, so from now on $\mathrm{L}_H(x)$ denotes the number of conjugacy classes of irreducible lattices in H of covolume at most x. We recall (see Section 4.1) that H contains irreducible lattices only if it is isotypic, and that we can assume that $H = (\prod_{j=1}^{a} \mathrm{G}_j(\mathbb{R}) \times \mathrm{G}_{a+1}(\mathbb{C})^b)^o$ for some absolutely simple $\mathbb{R}$-groups G_j, $j = 1, \ldots, a+1$.

To obtain an analogue of the lower bound of Theorem 1 which was proved in Section 6 for a simple group H, we need to modify the choice of the fields of definition (k_i): now the fields have to be chosen so that

$$r_1(k_i) \geqslant a, \qquad r_2(k_i) = b \quad \text{and} \quad \mathcal{D}_{k_i}^{1/d_i} \leqslant c_0.$$

This can be always achieved using Corollary 3.5.

For each of the fields $k = k_i$ we have to define an extension l as in Section 6. Let G be an admissible group (in the sense of Section 4.1) defined over k, and suppose that G is inner over k_{v_j} for some t_1 real places v_j of k and is outer over the remaining $t_2 = r_1(k) - t_1$ real places. We note that either t_1 or t_2 depends only on the Lie group H (the former is the case when the compact real form of the simply connected covers of the simple factors of H is outer, and the latter, if it is inner). If $t_2 = 0$ (i.e. G is an inner form over k), we let $l = k$. Otherwise, l is defined as a quadratic extension of k such that precisely t_1 real places of k split in l. Similarly to Section 6, we can always achieve that $\mathcal{D}_{l/k} \leqslant c_0'^d$: If k is a totally real field, we can take $l = k[\sqrt{-(1-\theta_1)\ldots(1-\theta_{t_1})}]$ or $l = k[\sqrt{(1-\theta_1)\ldots(1-\theta_{t_2})}]$ depending on the above mentioned two cases, where $\theta_1, \ldots, \theta_t$ are Pisot numbers in k provided by Lemma 3.4(b). If k has complex places and $t_2 \neq 0$, we can first consider its maximal totally real subfield k', using Pisot numbers define its quadratic extension l' which splits t_1 infinite places of k' (which correspond to real

places of k in the extension k/k') and has $\mathcal{D}_{l'/k'} \leqslant c_1'^{d(k')}$, and then define l as a compositum of k and l'.

With such fields k and l at hand we can repeat the rest of the argument in Section 6 and thus show that the lower bound in Theorem 1 is valid for any semisimple group H which contains irreducible lattices (i.e. for any isotypic semisimple Lie group).

The proof of the upper bound in Section 7 does not use the assumption that the Lie group is simple and can be applied without any changes to semisimple groups H assuming validity of the congruence subgroup property and Margulis–Platonov conjecture.

Thus we obtain the following generalization of Theorem 1 to semisimple Lie groups.

Theorem 8.1. *Let H be an isotypic semisimple Lie group of real rank at least* 2. *Then*:

(i) *There exists a positive constant a such that $\mathrm{L}_H(x) \geqslant x^{a \log x}$ for all sufficiently large x.*
(ii) *Assuming the CSP and MP, there exists a positive constant b such that $\mathrm{L}_H(x) \leqslant x^{b \log x}$ for all sufficiently large x.*

Acknowledgments

The authors are grateful to T. Gelander, G. Prasad, A. Rapinchuk, A. Salehi Golsefidy and Ya. Varshavsky for helpful discussions.

References

[1] M. Belolipetsky, Counting maximal arithmetic subgroups (with an appendix by J. Ellenberg and A. Venkatesh), Duke Math. J. 140 (1) (2007) 1–33.
[2] M. Belolipetsky, Geodesics, volumes and Lehmer's conjecture, Oberwolfach Rep. 7 (2010) 2136–2139.
[3] M. Belolipetsky, T. Gelander, A. Lubotzky, A. Shalev, Counting arithmetic lattices and surfaces, Ann. of Math. 172 (2010) 2197–2221.
[4] M. Belolipetsky, A. Lubotzky, Finite groups and hyperbolic manifolds, Invent. Math. 162 (2005) 459–472.
[5] M. Belolipetsky, A. Lubotzky, Counting non-uniform lattices, in preparation.
[6] M.J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, J.P. Schreiber, Pisot and Salem Numbers, Birkhäuser Verlag, Basel, 1992.
[7] A. Borel, Compact Clifford–Klein forms of symmetric spaces, Topology 2 (1963) 111–122.
[8] A. Borel, Commensurability classes and volumes of hyperbolic 3-manifolds, Ann. Sc. Norm. Super. Pisa (4) 8 (1981) 1–33.
[9] A. Borel, G. Harder, Existence of discrete cocompact subgroups of reductive groups over local fields, J. Reine Angew. Math. 298 (1978) 53–64.
[10] A. Borel, G. Prasad, Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups, Publ. Math. Inst. Hautes Études Sci. 69 (1989) 119–171; Addendum: Publ. Math. Inst. Hautes Études Sci. 71 (1990) 173–177.
[11] F. Bruhat, J. Tits, Groupes réductifs sur un corps local, I, Publ. Math. Inst. Hautes Études Sci. 41 (1972) 5–251; II, Publ. Math. Inst. Hautes Études Sci. 60 (1984) 5–184.
[12] M. Burger, T. Gelander, A. Lubotzky, S. Mozes, Counting hyperbolic manifolds, Geom. Funct. Anal. 12 (2002) 1161–1173.
[13] V.I. Chernousov, A.A. Ryzhkov, On the classification of maximal arithmetic subgroups of simply connected groups, Sb. Math. 188 (1997) 1385–1413.
[14] D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal, Analytic Pro-p Groups, second edition, Cambridge Stud. Adv. Math., vol. 61, Cambridge Univ. Press, Cambridge, 1999.
[15] T. Gelander, Homotopy type and volume of locally symmetric manifolds, Duke Math. J. 124 (2004) 459–515.
[16] T. Gelander, Non-compact arithmetic manifolds have simple homotopy type, preprint, arXiv:math/0111261v1 [math.DG].

[17] D. Goldfeld, A. Lubotzky, N. Nikolov, L. Pyber, Counting primes, groups and manifolds, Proc. Natl. Acad. Sci. 101 (2004) 13428–13430.
[18] D. Goldfeld, A. Lubotzky, L. Pyber, Counting congruence subgroups, Acta Math. 193 (2004) 73–104.
[19] E.S. Golod, I.P. Shafarevich, On the class field tower, Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964) 261–272 (in Russian).
[20] F. Hajir, C. Maire, Tamely ramified towers and discriminant bounds for number fields, II, J. Symbolic Comput. 33 (2002) 415–423.
[21] S. Lang, Algebraic Number Theory, Addison–Wesley, 1970.
[22] A. Lubotzky, Subgroup growth and congruence subgroups, Invent. Math. 119 (1995) 267–295.
[23] A. Lubotzky, N. Nikolov, Subgroup growth of lattices in semisimple Lie groups, Acta Math. 193 (2004) 105–139.
[24] A. Lubotzky, D. Segal, Subgroup Growth, Progr. Math., vol. 212, Birkhäuser Verlag, Basel, 2003.
[25] G.A. Margulis, Discrete Subgroups of Semisimple Lie Groups, Ergeb. Math. Grenzgeb. (3), vol. 17, Springer-Verlag, Berlin, 1991.
[26] J. Martinet, Tours de corps de classes et estimations de discriminants, Invent. Math. 44 (1978) 65–73.
[27] T. Ono, On algebraic groups and discontinuous groups, Nagoya Math. J. 27 (1966) 279–322.
[28] V.P. Platonov, A.S. Rapinchuk, Algebraic Groups and Number Theory, Pure Appl. Math., vol. 139, Academic Press, Boston, 1994.
[29] G. Prasad, Volumes of S-arithmetic quotients of semi-simple groups, Publ. Math. Inst. Hautes Études Sci. 69 (1989) 91–117.
[30] G. Prasad, A.S. Rapinchuk, On the existence of isotropic forms of semi-simple algebraic groups over number fields with prescribed local behavior, Adv. Math. 207 (2006) 646–660.
[31] G. Prasad, A.S. Rapinchuk, Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre, in: John Milnor's Collected Works, vol. V, Amer. Math. Soc., 2010, pp. 307–325.
[32] M.S. Raghunathan, Discrete Subgroups of Lie Groups, Springer, New York, 1972.
[33] J. Rohlfs, Die maximalen arithmetisch definierten Untergruppen zerfallender einfacher Gruppen, Math. Ann. 244 (1979) 219–231.
[34] A. Salehi Golsefidy, Counting lattices in simple Lie groups: the positive characteristic case, preprint, arXiv:1109.6427v1 [math.GR].
[35] J.-P. Serre, Le problème des groupes de congruence pour SL_2, Ann. of Math. 92 (1970) 489–527.
[36] J. Tits, Classification of algebraic semisimple groups, Proc. Sympos. Pure Math. 9 (1966) 33–62.
[37] J. Tits, Reductive groups over local fields, Proc. Sympos. Pure Math. 33 (1979) 29–69. Part I.
[38] H.C. Wang, Topics on totally discontinuous groups, in: Symmetric Spaces, St. Louis, MO, 1969–1970, in: Pure Appl. Math., vol. 8, Dekker, New York, 1972, pp. 459–487.
[39] A. Weil, Sur les "formules explicites" de la théorie des nombres premiers, Comm. Sém. Math. Univ. Lund (tome supplémentaire dédié à Marcel Riesz) (1952) 252–265.